Modular Forms

ky

May 27, 2025

1 Basic Definitions

1.1 Modular Groups, Modular Functions and Modular Forms

Definition 1.1 (*upper half plane* $\mathfrak{H}$)

$$\mathfrak{H} = \{z \in \mathbb{C} | Im(z) > 0\}$$

.

remark 1

Why we investigate a "half" of the plane:

Because there is conformal mapping to unit disc, $q : \mathfrak{H} \Rightarrow D \setminus \{0\}, \quad z \mapsto e^{2\pi i z}$. And it maps ∞ to 0, which helps us to investigate the property at ∞ on $\mathfrak{H}$. (Recall Conformal Mapping: f is conformal on U iff it is holomorphic and $f'(z) \neq 0$ on U.)

Proposition 1.1

The $SL(2,\mathbb{Z})$ -action on $\mathfrak{H}$ by $\gamma z = \frac{az+b}{cz+d} \quad \gamma \in SL(2,\mathbb{Z})$ is well-defined.

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

remark 2

$SL(2,\mathbb{Z})$ *is called "the full modular group",also denoted by* Γ_1.

remark 3

The matrices $\pm\gamma$ have same act on $\mathfrak{H}$, so we often work with $PSL(2,\mathbb{Z})$

Definition 1.2 (*Modular Function*)

Γ-*invariant meromorphic functions in* $\mathfrak{H}$ *which are of exponential growth at infinity (i.e.* $f(x+yi) = O(e^{Cy})$ *as* $y \to \infty$ *and* $f(x+yi) = O(e^{C/y})$ *as* $y \to 0$ *for* **some** $C > 0$ *)*

remark 4

Modular function is a well-defined function on the compact quotient space $\overline{\Gamma \setminus \mathfrak{H}}$.

In the view of Riemann surface, a modular function is a holomorphic map from compact Riemann surface $\overline{\Gamma \setminus \mathfrak{H}}$ *to Riemann Sphere* $\mathbb{C}P^1$*(*$\mathbb{C}$ *plus a point* ∞*). In addition, it is onto if the function is non-constant(by open mapping theorem).*

remark 5

Because there is no (non-constant) global holomorphic function on compact Riemann Surface $\overline{\Gamma \setminus \mathfrak{H}}$*, so a modular function must be meromophic. To break this restriction, we introduce modular form, which is global holomorphic on* $\mathfrak{H}$.

"It turns out, however, that for the purposes of doing interesting arithmetic the modular functions are not enough and that one needs a more general class of functions called modular forms."

remark 6

(?) exponential growth condition being equivalent to the requirement that f extends to a meromorphic function on the compactified space $\overline{\Gamma \setminus \mathfrak{H}}$ obtained by adding finitely many "cusps" to $\Gamma \setminus \mathfrak{H}$.

Definition 1.3 (*weakly modular of weight k*)

Let k be an integer. A meromorphic function $f : \mathfrak{H} \to \mathbb{C}$ is called a weakly modular function if it satisfies :

$$f(\gamma z) = (cz + d)^k f(z) \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}), \quad z \in \mathfrak{H} \tag{1}$$

is called a weakly modular of weight k.

remark 7

Since Γ_1 is generated by S and T, so to verify f is a weakly modular form, it's sufficient to only verify S and T satisfy equation 1.

Definition 1.4 (*modular form of weight k on Γ_1*)

A function $f : \mathfrak{H} \to \mathbb{C}$ is a modular form of weight k on Γ_1 if

(1) f is holomorphic on $\mathfrak{H}$,

(2) f is weakly modular of weight k,

*(3) f is holomorphic at ∞. (why) (another definition of (3) is f is subexponential growth at infinity.(i.e.$f(x + yi) = O(e^{Cy})$ as $y \to \infty$ and $f(x + yi) = O(e^{C/y})$ as $y \to 0$ for **any** $C > 0$))*

remark 8

The set of modular forms of weight k on Γ is denoted $M_k(\Gamma)$. We will prove latter $M_k(\Gamma_1)$ is finite-dimensional and the dimension can by compute by k.

remark 9

By the modular transformation property we can find for k odd, $M_k(\Gamma) = \{0\}$. Since $f(\frac{az+b}{cz+d}) = f(\frac{-az-b}{-cz-d}) \Rightarrow (cz + d)^k f(z) = (-cz - d)^k f(z) = -(cz + d)^k f(z) \Rightarrow f(z) = 0$ (when k odd).

Definition 1.5 (*Ring of modular forms*)

$$M_*(\Gamma) := \bigoplus_k M_k(\Gamma)$$

.

remark 10

We will prove that $M_*(\Gamma_1)$ is generated by $E_4(z)$ and $E_6(z)$.

Consider $T \in \Gamma_1$, any $f \in M_k(\Gamma_!1)$ satisfies $f(z + 1) = f(z)$, f is a periodic function of period 1. Therefore f can be written as a function of $q := e^{2\pi iz}$. That is:

Definition 1.6 (*Fourier development*)

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

1.2 The Fundamental Domain of the Full Modular Group

The act of modular group introduce an equivalence on $\mathfrak{H}$. We wonder if there is a equivalent class which is "regular" enough. We introduce the Fundamental domain of a modular group.

Definition 1.7 (*Fundamental domain for* Γ_1)

The fundamental domain $\mathcal{F}$ *for* Γ_1 *is a close subset such that:*

(1) Every point on $\mathfrak{H}$ *is equivalent under the act of* Γ_1.

(2) Any two points in the interior of $\mathcal{F}$ *is not equivalent.*

remark 11

If a subset that every point represent exactly one orbit of the action, then it's called a ***strict fundamental domain*** $\tilde{\mathcal{F}}$.

Proposition 1.2

A fundamental domain for Γ_1 *is:*

$$\mathcal{F} = \{z \in \mathfrak{H} || z| \geq 1 \quad and \quad |Re(z)| \leq \frac{1}{2}\} \tag{3}$$

And the strict fundamental domain is obtained by remove half of the boundary(keep i*).*

Proof: (to be added) rf. *A first course in modular form.* Lemma 2.3.2. ■

Finiteness of Class Numbers ♣

Definition 1.8 (*quadratic forms*)

Consider quadratic form

$$Q(x, y) = Ax^2 + Bxy + Cy^2$$

$A, B, C \in \mathbb{Z}$,$A > 0$, *and* $gcd(A, B, C) = 1$, *and the discriminant* $D = B^2 - 4AC \equiv 0, 1(mod 4)$.

Fix D, *denote by* $\mathfrak{Q}_D$ *the set of quadratic forms whose discriminant is* D.

$$\mathfrak{Q}_D = \{Q(x, y) = Ax^2 + Bxy + Cy^2 | B^2 - 4AC = D, \quad A > 0, \quad gcd(A, B, C) = 1\} \tag{4}$$

When $D < 0$, $Q \in \mathfrak{Q}_D$ *is* ***definite***. *(* $Q(x, y) = Ay^2((x + B/2A)^2 - D/4A^2) \geq 0$ *and* $Q(x, y) = 0$ *iff* $x = y = 0$*).*

When $D > 0$ $Q \in \mathfrak{Q}_D$ *is* ***indefinite***. *(* $Q(1, 0) = A > 0$ *and* $Q(b, -2a) = -da < 0$*).*

Definition 1.9 (Γ_1- *act on* $\mathfrak{Q}_D$)

Γ_1 *acts on* $\mathfrak{Q}_D$ *by* $(Q \circ \gamma)(x, y) = Q(ax + by, cx + dy)$ *for* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *(It is easy to verify that under the act of* γ, D *a is invariable).*

We say $(Q \circ \gamma)(x, y)$ *and* $Q(x, y)$ *is* ***similar***. D *is similar invariant.(next proposition)*

Proposition 1.3

If $Q_1 \sim Q_2$ *then* $D_1 = D_2$, *(The reverse is NOT true. Because the class number may not be 1). The reverse has another statement: if the matrix of two quadratic form has same determinant then they are congruent under* Γ_1.

Proof: Assume $Q_1 \circ \gamma = Q_2$, $\gamma \in \Gamma_1$, then $\gamma^T \begin{pmatrix} A_1 & B_1/2 \\ B_1/2 & C_1 \end{pmatrix} \gamma = \begin{pmatrix} A_2 & B_2/2 \\ B_2/2 & C_2 \end{pmatrix}$.Take the determinant we get: $-D_1/4 = -D_2/4$.

Warning: the quadratic form is similar is NOT equivalent to that the matrix of the quadratic form is similar. Because $\gamma^T \gamma = I \iff \gamma = I$. ■

We will proof that the number of equivalence classes, the **Class number** $h(D)$, under this action is **finite**.

Proposition 1.4

For each $Q(x,y) \in \mathfrak{Q}$, it is associated to a unique root of $Q(r,1)$ in the upper half-plane : $r_Q = (-B+i\sqrt{-D})/2A$. And we have:

$$r_{Q\circ\gamma} = \gamma^{-1}(r_Q). \quad (\gamma \in \Gamma_1)$$

(proof: calculate each roots). This means that an act on Q correspond to an act on a point in $\mathfrak{H}$. Moreover, $Q_1 \sim Q_2$ in $\mathfrak{Q}_D$ if and only if $r_{Q_1} \sim r_{Q_2}$ in $\mathfrak{H}$. (next proposition)

Proposition 1.5

$Q_1 \sim Q_2$ in $\mathfrak{Q}_D$ if and only if $r_{Q_1} \sim r_{Q_2}$ in $\mathfrak{H}$.

Proof: ($\Rightarrow$) If $Q_1 \sim Q_2$, let $Q_2 = Q_1 \circ \gamma$. Then $r_{Q_2} = \gamma^{-1}(r_{Q_1})$, $r_{Q_2} \sim r_{Q_1}$.

($\Leftarrow$) **Claim:** The map $\mathfrak{Q}_D \to \mathcal{H}_+ \quad Q(x,y) \mapsto r_Q$ is injective.

If $A_1x^2+B_1x+1=0$ and $A_2x^2+B_2x+1=0$ ($A_i, B_i \in \mathbb{Q}$) have a same root r on $\mathfrak{H}$. Then $r((A_1-A_2)r+(B_1-B_2))=0$, leads to $r=0$ or $r=-\frac{B_1-B_2}{A_1-A_2}$, contradiction.

If $\gamma r_{Q_1} = r_{Q_2}$ then $r_{Q_1} = \gamma^{-1}(r_{Q_2}) = r_{Q_2\circ\gamma}$. By injection: $Q_1 = Q_2 \circ \gamma$, $Q_1 \sim Q_2$. ■

To investigate the equivalent classes of $\mathfrak{Q}_D$, we only need consider those Q whose root is in the strict fundamental domain of Γ_1, by simple computation we get:

Definition 1.10 (*reduced quadratic forms*)

$$\mathfrak{Q}_D^{red} = \{[A,B,C] \in \mathfrak{Q}_D | -A < B \leq A < C \quad or \quad 0 \leq B \leq A = C\}$$

.

The reduced quadratic forms is the set of representative of $\mathfrak{Q}_D$ under the act of Γ_1.

$|B| \leq A \leq C$ implies $|D| = 4AC - B^2 \geq 3A^2$, so $|B|$ and A is bounded having finite possible values, so do $C = (|D|+B^2)/4A$. So we conclude that $h(D)$ is finite.

remark 12

This is a special case of the general theorem that the number of ideal classes in any number field is finite.

Example: 1. $\mathfrak{Q}_{-47}^{red} = \{[1,1,12],[2,\pm1,6],[3,\pm1,4]\}$. So $h(-47)=5$.

2. reduced quadratic forms when $-20 \leq d \leq -1$

d	-3	-4	-7	-8	-11	-12		-15		-16		-19	-20	
a	1	1	1	1	1	1	2	1	2	1	2	1	1	2
b	1	0	1	0	1	0	2	1	1	0	0	1	0	2
c	1	1	2	2	3	3	2	4	2	4	2	5	5	3

Analytic representation of class number

Formula of class number

1.3 The Finite Dimensionality of $M_k(\Gamma)$

By applying the fundamental domain, we will prove that for every k, the linear space of modular forms of weight k,$M_k(\Gamma_1)$ is finite-dimensional.

Because of the modular transformation property $(f(\frac{az+b}{cz+d}) = (cz+d)^k f(z))$, f is not well-defined on $\mathfrak{H}/\Gamma$. But the order of vanishing of a point is invariant under the transformation of Γ, so we can define $ord_P(f)$ on $\mathfrak{H}/\Gamma$

Definition 1.11 (*order of f at the point p*)

Let f be a meromorphic function on $U \subset \mathbb{C}$, then for each $p \in U$ there is a unique integer $ord_p(f)$,a $\epsilon > 0$ and a holomorphic function g with $g(p) \neq 0$, such that $f(z) = (z-p)^{ord_p(f)} g(z) \quad \forall z \in B(p,\epsilon) \setminus \{p\}$. The integer $ord_p(f)$ is called **the order of f at p.** *And we have:*

1. *If $ord_p(f) > 0$, then f has a zero of order $|ord_p(f)|$ at p.*
2. *If $ord_p(f) < 0$, then f has a pole of order $|ord_p(f)|$ at p.*
3. *If $ord_p(f) = 0$, then p is neither a zero nor a pole.*

remark 13

By Laurent expansion, a meromorphic function has expansion:

$$f(z) = \sum_{n=ord_p(f)} a_n (z-p)^n$$

with $a_{ord_p(f)} \neq 0$, for $z \in B(p,\epsilon) \setminus \{p\}$

Proposition 1.6

f is a modular form of weight k on Γ_1, then $ord_z(f)$ only depend on the orbit Γz

Proof: Multiplying a $(cz+d)^k$ on $f(z)$ don't change the order of f at z, since $z = -c/d \notin \mathfrak{H}$. ■

Definition 1.12 (*elliptic fixed points (singular points)*)

If $z \in \mathcal{H}_+$ have a non-trivial stabilizer subgroup in Γ_1, then z is a elliptic fixed points of Γ_1.

remark 14

we claim that in $\tilde{\Gamma}_1$(strict fundamental domain) we have only two elliptic fixed points : $\omega = \frac{1}{2}(-1+i\sqrt{3})$ and i, whose stabilizer subgroups are $< 1, ST, (ST)^2 >$ and $< 1, S >$ respectively. This means that in the quotient manifold $\mathfrak{H}/\Gamma$, ω and i are singular.

Definition 1.13 (*Compactified quotient space*)

$\overline{\mathfrak{H}/\Gamma_1} := \mathfrak{H}/\Gamma_1 \cup \{\infty\}$,it is compact. ∞ is called a cusp.

Definition 1.14 (*Fourier development*)

$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1$, $f(\gamma z) = f(z)$, so modular form $f(z)$ can be written as a function of $e^{2\pi i z} := q$. Because f is holomorphic at ∞, we have the Fourier development :

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i z n} = \sum_{n=0}^{\infty} a_n q^n (z \in \mathfrak{H}) \tag{5}$$

To investigate the property near ∞, we consider $q = e^{2\pi i z}$. The line $Im(z) = Y, (Y > 1)$ can be identified via a punctured disc $B(0, e^{-2\pi Y})$.

Definition 1.15 (*order of vanishing at ∞*)

a_n is Fourier coefficient of f. $order_\infty(f) := min\{n \geq 0 | a_n \neq 0\}$

remark 15

There's another way to understand the compactified space $\overline{\mathfrak{H}/\Gamma_1}$: $\overline{\mathfrak{H}/\Gamma_1} = \overline{\mathfrak{H}}/\Gamma_1$, where $\overline{\mathfrak{H}} = \mathfrak{H} \cup \mathbb{Q} \cup \infty$. Obviously, $\mathbb{Q} \cup \{\infty\}$ is $\{\infty\}$'s Γ_1- orbit.

Proposition 1.7

Let f be a non-zero modular form of weight k on Γ_1. Then

$$\sum_{P\in\mathfrak{H}/\Gamma_1}\frac{1}{n_P}ord_P(f)+ord_\infty(f)=\frac{k}{12}. \tag{6}$$

The process is available for all $k\in\mathbb{Z}$ so when $k<0$, $M_k(\Gamma_1)=\emptyset$, and when $k=0$, $f=const$ for all points, $M_0(\Gamma_1)=\mathbb{C}$ (When $k=0$, f is a holomorphic modular function on $\overline{\Gamma\setminus\mathfrak{H}}$, so it must be a constant.)

Proof: (consider the contour integral of $\frac{f'(z)}{f(z)}dz$ on strict fundamental domain). Handle carefully zeros of f on the boundary , the infinity point and the "singular points" . ■

Corollary 1.8

The dimension of $M_k(\Gamma_1)$ is 0 for $k<0$ or k odd, while for even $k\geq 0$ we have

$$dimM_k(\Gamma_1)\leq\begin{cases}[k/12]+1 & if \quad k\not\equiv 2(mod12)\\ [k/12] & if \quad k\equiv 2(mod12)\end{cases} \tag{7}$$

Proof: We have explain the case $k<0$; and for k odd, by modular transformation property $M_k(\Gamma_1)=0$.

In other cases: Choose $m=[k/12]+1$ distinct non-elliptic points P_i in $\mathfrak{H}/\Gamma_1$. Given any $f_1...f_{m+1}$, there exist a linear combination of f_i (by linear algebra), denoted by f satisfying $f(P_i)=0\quad(i=1,2...m)$.

$$\sum_{i=1}^{m}ord_{P_i}(f)\geq m=[k/12]+1>k/12$$

By proposition above: $f\equiv 0$, implying that $\{f_i\}$ are linear dependent. So $dimM_k(\Gamma_1)\leq[k/12]+1$

When $k\equiv 2(mod12)$, $k/12=\mathbb{Z}+1/6$. (Which implies f must have zero at elliptic fixed point.) .

2(mod 12) is special because the minimum solution to $3I+2W\equiv 1(mod6)$ (obtained from $\frac{1}{2}I+\frac{1}{3}W\equiv\frac{1}{6}(mod1)$) is $(1,2)$ and $3\cdot 1+4\cdot 2=7>6$, while for other equation <6. This lead to a stronger upper bound of dimension :

$$\sum ord_P(f)\leq k/12-7/6=[k/12]-1$$

Similar to the first case, consider only $m-1$ distinct points and $f_1...f_m$, the f equals to zero at $m-1$ points,

$$\sum_{i=1}^{m-1}ord_{P_i}(f)\geq m-1=[k/12]$$

so $dimM_k(\Gamma_1)\leq m-1=[k/12]$. ■

Corollary 1.9

If $f,g\in M_{12}(\Gamma_1)$ are linearly independent, then the map

$$\mathfrak{H}/\Gamma_1\cup\{\infty\}\to\mathbb{P}^1(\mathbb{C})\quad z\mapsto f(z)/g(z)$$

is an bijection.

Proof: For any $(0,0)\neq(\lambda,\mu)\in\mathbb{C}$. $f,g\in M_{12}(\Gamma_1)$, By the formula of order, $k/12=1$, $\lambda f-\mu g$ has exactly one zero in $\Gamma\setminus\mathfrak{H}\cup\{\infty\}$. (There are 3 cases: (1)No zero at elliptic fixed point. (2)i is the only zero and $ord_i=2$; (3) ω is the only zero and $ord_\omega=3$.)

So for $\forall(\lambda,\mu)\neq(0,0)$, there is exactly a $z\in\Gamma\setminus\mathfrak{H}\cup\{\infty\}$ such that $\lambda f(z)-\mu g(z)=0$. So $z\mapsto f/g(z)$ is a bijection between $\Gamma\setminus\mathfrak{H}\cup\{\infty\}$ and $\mathbb{P}^1(\mathbb{C})$.

In fact we can choose $f(z)=E_4(z)^3$ and $g(z)=\Delta(z)$(discriminant function). Then $f/g(z)=E_4(z)^3/\Delta(z)$ is what we called **modular invariant** . ■

Definition 1.16 (*hyperbolic metric*)

$$d\mu(\tau)=y^{-2}dxdy,\quad \tau=x+iy\in\mathfrak{H}$$

is called the hyperbolic metric. Denote by $Vol(\mathfrak{H} \setminus \Gamma_1)$ the volume under hyperbolic metric.
The interpretation of the factor $1/12$ is $1/4\pi \times Vol(\mathfrak{H} \setminus \Gamma_1)$
More usage of hyperbolic metric refer to ***GTM 228 5.4***
Property of hyperbolic metric: (1) It is invariant under automorphism group $GL_2^+(\mathbb{R})$.

Proposition 1.10

Let Γ be a discrete subgroup of $SL(2,\mathbb{R})$, for which $\mathfrak{H} \setminus \Gamma$ has finite volume V. Then for all $k \in \mathbb{Z}$

$$dim M_k(\Gamma) \leq \frac{kV}{4\pi} + 1$$

Notice: There are some text in the book hard to understand.

remark 16

The discret group such that $Vol(\mathfrak{H} \setminus \Gamma) < \infty$ is called ***Fuchsian group of the first kind****.*

2 Eisenstein Series and the Discriminant Function

2.1 Eisenstein Series and the Ring structure of $M_*(\Gamma_1)$

We will provide two ways to define Eisenstein Series.

For the *first*, we treat space of modular forms $M_k(\Gamma)$ as stable subspace of holomorphic functions under group action of discrete subgroup of $SL_2(\mathbb{R})$. In the process of construct such a subspace we obtain Eisenstein Series as a special case.

Definition 2.1 (*space of modular forms*)

$$M_k(\Gamma) := \{f \in H(\mathfrak{H} \cup \{\infty\}) | f|_k\gamma = f\}$$

where

$$(f|_k\gamma)(z) := (cz+d)^{-k} f(\frac{az+b}{cz+d}) := \gamma z_{[k]} f(\gamma z) \quad (z \in \mathbb{C}, \quad \gamma \in \Gamma)$$

It is easy to verify (by$(\gamma_1\gamma_2)z_{[k]} = \gamma_1(\gamma_2 z)_{[k]} \cdot \gamma_2 z_{[k]}$.) that $f|_k\gamma$ is a group action of Γ on the vector space $H(\mathfrak{H})$.

When k fixed, we see $M_k(\Gamma)$ as a G-invariant subspace of function space V. To construct $M_k(\Gamma)$, consider the sum

$$v = \sum_{g \in G} v_0|g, \quad v_0 \in V$$

Obviously, v is in the G-invariant subspace.Furthermore, if v_0 have stability subgroup G_0, just consider the smaller sum

$$v = \sum_{g \in G_0 g} v_0|g, \quad v_0 \in V$$

An spacial case of the ideal is that when $G = \Gamma_1$, $v_0 = 1$ (constant function), and $G_0 = \Gamma_\infty$, which is the stability subgroup of the cusp at ∞.

Definition 2.2 (*Eisenstein Series*)

We have $\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | n \in \mathbb{Z} \right\}$ (exercise). Because we have assumed k is even, so just work with $\overline{\Gamma_1} = PSL(2,\mathbb{Z})$ and the stabilizer $\overline{\Gamma_\infty}$ is the cyclic group generated by T.

By observation we know that two matrix in $PSL(2,\mathbb{Z})$ are in same class if and only if they have same c, d. Also, $(c,d) = 1$ for any matrix we considered (since $ad - bc = 1$).

Thus:

$$E_k(z) = \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_1} 1|_k\gamma = \sum_{\gamma \in \overline{\Gamma_\infty} \setminus \overline{\Gamma_1}} 1|_k\gamma = \frac{1}{2} \sum_{c,d \in \mathbb{Z}, (c,d)=1} \frac{1}{(cz+d)^k} \quad (z \in \mathfrak{H}) \tag{8}$$

remark 17

If we consider the general case, that is, when we act $|_k\gamma$ on a holomorphic function $p(x)$ on $\mathfrak{H}$ which is of period 1, then we have:

Definition 2.3 (*Poincare series*)

$$P(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_1} p(z)|_k\gamma = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_1} j(\gamma,z)^{-k}p(\gamma z). \tag{9}$$

$P(z)$ is well-defined since p is of period 1, and $P(z)$ invariant under $|_k\gamma$. If we take $p(z) = p_m(z) = e^{2\pi im}$ $(m \in \mathbb{Z}_+)$, then $P(z)$ is called ***Poincare series****.*

To get the Fourier expansion of Poincare series, we need the double coset decomposition of Γ_1

Lemma 1 (*Double coset decomposition*)

Let $\Gamma_\infty = \{\pm\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} | n \in \mathbb{Z}\}$ be the fixing subgroup of cusp ∞, then we have:

$$\begin{aligned} SL(2,\mathbb{Z}) &= \Gamma_\infty \bigsqcup \left(\bigsqcup_{c=1}^{\infty} \bigsqcup_{1\le d\le c,(c,d)=1} \Gamma_\infty \begin{pmatrix} * & *\\ c & d\end{pmatrix} \Gamma_\infty \right) \\ &= \Gamma_\infty \bigsqcup \left(\bigsqcup_{c=1}^{\infty} \bigsqcup_{1\le d\le c,(c,d)=1} \bigsqcup_{n\in\mathbb{Z}} \Gamma_\infty \begin{pmatrix} * & *\\ c & d\end{pmatrix} \begin{pmatrix} 1 & n\\ 0 & 1\end{pmatrix} \right) \end{aligned} \tag{10}$$

The first Γ_∞ in the decomposition correspond to $c = 0$, and in fact by only right action of Γ_∞ we are able to get all the representation. The left action of Γ_∞ has no effect on the them.

Then we can write Poincare series explicitly.

$$P(z) = p(z) + \sum_{c=1}^{\infty} \sum_{1\le d\le c,(c,d)} \sum_{n\in\mathbb{Z}} (cz+cn+d)^{-k} p\left(\frac{az+an+b}{cz+cn+d}\right). \tag{11}$$

It seem that $P(x)$ is related to a and b, however,

$$p\left(\frac{az+an+b}{cz+cn+d}\right) = p\left(\frac{a}{c} - \frac{1}{c(cz+cn+d)}\right),$$

since $ad \equiv 1 \pmod c$, a is unique module c. By period of $p(z)$, term a/c only depend on d. Next, let $p(z) = p_m(z)$, by Poisson Summation Formula about n, we have:

$$\begin{aligned} &\sum_{n\in\mathbb{Z}} (cz+cn+d)^{-k} p_m\left(\frac{a}{c} - \frac{1}{c(cz+cn+d)}\right) \\ =&\frac{e^{2\pi im\frac{a}{c}}}{c} \sum_{n=1}^{\infty} e^{2\pi inz}\cdot e^{2\pi in\frac{d}{c}} \cdot \left(\frac{m}{n}\right)^{\frac{1-k}{2}} \cdot \int_{-\infty+ic\sqrt{\frac{n}{m}}}^{+\infty+ic\sqrt{\frac{n}{m}}} t^{-k}\exp\left(-2\pi i\frac{\sqrt{mn}}{c}(t+\frac{1}{t})\right)dt. \\ =&\frac{e^{2\pi im\frac{a}{c}}}{c} \sum_{n=1}^{\infty} e^{2\pi i\frac{d}{c}} \cdot \left(\frac{m}{n}\right)^{\frac{1-k}{2}} \cdot J_k(\sqrt{\frac{mn}{c}}) \cdot e^{2\pi in}. \end{aligned} \tag{12}$$

Finally we get:

$$\begin{aligned} P_m(z) &= e^{2\pi imz} + \sum_{c=1}^{\infty} \sum_{1\le d\le c,(c,d)=1} e^{2\pi im\frac{a}{c}} \frac{1}{c} \sum_{n=1}^{\infty} e^{2\pi in\frac{d}{c}} \cdot \left(\frac{m}{n}\right)^{\frac{1-k}{2}} \cdot J_k(\sqrt{\frac{mn}{c}}) \cdot e^{2\pi in} \\ &= e^{2\pi imz} + \sum_{n=1}^{\infty} \left[(\frac{m}{n})^{\frac{1-k}{2}} \sum_{c=1}^{\infty} J_k\left(\sqrt{\frac{mn}{c}}\right) K(m,n;c) \right] \cdot e^{2\pi inz}. \end{aligned} \tag{13}$$

with

$$K(m,n;c) =: \sum_{1\le d\le c,(c,d)=1} e^{2\pi i\frac{d^{-1}m+dn}{c}} = \sum_{d\in(\mathbb{Z}/c\mathbb{Z})^*} e^{2\pi i\frac{d^{-1}m+dn}{c}}, \quad d^{-1}d \equiv 1 \pmod c. \tag{14}$$

which is called **Kloosterman Sum**.

As a supplement, we introduce some properties of Kloosterman Sum:

Proposition 2.1

$K(m,n;c)$ is a Kloosterman Sum, then we have:

(1) $K(m,n;c)$ only depend on the residue class of m and $n \pmod c$.

*(2) **Symmetry**: $K(m,n;c) = K(n,m;c)$.*

(3) If $(m',c)=1$, $K(mm',n,c) = K(m,nm',c)$.

*(4) **Decomposition**: For $(c_1,c_2)=1$,*

$$K(m,n;c_1c_2) = K(p_2m,p_2n,c_1)\cdot K(p_1m,p_1n,c_2).$$

where $p_1 \equiv c_1^{-1} \pmod{c_2}$, $p_2 \equiv c_2^{-1} \pmod{c_1}$.

Proof: (1),(2) are obvious by definition. For (3), since $(m',c)=1$, we can change the summation index.

For (4), notice that $(\mathbb{Z}/c_1c_2\mathbb{Z})^\times \cong (\mathbb{Z}/c_1\mathbb{Z})^\times \times (\mathbb{Z}/c_2\mathbb{Z})^\times \quad D \mapsto (d_1,d_2)$, ($D,d_1,d_2$ denote residue class). The left hand is where $K(m,n;c_1c_2)$ runs, and the right is where $K(...;c_1)$ and $K(...;c_2)$ runs. Thus, the term (d_1,d_2) on the right side has index

$$\frac{d_1mp_2+d^{-1}np_2}{c_1}+\frac{d_2mp_1+d_2^{-1}np_1}{c_2}=\frac{m(d_1p_2c_2+d_2p_1c_1)+n(d_1^{-1}p_2c_2+d_2^{-1}p_1c_1)}{c_1c_2}$$

Notice that by Chinese remainder theorem:

$$d_1p_2c_2+d_2p_1c_1 \equiv D \pmod{c_1c_2}, \quad d_1^{-1}p_2c_2+d_2^{-1}p_1c_1 \equiv D^{-1} \pmod{c_1c_2}.$$

Thus it is:

$$\frac{mD+nD^{-1}}{c_1c_2} \pmod{\mathbb{Z}}$$

exactly the index of term on the left hand side. Terms of both sides are one-one corresponding. ■

By property (3), we can now only deal with Kloosterman Sum when c is like p^k for p prime.

Proposition 2.2

When $(m,n,c)=1$ we have:

$$K(m,n;c) = K(mn,1;c)$$

Proof: This is stronger than property (2) above, since we only have greatest common divisor of m,n,c equals to 1.

First, we prove for $c=p^k$, p prime. Since $(a,b,p^k)=1$, there must be one of a,b not divided by p. Assume that $p \nmid b$, so $(b,p^k)=1$, and by property above:

$$K(a,b,p^k) = K(ab,1,p^k).$$

Next for general c, consider it factor decomposition. We only deal with $c=p_1^{k_1}p_2^{k_2}=c_1c_2$, $(c_1,c_2)=1$, since by induction other cases are easy.

$$\begin{aligned}K(m,n,c_1c_2) &= K(mc_1',nc_1',c_2)\cdot K(mc_2',nc_2',c_1)\\ &= K(mnc_1'^2,1,c_2)\cdot K(mnc_2'^2,1,c_1).\end{aligned}$$

And

$$\begin{aligned}K(mn,1,c_1c_2) &= K(mnc_1',c_1',c_2)\cdot K(mnc_2',c_2',c_1)\\ &= K(mnc_1'^2,1,c_2)\cdot K(mnc_2'^2,1,c_1).\end{aligned}$$

Thus we get

$$K(m,n,c) = K(mn,1,c).$$

Proposition 2.3

When $k > 2$, $E_k(z)$ is absolutely convergent

Proof: The number of pairs (c, d) with $N \leq |cz + d| < N + 1 \approx \pi(N + 1)^2 - \pi N^2 \approx O(N)$. ■

Proposition 2.4

$E_k(z)$ is non-zero

The *second* way to introduce Eisenstein series is to consider the equivalent definition of f from

$$f : \mathfrak{H} \to \mathbb{C} \quad \text{to} \quad F : L(\mathbb{C}) \to \mathbb{C}$$

by the relation $f(z) = F(\Lambda_z)$. $L(\mathbb{C})$ means lattice on $\mathbb{C}$; $\Lambda_z = \mathbb{Z}.z + \mathbb{Z}.1$.

So we see modular forms $f(z)$ as a function on lattice and get an analogous of modular transformation:

Proposition 2.5

$\lambda \in \mathbb{C}^*$ ($\mathbb{C} \setminus \{0\}$), $\Lambda \in L(\mathbb{C})$, $F(\Lambda_z) = f(z)$,where $f(z)$ is a modular form of weight k then:

$$F(\lambda\Lambda) = \lambda^{-k} F(\Lambda) \tag{15}$$

Proof: (to be added) ■

We have known that the homothety on normalized lattice correspond to equivalence on $\mathfrak{H}$ under action of Γ_1.

to construct a function F on lattice satisfying the equation above, consider:

$$G_k(\Lambda_{z_0}) = \frac{1}{2} \sum_{z \in \Lambda_{z_0} \setminus 0} z^{-k}$$

or expansion:

$$G_k(z) = \frac{1}{2} \sum_{m,n \in \mathbb{Z}(m,n) \neq (0,0)} \frac{1}{(mz + n)^k} \quad (k > 2, z \in \mathfrak{H})$$

Proposition 2.6

$\zeta(k) = \sum_{n \geq 1} \frac{1}{n^k}$ is Riemann zeta function,then:

$$G_k(z) = \zeta(k) E_k(z) \tag{16}$$

remark 18

Regard $G_k(z)$ as normalization of $E_k(z)$

Definition 2.4 (*third normalization*)

$$\mathbb{G}_k(z) = \frac{(k-1)!}{(2\pi i)^k} G_k(z) \tag{17}$$

remark 19

*We do this normalization in order that $\mathbb{G}_k(z)$ has **rational** Fourier coefficients (in section 2.2). And it is also eigenfunction for Hecke operator (in section 4).*

As a first application of Eisenstein series, we now determine the ring structure of $M^*(\Gamma_1)$.

Proposition 2.7

The ring $M^*(\Gamma_1)$ is freely generated by the modular forms E_4 and E_6. (i.e. Every modular form

can be uniquely written as polynomial of $E_4(z)$ and $E_6(z)$ and E_4, E_6 are algebra independent).

Corollary 2.8

*The inequality for dimension of $M_k(z)$ is **actually an equality** for all even $k \geq 0$.*

To prove the Proposition and Corollary, we need following lemmas.

Lemma 2

Modular forms with different weights are linearly independent.

Proof: By Vandermonde Matrix trick.

Let:

$$\alpha_1 f_1(z) + ... + \alpha_m f_m(z) = 0. \quad (\forall z \in \mathfrak{H})$$

then $\forall z \in \mathfrak{H}$:

$$\alpha_1 (cz+d)^{k_1} f_1(z) + ... + \alpha_m (cz+d)^{k_m} f_m(z) = 0.$$

$$...$$

$$\alpha_1 (cz+d)^{(m-1)k_1} f_1(z) + ... + \alpha_m (cz+d)^{(m-1)k_m} f_m(z) = 0.$$

By choosing z to be point on $\mathfrak{H}$ except vanishing point of $f_1, ..., f_m$ and unit circle, we get $\alpha_i = 0 (i = 1, 2, ..., m)$. ■

Lemma 3

Any two non-proportional modular forms of same weight is algebra independent. (Is the set of linear(Hamel) basis of $M_k(\Gamma)$ also algebraic independent?)

Proof: By contradiction. Assume modular form f_1 and f_2 have weight k. Let $P(f_1, f_2) = 0 (\forall z \in \mathfrak{H})$. Consider the (weight) homogeneous term $P_d(f_1, f_2)$ of $P(f_1, f_2)$.

$$P(f_1, f_2) = \sum_{d=1}^{N} P_d(f_1, f_2) = 0.$$

Obviously $P_d(f_1, f_2)$ has weight dk. By lemma above, $P_i (i = 1, 2, ..., N)$ are linear independent. So $P_d(f_1, f_2) = 0 (\forall z \in \mathfrak{H})$ for each d.

Let:

$$p(f_1/f_2) := P_d(f_1, f_2)/f_2^d = 0 \quad (\forall z \in \mathfrak{H}).$$

$p(t)$ has only finite roots. However f_1/f_2 is a modular function, which is a holomorphic map from $\overline{\mathfrak{H}}$ to $\mathbb{C}P^1$. By open mapping theorem[1], if f_1/f_2 is non-constant, then the image of the modular function is open, and compact, thus closed(because $\mathbb{C}P^1$ is Hausdorff). Since $\mathbb{C}P^1$ is connected, the image of f_1/f_2 is $\mathbb{C}P^1$. This is a contradiction. Thus f_1 and f_2 must be proportional. ■

By this lemma, we know that E_4^3 and E_6^2 are algebra independent. Furthermore, we can conclude that:

Corollary 2.9

E_4 and E_6 are algebra independent.

Proof: If there's $P \in C[X, Y]$ such that $P(E_4, E_6) = 0$. Because of the linear independence of modular form of different weight, just assume $P(E_4, E_6)$ have weight k.

(1) If $12|k$, then $P(E_4, E_6) = \tilde{P}(E_4^3, E_6^2) \quad (\tilde{P} \in C[X, Y])$. Since for every term of $P(E_4, E_6)$, like $E_4^p E_6^q \quad (p, q \geq 0)$, we have

$$4p + 6q = k = 12K \iff 2p + 3q = 6K.$$

then $2|q, 3|p$.

Since E_4^3, E_6^2 are algebra independent, so are E_4, E_6.

(2)For general cases, if

$$4p + 6q = k = 12m + 2r \quad (4 \leq 2r \leq 14).$$

[1]Non-constant holomorphic map between Riemman surface is open.

which is:

$$2p + 3q = 6m + r \quad (2 \leq r \leq 7).$$

We can express r as $r = 2x + 3y$ with $(0 \leq x \leq 2, 0 \leq y \leq 1)$. Then,

$$2(p - x) + 3(q - y) = 6m.$$

If $-x \leq p - x < 0$,then it is a contradiction with $3|(p - x)$. So $p \geq x$. In similar way, $q \geq y$.

By argument above, for any $P(E_4, E_6)$ of weight $k = 12m + 2r$, we can always factor out the common factor $E_4^x E_6^y \quad (4x + 6y = 2r)$ of terms of $P(E_4, E_6)$, such that

$$P(E_4, E_6) = E_4^x E_6^y \hat{P}(E_4, E_6)$$

where $\hat{P}$ has weight $12m$, going back to case (1). ■

Lemma 4 (*Basis of $M_k(\Gamma_1)$*)

For $k \geq 0$, the set $B_k = \{E_4^a E_6^b | a, b \geq 0, 4a + 6b = k\}$ is a basis of the space $M_k(\Gamma_1)$.

Proof: Since E_4 and E_6 are algebra independent, B_k is linear independent. And we have:

$$|B_k| = \#\{(a, b) \in \mathbb{Z}^2 | a, b \geq 0, 4a + 6b = k\} = \begin{cases} [k/12] + 1 & if \quad k \not\equiv 2(mod 12) \\ [k/12] & if \quad k \equiv 2(mod 12) \end{cases}$$

Because of

$$dim M_k(\Gamma_1) \leq \begin{cases} [k/12] + 1 & if \quad k \not\equiv 2(mod 12) \\ [k/12] & if \quad k \equiv 2(mod 12) \end{cases}$$

so B_k is a basis of space $M_k(\Gamma_1)$. ■

By lemmas above, we can get:

Proof of Proposition 2.7: By 4, we have:

$$M_*(\Gamma_1) := \bigoplus_k M_k(\Gamma) = \mathbb{C}[E_4, E_6] \cong \mathbb{C}[X, Y]. \tag{18}$$

So we get the structure of space of all modular forms, which is $\mathbb{C}[X, Y]$. ■

Proof of Corollary 2.8: It follows from 4 immediately.

In fact, by using discriminant function defined in Section 2.4, we can construct another basis of $M_k(\Gamma_1)$ by induction in a simpler way. Precisely, if

$$\{f_1, \ldots, f_r\}$$

is a basis of M_{k-12}. Then

$$\{\Delta(z) f_1, \ldots, \Delta(z) f_r, E_k\}$$

are linear independent in $M_k(\Gamma_1)$, E_k is the Eisenstein series of weight k.

This indicates that when the weight k plus 12, the dimension of $M_k(\Gamma_1)$ plus 1. Using induction from the first spaces $M_k \quad (k = 4, 6, 8, 10, 12, 14)$, and the upper bound of dimension then we get dimension formula.

The new basis implies the important fact that $\dim S_k(\Gamma_1) = \dim M_k(\Gamma_1) - 1$, or more precisely:

$$M_k(\Gamma_1) = \mathbb{C} E_k(z) \oplus S_k(\Gamma_1).$$

■

2.2 Fourier Expansions of Eisenstein Series

Proposition 2.10

The Fourier expansion of the Eisenstein Series $\mathbb{G}_k(z)$ (k even, $k > 2$) is

$$\mathbb{G}_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \tag{19}$$

where B_k is the kth Bernoulli number and where $\sigma_{k-1}(n)$ denotes the sum of the (k-1)st powers of the positive divisor of n.

Recall: Bernoulli number. $\sum_{k=0}^{\infty} \frac{B_k}{k!} x^k = \frac{x}{e^x - 1}$
First values are:

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30},$$
$$B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, B_{14} = \frac{7}{6}, B_{16} = -\frac{3617}{510}, B_{18} = \frac{43867}{798} \dots$$

There is an important identity about Bernoulli number and zeta function:

$$\zeta(2m) = -\frac{(2\pi i)^{2m}}{2(2m)!} \cdot B_{2m} \quad (m \in \mathbb{Z}_{\geq 1}).$$

which is:

$$\zeta(k) = -\frac{(2\pi i)^k}{2 \cdot k!} \cdot B_k \quad (k \in \mathbb{Z}, even).$$

Proof: (to be added) By calculation we get

$$G_k(z) = \frac{1}{2} \sum_{n \in \mathbb{Z}, n \neq 0} \frac{1}{n^k} + \frac{1}{2} \sum_{m,n \in \mathbb{Z}, m \neq 0} \frac{1}{(mz+n)^k} = \frac{(2\pi i)^k}{(k-1)!} \left(-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right). \tag{20}$$

■

Thus by 2.4 we get,

$$\mathbb{G}_k(z) = \frac{(k-1)!}{(2\pi i)^k} G_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{21}$$

$$\begin{aligned} E_k(z) = \frac{1}{\zeta(k)} G_k(z) &= \frac{(2\pi i)^k}{(k-1)! \zeta(k)} \left(-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right) \\ &= 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \end{aligned} \tag{22}$$

(The rest of this subsection 2.3 (except for the application) can be skipped before Section 4 is finished.)

We have only discussed Eisenstein series on full modular group Γ_1. However, we can also define it on subgroups $\Gamma_1 \subset \Gamma_1$. Here we give a useful example, which will appear in the application in Section 4.3 again.

Definition 2.5 (*Dirichlet character*)

The Dirichlet character modulo $N \in \mathbb{N}$ is a homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*.$$

For convenient, we extend χ to $\mathbb{Z}$, by defining $\chi(n) = 0$ if $\gcd(n, N) > 1$.

*The **order of a character** is the minimal integer n such that $\chi^n = 1$ (the power is multiplication). The trivial character $\chi_0 = 1$ has order 1.*

We know that the Kronecker symbol $(\frac{D}{n})$ for $D \equiv 0, 1 \pmod 4$ is a character. (Cf. Hua. Introduction to Number Theory. Chapter 7.2)

remark 20

In fact, the Dirichlet character is some kind of representation of the group $(\mathbb{Z}/N\mathbb{Z})^*$. For another example, we can represent the addition group $\mathbb{Z}/N\mathbb{Z}$ by $\phi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^* \quad \phi(a) = e^{2\pi i a/N}$. The advantages of such "representation" are on the one hand, we can denote an abstract class by one simple number and the operation is kept. On the other hand, it provide a way from discrete question to analytic method. (Cf Hua. Introduction to Number Theory. Chapter 7.1,7.2)

Definition 2.6 (*Eisenstein series with character*)

If χ is a non-trivial character modulo N and k is a positive integer with $\chi(-1) = (-1)^k$ (why?), then

$$\mathbb{G}_{k,\chi}(z) = c_k(\chi) + \sum_{n=1}^{\infty}\left(\sum_{d|n}\chi(d)d^{k-1}\right)q^n \tag{23}$$

satisfies modular transformation:(why?)

$$\mathbb{G}_{k,\chi}\left(\frac{az+b}{cz+d}\right) = \chi(a)(cz+d)^k\mathbb{G}_{k,\chi}(z) \quad z\in\mathfrak{H}, \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(N).$$

*$\mathbb{G}_{k,\chi}$ is called **Eisenstein series of weight k and character χ** on $\Gamma_0(N)$. Here $\Gamma_0(N)$ is congruence group defined in 3.3. And $c_k(\chi)\in\overline{\mathbb{Q}}$ is a constant given by $c_k(\chi) = \frac{1}{2}L(1-k,\chi)$, where $L(s,\chi)$ is the analytic continuation of L-serise of χ.(this implies the class number $h(D) = L(0,\epsilon_D)$) in Section 4.3*

The simplest examle is:

♣ Identities Involving Sums of Power of Divisors

By Fourier Expansions of Eisenstein Series, we can deduce non-trivial number-theoretic identities.

Notice that each of the space $M_4(\Gamma_1), M_6(\Gamma_1), M_8(\Gamma_1), M_{10}(\Gamma_1), M_{14}(\Gamma_1)$ has dimension 1 by formula of dimension. So they are spanned by respectively by $E_k(z)$ with leading coefficient 1. So we get identities:

$$E_4(z)^2 = E_8(z), \quad E_4(z)E_6(z) = E_{10}(z), \quad E_6(z)E_8(z) = E_4(z)E_10(z) = E_{14}(z)$$

Combined with Fourier expansions, for example the first being:

$$\sum_{k=1}^{N-1}\sigma_3(k)\sigma_3(N-k) = \frac{\sigma_7(N)-\sigma_3(N)}{120}$$

Of course similar identities can be obtained from modular forms in higher weights, even though the dimension of modular space is no longer 1. For instance $M_{12}(\Gamma_1)$ is 2-dimensional and E_4E_8, E_6^2 and E_12 is in it. So the three functions is linear dependent. In fact $441E_4E_8 + 250E_6^2 = 691E_{12}$.

2.3 The Eisenstein Series of Weight 2

In 2.1 and 2.2 we restricted to the case when $k > 2$, which guaranteed the series is absolutely convergent. The absolute convergence implies that the series is holomorphic on the upper half plane and at infinity, as well as the modular conditions(the key is arranging the terms in any way).

So the series $E_k(z), (k > 2)$ are able to be a modular forms while $E_2(z)$ not.(refer:Lec page 10).

However the formula of Fourier expansion of $\mathbb{G}_k(z)$ converges rapidly enough and defines a holomorphic function $\mathbb{G}_2(z)$. So we define Eisenstein series $E_2(z)$ in this way.

Definition 2.7 (*The Eisenstein Series of Weight 2*)

$$\mathbb{G}_2(z) = -\frac{1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)q^n = -\frac{1}{24} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + ... \tag{24}$$

.

And other forms:

$$G_2(z) = -4\pi^2\mathbb{G}_2(z)$$

$$E_2(z) = \frac{6}{\pi^2}G_2(z) = -24\mathbb{G}_2(z) = 1 - 24q - 72q^2 - ...$$

In fact, $G_2(z)$ defined above agrees with its original definition with the restriction of order of summation(n first and then m) :

$$G_2(z) = \frac{1}{2}\sum_{n\neq 0}\frac{1}{n^2} + \sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2} \tag{25}$$

The only difference is that, because we can not interchange the order of summation , the transformation equation $G_2(-1/z) = z^2 G_2(z)$ no longer establish.(However the other equation $G_2(z+1) = G_2(z)$ still holds.) So $E_2(z)$ cannot be a true modular form, nevertheless, it still have some modular property.

Proposition 2.11

For $z \in \mathfrak{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ we have

$$G_2(\frac{az+b}{cz+d}) = (cz+d)^2 G_2(z) - \pi i c(cz+d). \tag{26}$$

Proof: (Hecke)

Modify the sum slightly by:

$$G_{2,\epsilon}(z) = \frac{1}{2}\sum_{m,n}{}' \frac{1}{(mz+n)^2|mz+n|^{2\epsilon}} \quad (z \in \mathfrak{H}, \epsilon > 0). \tag{27}$$

The new series converges absolutely and we have $G_{2,\epsilon}(\frac{az+b}{cz+d}) = (cz+d)^2|cz+d|^{2\epsilon} G_{2,\epsilon}(z)$. We claim that $\lim_{\epsilon\to 0} G_{2,\epsilon}(z)$ exists and :

$$G_2^*(z) := \lim_{\epsilon\to 0} G_{2,\epsilon}(z) = G_2(z) - \frac{\pi}{2y}$$

So $G_2^*(z)$ still satisfies the modular transformation. Then we can easily get the equation we want.

To prove the claim, we first define:(when $\epsilon > -\frac{1}{2}$ $I_\epsilon(z)$ is uniformly integrable to ϵ)

$$I_\epsilon(z) = \int_{-\infty}^{+\infty} \frac{dt}{(z+t)^2|z+t|^{2\epsilon}} \quad (z \in \mathfrak{H}, \epsilon > -\frac{1}{2})$$

Then when $\epsilon > 0$

$$G_{2,\epsilon} - \sum_{m=1}^{\infty} I_\epsilon(mz) = \sum_{n=1}^{\infty} \frac{1}{n^{2+2\epsilon}} + \sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty} [\frac{1}{(mz+n)^2|mz+n|^{2\epsilon}} - \int_n^{n+1} \frac{dt}{(mz+t)^2|mz+n|^{2\epsilon}}] \tag{28}$$

Both sums on the right converge absolutely (for the integral term, use mean-value theorem).So when calculate the limit of $\epsilon \to 0$,we can interchange the limit and summation.

On the other hand for $\epsilon > -\frac{1}{2}$, we have:

$$I_\epsilon(x+iy) = \frac{1}{y^{1+2\epsilon}} \int_{-\infty}^{+\infty} \frac{dt}{(t+i)^2(t^2+1)^\epsilon} := \frac{1}{y^{1+2\epsilon}} I(\epsilon).$$

Notice that $I(\epsilon)$ is independent of z, so

$$\sum_{m=1}^{\infty} I_\epsilon(mz) = I(\epsilon)\zeta(1+2\epsilon)/y^{1+2\epsilon}$$

By Taylor expansion:

$$I(\epsilon) = -\pi\epsilon + o(\epsilon).$$

According to the knowledge of complex analysis:

$$\zeta(1+2\epsilon) = \frac{1}{2\epsilon} + O(1).$$

So $I(\epsilon)\zeta(1+2\epsilon)/y^{1+2\epsilon}$ tends to $-\frac{\pi}{2y}$ when ϵ tends to zero. Let $\epsilon \to 0$ on both sides of 28, we get:

$$G_2^*(z) + \frac{\pi}{2y} = \sum_{n=1}^{\infty} \frac{1}{n^2} + \sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty} [\frac{1}{(mz+n)^2} + (\frac{1}{(n+1)+mz} - \frac{1}{n+mz})] = G_2(z)$$

■

remark 21

*The function $G_2^*(z)$ is called **almost holomorphic modular form** of weight 2 (since $\pi/2y$ is not*

holomorphic on $\mathfrak{H}$), and $G_2(z)$ is called ***quasimodular form****.*

Generally, almost holomorphic modular form is a generalization of modualr form that (1) are polynomial in $1/Im(z)$ with coefficient that are holomorphic function of z, (2)satisfy the modular transformation. A quasimodular form is the holomorphic part of an almost holomorphic modular form.

2.4 The Discriminant Function and Cusp Forms

Definition 2.8 (*discriminant function $\Delta(z)$*)

$$\Delta(z) = e^{2\pi iz}\prod_{n=1}^{\infty}(1-e^{2\pi izn})^{24}. \tag{29}$$

Notice that $|e^{2\pi iz}| < 1$ for $z \in \mathfrak{H}$, the term of infinite product are non-zero and tend to 1 exponentially rapid as y tends to infinity ($e^{2\pi iz} = e^{-2\pi y+2\pi ix}$).

So we conclude :

Lemma 5

$\Delta(z)$ converges everywhere and defines a holomorphic and everywhere non-zero function on the upper half-plane.

Proof: Show $\Delta(z)$ is absolutely converges by using the proposition: When $a_n \geq 0$, $\prod(1+a_n)$ converges if and only if $\sum a_n$ converges.

$$|\Delta(z)| = e^{-2\pi y}\prod_{n=1}^{\infty}|1-e^{2\pi inz}|^{24} \leq e^{-2\pi y}\prod_{n=1}^{\infty}|1+e^{-2\pi ny}|^{24} = e^{-2\pi y}\prod_{n=1}^{\infty}(1+b_n) < \infty$$

(b_n is obtained by binomial theorem and $b_n = o(e^{-n})$, so $\sum b_n < \infty$.)

By order formula of modular form, there is only one zero at infinity, thus no zero at $\mathfrak{H}$. ■

Proposition 2.12

The function $\Delta(z)$ is a cusp form of weight 12 on $SL(2,\mathbb{Z})$.

Proof:

$$\frac{1}{2\pi i}\frac{d}{dz}log\Delta(z) = E_2(z)$$

By transformation equation of $E_2(z)$:

$$\frac{1}{2\pi i}\frac{d}{dz}log(\frac{\Delta(\frac{az+b}{cz+d})}{(cz+d)^12\Delta(z)}) = 0$$

So we get $(\Delta|_{12}\gamma)(z) = C(\gamma)\Delta(z)$ for all $z \in \mathfrak{H}$ and all $\gamma \in \Gamma_1$, where $C(\gamma)$ is a non-zero number depending only on γ. As we have proved $|_{12}$ is a group action, so $C : \Gamma_1 \to \mathbb{C}^*$ is a homomorphism. So it suffices to check $C(\gamma) = 1$ for generators T and S. The first is obvious and

$$\Delta(-1/z) = C(S)z^{12}\Delta(z),$$

let $z = i$, we get $C(S) = 1$. ■

The space $M_{12}(\Gamma_1)$ has dimension 2, so $\Delta(z)$ is a linear combination of the two function $E_4(z)^2$ and $E_6(z)^2$ (recall that they are linear independent).

From Fourier expansion of these modular forms, we find:

$$\Delta(z) = \frac{1}{1728}(E_4(z)^2 - E_6(z)^2). \tag{30}$$

remark 22

If we directly define $\Delta(z)$ by this equation, we can also get it's two important properties.

(1) by expansion it is obvious $\Delta(z) = q + o(q)$,no constant coefficient.

(2) recall the definition of order of vanishing at infinity: $ord_\infty(f)$: the smallest integer n such that $a_n \neq 0$ in the Fourier expansion. and formula of counting zero. By calculation, $ord_\infty(\Delta) = 1$ and the total number of zero is $k/12 = 1$. So there are no zero on $\mathfrak{H}$.

Next we introduce some application of discriminant function. By this identity, we can give another proof of 2.7

Proposition 2.13

modular form on Γ_1 is a polynomial in E_4 and E_6.

Proof: For modular form $f(z)$ of weight k,use induction by

$$h(z) = (f(z) - a_0 E_4(z)^a E_6(z)^b)/\Delta(z) \quad (4a + 6b = k)$$

Notice that, $h(z)$ is holomorphic on $\mathfrak{H}$ (since $\Delta(z)$ is non-zero at $\mathfrak{H}$) and at ∞ (since $f - a_0 E_4^a E_6^b$ has no constant coefficient and $\Delta(z)$ begin with q), so $h(z)$ is a modular form of weight $k-12$. By noticing that $\Delta(z)$ is a polynomial of E_4 and E_6 and induction on k we done. ■

Definition 2.9 (*Modular invariant*)

The modular function

$$j(z) = \frac{E_4(z)^3}{\Delta(z)} = q^{-1} + 744 + 196884q + ... \tag{31}$$

is called the modular invariant. This function defines an isomorphism from $\Gamma_1 \setminus \mathfrak{H}$ to $\mathbb{C}$.

The other application about $\Delta(z)$, we introduce the property of $\Delta(z)$'s Fourier coefficient, which is called **Ramanujan tau function**.

By expand the infinite product of Delta function we obtain:

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^2 4 = \sum_{n=1}^{\infty}\tau(n)q^n \quad (q = e^{2\pi iz}) \tag{32}$$

Obviously, $\tau(n)$ are certain integers.

remark 23

(1)Multiplicativity property of tau function: When p, q are co-prime, then $\tau(pq) = \tau(p)\tau(q)$

(2)$\tau(p^2) = \tau(p)^2 - p^{11}$ if p is prime. This property is generalized by Hecke to the theory of Hecke operators.

(3)Ramanujan observed that $|\tau(p)|$ was bounded by $2p^5\sqrt{p}$ for p prime. This is proved in 1974 by Deligne as a consequence of his proof of Weil conjecture.

A weaker bound for $\tau(p) \leq Cp^6$ is much easier to prove. The proof applies to a much more general class of modular forms, which is called **cusp form**.

Definition 2.10 (*cusp form*)

*A modular form on Γ_1 is a **cusp form** if the constant term a_0 in the Fourier expansion is zero. The space of all cusp forms of weight k is denoted by S_k.*

remark 24

The definition of cusp forms given above is actually valid only for the full modular group Γ_1 or for other groups having only ONE cusp.

In general, one must require the vanishing of the constant term of the Fourier expansion of f, suitably defined, at every cusp of the group Γ, in which case it again follows that f can be estimated as by 34.

Actually, it is easier to simply define cusp forms of weight k as modular forms for which $y^{k/2}f(x+iy)$ is bounded, a definition which is equivalent but does not require the explicit knowledge of the Fourier expansion of the form at every cusp.

So $ord_\infty(f) > 0$ for $f \in S_k$, in other words, f vanishes when z tends to ∞, the point ∞ is the "cusp" of the quotient space $\overline{\Gamma \setminus \mathfrak{H}}$. "Cusp form" can be interpreted as "modular form which vanishes at cusp".

Compare cusp form with Eisenstein series, both are basic examples of modular form. We notice that the constant coefficient of Eisenstein series $a_0 \neq 0$. We have decomposition

Proposition 2.14

$$M_k(\Gamma_1) = \mathbb{C}E_k \oplus S_k(\Gamma_1) \tag{33}$$

Proof: (lww Pro 2.6.3) ■

For Eisenstein series $\mathbb{G}_k(z)$, the Fourier coefficient $a_n \sim n^{k-1}$ (since $n^{k-1} \leq \sigma_{k-1}(n) < \zeta(k-1)n^{k-1}$).

For cusp form, we have

Proposition 2.15

Let $f(z)$ be a cusp form of weight k on Γ_1 with Fourier expansion $\sum_{n=1}^{\infty} a_n q^n$.Then

$$|a_n| \leq Cn^{k/2} \quad (n \geq 1)$$

for some C depending only on f.

Proof: Consider the function $g(z) = y^{k/2}|f(z)| \quad z = x + iy \in \mathfrak{H}$, easy to verify it is Γ_1-invariant.

Since $|f(z)| = O(|q|) = O(e^{-2\pi i})t$ when $q \to 0$, we have

$$g(z) = y^{k/2}|f(z)| \sim y^{k/2}e^{-2\pi y} \to 0, \quad y \to 0$$

.

So $g(z)$ bounded on Γ_1's fundamental domain, which means it is bounded on $\mathfrak{H}$.Thus we have

$$|f(z)| \leq cy^{-k/2} \quad z \in \mathfrak{H} \tag{34}$$

Consider the integral representation of Fourier coefficient:

$$a_n = e^{2\pi ny} \int_0^1 f(x+iy)e^{-2\pi nx}dx \tag{35}$$

we have :

$$|a_n| \leq cy^{-k/2}e^{2\pi ny}$$

Let $y = \frac{1}{n}$,we get

$$|a_n| \leq ce^{2\pi} \cdot n^{k/2}.$$

■

By this proposition, we get $\tau(p) \leq Cp^6$.

♣ Congruences for $\tau(n)$

Proposition 2.16

$\tau(n)$ is Fourier coefficient of $\Delta(z)$, we have congruence relation :

$$\tau(n) \equiv \begin{cases} 1 \pmod 2 & \text{if } n \text{ is an odd squre,} \\ 0 \pmod 2 & \text{otherwise.} \end{cases} \tag{36}$$

Proposition 2.17 (*Ramanujan Congruence*)

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691} \quad (n \geq 1) \tag{37}$$

remark 25

the number "691" comes from the relation(write $\mathbb{G}_{12}(z)$ as $\Delta(z)$ and its remainder by E_4 and E_6):

$$\mathbb{G}_{12}(z) = \Delta(z) + \frac{691}{156}(\frac{E_4(z)^3}{720} + \frac{E_6(z)^2}{1008})$$

3 Theta Series

"The problem of the representation of an integer n as the sum of a given number k of integral squares is one of the most celebrated in the theory of numbers. Its history may be traced back to Diophantus, but begins effectively with Girard's (or Fermat's) theorem that a prime $4m+1$ is the sun of two squares. Almost every arithmetician of note since Fermat has contributed to the solution of the problem, and it has its puzzles for us still. —G.H.Hardy, 1940"

For a positive definite integer valued quadratic form Q in m variables, there is an associated modular form of weight $m/2$, called the **theta series** of Q. The nth Fourier coefficient for every $n \geq 0$ is the number of representations of n by Q.

Definition 3.1 (*Theta series*)

Consider a positive definite quadratic form in m variables $Q(x)$, and define:

$$r_Q(n) = \#\{x \in \mathbb{Z}^m | Q(x) = n\},$$

which is the number of representations of n by $Q(x)$. The theta function associated to $Q(x)$ is

$$\theta_Q(z) = \sum_{x \in \mathbb{Z}^m} q^{Q(x)} = \sum_{n=0}^{\infty} r_Q(n) q^n.$$

where as usual $q = e^{2\pi i z}$.

This is one of the main constructions of modular form, as well as gives some important application in number theory.(such as sum of squares problem).

3.1 Jacobi's Theta Series

We first consider unary theta series ($m = 1$). Take $Q(x) = x^2$, we get Jacobi's theta series.

Definition 3.2 (*Jacobi's theta series*)

$$\theta = \sum_{n \in \mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + ..., \tag{38}$$

where $z \in \mathfrak{H}$

The transformation properties are as follows:

Proposition 3.1

The function $\theta(z)$ satisfies:

$$\theta(z+1) = \theta(z), \quad \theta(\frac{-1}{4z}) = \sqrt{\frac{2z}{i}}\theta(z) \quad (z \in \mathfrak{H}). \tag{39}$$

Proof: The first one is trivial. For the second, use *Poisson transformation formula*: Function f satisfying

(i) f is holomorphic on some horizontal strip $S_a = \{z \in \mathbb{C} || Im(z)| < a\}$.

(ii) There exists constant $A > 0$ such that $|f(x+iy)| \leq \frac{A}{1+x^2}$, for $x \in \mathbb{R}$ and $|y| < a$

is called **moderate decrease** function, denoted by $\mathfrak{F}$. If $f \in \mathfrak{F}$, then

$$\sum_{n \in \mathbb{Z}} f(z) = \sum_{n \in \mathbb{Z}} \hat{f}(z). \quad \text{(Poisson summation formula)} \tag{40}$$

Let $f = e^{-\pi t n^2} \quad (t > 0)$, we get

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} \frac{e^{-\pi n^2/t}}{\sqrt{t}}.$$

So when $t = -i2z > 0$ (i.e. on the line $z = \frac{it}{2}$), we have:

$$\theta(\frac{-1}{4z}) = \sum_{n\in\mathbb{Z}} e^{\frac{-\pi n^2}{-i2z}} = \sqrt{\frac{2z}{i}} \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 t} = \sqrt{\frac{2z}{i}}\theta(z).$$

The general case follows by analytic continuation. ■

Before continuing the following argument, we first introduce the modular form of higher level.

Definition 3.3

For $N \in \mathbb{Z}_{\geq 1}$ we define following subgroup of $SL(2,\mathbb{Z})$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \middle| c \equiv 0 \mod N \right\}.$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \middle| a, d \equiv 1 \mod N \right\}.$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \middle| b \equiv 0 \mod N \right\}.$$

*A subgroup $\Gamma \subset SL(2,\mathbb{Z})$ is called **congruence subgroup** if there exists a N with $\Gamma(N) \subset \Gamma$, the smallest sub N is called the **level of** Γ.*

We have:

$$\Gamma(1) = \Gamma_1(1) = \Gamma_0(1) = SL(2,\mathbb{Z})$$

So if Γ is a congruence subgroup then it must be $SL(2,\mathbb{Z})$, hence $SL(2,\mathbb{Z})$ is the only congruence subgroup of level 1.

Corollary 3.2 (*of 3.1*)

$\theta(z)$ is Jacobi theta function,

$$\theta(z)^4 \in M_2(\Gamma_0(4)).$$

Proof: (To be supplied: A First Course in Modular form, Definition 1.2.3)

The generators of $\Gamma_0(4)$ are T and $(1, 0; 4, 1)$, so it's enough to verify the transformation property on them, by 3.1. ■

So we can say, $\theta(z)$ is a modular form of "weight 1/2" on $\Gamma_0(4)$, . (The modular form of half weight has not been defined yet, we interpret it as a function satisfying modular transformation).

The modular transformation property of $\theta(z)$ indicate a subgroup of $SL(2,\mathbb{R})$ (similar to S, T generated $SL(2,\mathbb{Z})$).We introduce the "higher level" modular form, modular forms on **congruence subgroup** .

Furthermore than congruence subgroup we have the larger group

$$\Gamma_0^+(N) := \langle \Gamma_0(N), W_N \rangle = \Gamma_0(N) \cup \Gamma_0(N) W_N.$$

where W_N is called Fricke involution.

Definition 3.4 (*Fricke involution*)

$$W_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \in SL(2,\mathbb{R})$$

*is called **Fricke involution**.*

W_N has order 2 (in meaning of $PSL(2,\mathbb{R})$), and is a nomalizer of $\Gamma_0(N)$, i.e. $W_N\Gamma_0(N) = \Gamma_0(N)W_N$, which explains the second equal above.

(rf. Topics in classical automorphic forms (Henryk Iwaniec) P112)

In general T and W_N generate a subgroup of (?)$\Gamma_0(N)$ of infinite index. So to check the modularity in $\Gamma_0(N)$, it does not suffice to verify just on T and W_N.

But for $N = 4$, they can generate the full group $\Gamma_0(4)$. (this is only sufficient condition, the group generated by T and W_N is obviously out of $SL(2,\mathbb{Z})$)

Proposition 3.3

$-Id$, T and W_N can generate congruence subgroup $\Gamma_0(4)$. (that is, T and W_N can generate $\Gamma_0(4)$'s image in $PSL(2,\mathbb{Z})$).

Specially, $\Gamma_0(4) = \left\langle -Id, T, \tilde{T} \right\rangle$

Proof: It is sufficient to show that $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\tilde{T} := W_N T^{-1} (W_N)^{-1} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$ generates $\Gamma_0(4)$.

For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$, we apply right action $T^{\pm 1}$, $\tilde{T}^{\pm 1}$ on γ. We find under the right action, it is invariant that $c \equiv 0 \pmod 4$ and $ad - bc = 1$. Thus a is odd under the action.

$$T^{\pm 1} : (a, b) \mapsto (a, b \pm a),$$

$$\tilde{T}^{\pm 1} : (a, b) \mapsto (a \pm 4b, b).$$

By applying these to action, we decease the absolute value of a and b respectively. In detail, $|a| < 2|b|$ iff $b^2 > (b \pm a)^2$, so apply $T^{\pm 1}$, or $|a| > 2|b|$ iff $a^2 > (a \pm 4b)^2$ just apply $\tilde{T}^{\pm 1}$. Finally we get $(\hat{a}, \hat{b}) = (\pm 1, 0)$, and implies $\hat{\gamma} = Id$. So γ can be written as words of T and $\tilde{T}$. ■

So when $N = 4$ we can check modularity on $\Gamma_0(4)$ of a given function just on $z \mapsto z + 1$ and $z \mapsto -1/4z$

Now, by the principle "a finite number of q-coefficients suffice" formulated at the end of Section 1, the mere fact that $\theta(z)$ is a modular form is already enough to let one prove non-trivial identities. And indeed, with almost no effort we obtain proofs of two of the most famous results of number theory of the 17th and 18th centuries, the theorems of Fermat and Lagrange about sums of squares.

♣ Sum of Two and Four Squares

Let $r_2(n)$ be the number of representation of positive integer n as sum of two squares, that is:

$$r_2(n) = \#\{(a, b) \in \mathbb{Z}^2 | a^2 + b^2 = n\}.$$

Using theta series, we get generate function of $r_2(n)$

$$\sum_{n \geq 0} r_2(n) q^n = \theta(z)^2. \tag{41}$$

To solve the problem of sum of two squares, we need investigate the property of $\theta(z)^2$. Before that, we introduce Dirichlet character first. Because the weight may be no longer even, it is worth considering the sign of our transformation.

Definition 3.5 (*Dirichlet character modulo N*)

If there is a homomorphism

$$\hat{\chi} : (\mathbb{Z}/N\mathbb{Z})^* \mapsto \mathbb{C}^*$$

extend it to

$$\chi : \mathbb{Z} \mapsto \mathbb{C}.$$

by setting $\chi(n)$ equal to $\hat{\chi}(n \pmod N)$ if $(n, N) = 1$ and equal to 0 otherwise. χ is called ***Dirichlet character modulo*** *N.*

Because of homomorphism, $\chi((-1)(-1)) = \chi(1) = 1$, so $\chi(-1)^2 = 1$.Moreover, because of finite order of $(\mathbb{Z}/N\mathbb{Z})^*$ for $n \in (\mathbb{Z}/N\mathbb{Z})^*$, $\chi(n)$ must be a unity root.

Use Dirichlet character we can extend the definition of modular form,as follows:

Definition 3.6 (*?*)

If χ is a non-trivial Dirichlet character and k is a positive integer with $\chi(-1) = (-1)^k$, then

$$\mathbb{G}_{k,\chi}(z) = c_k(\chi) + \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi(d) d^{k-1} \right) q^n. \tag{42}$$

is Fourier series of an Eisentstein series which is a modular form of weight k and character χ on $\Gamma_0(N)$. Here $c_k(\chi) \in \overline{\mathbb{Q}}$ is a constant, given by $c_k(\chi) = \frac{1}{2}L(1-k,\chi)$, $L(s,\chi)$ is the analytic continuation of Dirichlet series $\sum_{n=1}^{\infty}$.

The modular form of weight k and character χ means

$$\mathbb{G}_{k,\chi}(\frac{az+b}{cz+d}) = \chi(a)(cz+d)\mathbb{G}_{k,\chi}(z) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4).$$

Here is a simple example. For $N = 4$, Dirichlet character modulo 4 is

$$\chi_{-4}(n) = \begin{cases} +1, n \equiv 1 \pmod 4 \\ -1, n \equiv 3 \pmod 4 \\ 0, n \text{ is even} \end{cases} \tag{43}$$

and here $k = 1$, so we can get a modular form:

$$\mathbb{G}_{1,\chi_{-4}}(z) = c_1(\chi_{-4}) + \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_{-4}(d) d^{k-1} \right) q^n = \frac{1}{4} + q + q^2 + q^4 + 2q^5 + q^8 + ...$$

of weight 1 and character χ_{-4} on $\Gamma_0(4)$.

Proposition 3.4

The function $\theta(z)^2$ is a modular form of weight 1 and character χ_{-4} on $\Gamma_0(4)$.

Proof: For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$, We want to prove that

$$\theta(\gamma z)^2 = \chi_{-4}(a)(cz+d)\theta(z)^2$$

We claim that a is odd and:

$$\gamma \in -Id < T, \tilde{T} > \iff a \equiv 3 \pmod 4, \quad \gamma \in < T, \tilde{T} >, \iff a \equiv 1 \pmod 4$$

Since $ad - bc = 1$ and $4|c$, so a must be odd. And because $a \pmod 4$ is invariant under the right multiple of T and $\tilde{T}$ and by 3.3, we proved the claim.

Now verify the modularity. By 3.1 we know that $\forall \gamma \in < T, \tilde{T} >$:

$$\theta(\gamma z)^2 = (cz+d)\theta(z)^2.$$

This equation agree with what we want, since $\chi_{-4}(a) = 1$ when $a \equiv 1 \pmod 4$.

If $\hat{\gamma} \in -Id < T, \tilde{T} >$ and $\hat{\gamma} = -Id\gamma = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$,

$$\theta(\hat{\gamma} \cdot z) = \theta(-Id\gamma \cdot z)^2 = (cz+d)\theta(-Idz)^2 = (-1)(-cz-d)\theta(z)^2,$$

agree with that $\chi_{-4}(a) = -1$ when $a \equiv 3 \pmod 4$. ■

Now we find that both $\mathbb{G}_{1,\chi_{-4}}$ and $\theta(z)^2$ are modular form of weight 1 and character χ_{-4}. By 1.10, we can calculate upper bound of $M_1(\Gamma_0(4)$.

$$V = Vol(\Gamma_0(4) \setminus \mathfrak{H}) = \frac{\pi}{3} \times [SL(2,\mathbb{Z}) : \Gamma_0(4)] = 2\pi.$$

$$dim(M_1(\Gamma_0(4)) \leq \frac{1 \times V}{4\pi} + 1 = \frac{3}{2}.$$

So $\mathbb{G}_{1,\chi_{-4}}$ and $\theta(z)^2$ must be proportional,

$$\theta(z)^2 = 4\mathbb{G}_{1,\chi_{-4}}.$$

We obtained:

Proposition 3.5 (*Represent number of sum of two squares*)

Let n be a positive integer. Then

$$r_2(n) = 4 \sum_{d|n, 2\nmid d} \chi_{-4}(d) = 4 \sum_{d|n, 2\nmid d} (-1)^{\frac{d-1}{2}} \tag{44}$$

Corollary 3.6 (*Theorem of Fermat*)

Every prime number $p \equiv 1 \pmod 4$ is a sum of two squares.

We can use same method to other powers of θ. Particularly, we can get $r_4(n)$ by considering $\theta(z)^4$, which is a modular form of weight 2 on $\Gamma_0(4)$. What we need to do is to find a base for $M_2(\Gamma_0(4))$.

Proposition 3.7 (*Represent number of sum of four squares*)

Let n be a positive integer. Then

$$r_4(n) = 8 \sum_{d|n, 4\nmid d} d = \sigma_1(n) - 4\sigma_1(\frac{n}{4}). \tag{45}$$

Here when $n/4$ is not an integer $\sigma_1(\frac{n}{4}) = 0$.

Proof: Firstly, by proposition 1.10, we know that $dim(M_2(\Gamma_0(4)) \leq 2$.

We have got the Eisenstein series of weight 2, $G_2(z)$, which is a quasimodular form on $SL(2,\mathbb{Z})$, and corresponding almost holomorphic modular form $G_2^*(z) = G_2(z) - \frac{\pi}{2y}$. We try to build base for $M_2(\Gamma_0(4))$ by $G_2(z)$.

$G_2^*(z)$ is not holomorphic because of it's non-holomorphic part $\frac{pi}{2y}$. Thus $G_2^*(z) \notin M_2(\Gamma_0(4)$ itself. For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$. By modularity of $G_2^*(z)$ in $SL(2,\mathbb{Z})$ and that $\begin{pmatrix} a & 2b \\ c/2 & d \end{pmatrix} \in \Gamma_0(4)$, we get:

$$G_2^*(2 \cdot \frac{az+b}{cz+d}) = G_2^*(\frac{a \cdot 2z + 2b}{\frac{c}{2} \cdot 2z + d}) = (cz+d)^2 G_2^*(2z).$$

So $G_2^*(2z)$ have modularity. Thus

$$G_2^*(z) - 2G_2^*(2z) \in M_2(\Gamma_0(4)).$$

(it is holomorphic because the $\pi/2y$ part have been canceled out.

In similar way,

$$G_2^*(2z) - 2G_2^*(4z) \in M_2(\Gamma_0(4)).$$

By comparing the q-series of $G_2^*(z) - 2G_2^*(2z)$ and $G_2^*(2z) - 2G_2^*(4z)$, we know that they're linear independent. So they are a set of basis of $M_2(\Gamma_0(4)$. For simplicity, replace $G_2^*(z)$ with

$$\mathbb{G}_2^*(z) = -\frac{1}{4\pi} G_2^*(z) = -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

and

$$\mathbb{G}_2^*(z) - 2\mathbb{G}_2^*(2z) = \frac{1}{24} + \sum_{n=1}^{\infty} q^n - 2\sum_{n=1}^{\infty} q^{2n}.$$

$$\mathbb{G}_2^*(2z) - 2\mathbb{G}_2^*(4z) = \frac{1}{24} + \sum_{n=1}^{\infty} q^{2n} - 2\sum_{n=1}^{\infty} q^{4n}.$$

$\theta(z)^4 = 1 + 8q + 24q^2 + ...$ By the first two terms of $\theta(z)^4$, we have:

$$\theta(z)^4 = 8(\mathbb{G}_2^*(z) - 2\mathbb{G}_2^*(2z)) + 16(\mathbb{G}_2^*(2z) - 2\mathbb{G}_2^*(4z)) = 1 + 8\left[\sum_{n=1}^{\infty} q^n - 4\sum_{n=1}^{\infty} q^{4n}\right]. \tag{46}$$

■

Corollary 3.8 (*Theorem of Lagrange*)

Every positive integer is a sum of four squares.

(To be added: variant of theta function)

♣ The Kac-Wakimoto Conjecture

3.2 Theta Series in Many Varibles

We now consider quadratic form in an arbitrary number m of variables.

Definition 3.7 (*Theta series in m varibles*)

Let $Q : \mathbb{Z}^m \mapsto \mathbb{Z}$ to be a positive definite quadratic form. We associate to Q the theta series

$$\Theta_Q(z) = \sum x_1, ..., x_m \in \mathbb{Z} q^{Q(x_1,...,x_m)} = \sum_{n=0}^{\infty} R_Q(n) q^n, \tag{47}$$

where $q = e^{2\pi iz}$ and $R_Q(n)$ denotes the number of representations of n by Q.

Proposition 3.9

Θ_Q is always a modular form of weight $m/2$.

We can write $Q(x)$ uniquely as

$$Q(x) = \frac{1}{2} x^t A x = \frac{1}{2} \sum_{i,j=1}^{m} a_{ij} x_i x_j, \tag{48}$$

where $A = (a_{ij})$ is a symmetric $m \times m$ matrix.

The integrality of Q is equivalent to that A has integral element and its diagonal elements a_{ii} are even. Such matrix is called **even integral matrix**. And A is positive definite, since $Q(x)$ is. So A is also non-singular, and $A^{-1} \in M_m(\mathbb{Q})$. The **level** of Q is defined as the smallest positive integer $N = N_Q$ such that NA^{-1} is again an even integral matrix. The **discriminant** $\Delta = \Delta_Q$ of A is defined as $\Delta = (-1)^m \det(A)$.

Proposition 3.10

Let Δ be discriminant of positive definite quadratic form $Q : \mathbb{Z}^m \mapsto \mathbb{Z}$, then

$$\Delta \equiv 0, 1 \pmod 4.$$

Proof: (?) ■

So the discriminant of A is associated to Kronecker symbol $\chi_\Delta(n) = (\frac{\Delta}{n})$.

Definition 3.8 (*Kronecker symbol*)

*Let $D \equiv 0, 1 \pmod 4$. Define function for $n \in \mathbb{Z}$ $(\frac{D}{n})$, which is called **Kronecker symbol**, to be :*

1. *When $(D, n) > 1$, $(\frac{D}{n}) = 0$.*
2. *$(\frac{D}{1}) = 1$.*
3. *When D odd, $(\frac{D}{2}) = (\frac{2}{|D|})$, the latter is **Jacobi symbol**.*
4. *When $n = p_1...p_r$, p_i is prime, $(\frac{D}{n}) = (\frac{D}{p_1})...(\frac{D}{p_r})$, where $(\frac{D}{p_i})$ is Legendre symbol when p_i is odd.*

And the relation between Kronecker symbol and Dirichlet character is:

Proposition 3.11

Kronecker symbol is the unique Dirichlet character modulo N satisfying

$$\chi_\Delta(p) = (\frac{\Delta}{p}) \quad \textit{(Legendre symbol)}$$

for any odd prime $p \nmid N$.

Now we can have precise description of the modular behavior of Θ_q for $m \in 2\mathbb{Z}$, which is :

Theorem 3.1 (*Hecke, Schoenberg*)

Let $Q : \mathbb{Z}^{2k} \mapsto \mathbb{Z}$ be a positive definite integer-valued form in $2k$ varibles of level N and discriminant Δ. Then Θ_Q is a modular form on $\Gamma_0(N)$ of weight k and character χ_Δ. i.e.

$$\Theta_Q(\frac{az+b}{cz+d}) = \chi_\Delta(a)(cz+d)^k\Theta_Q(z) \quad \forall z \in \mathfrak{H}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{49}$$

There is another language for quadratic forms which is often more convenient – the language of Lattice.

The lattice Λ is a free $\mathbb{Z}$-module of rank m. And **the quadratic form** Q is a function from Λ to $\mathbb{Z}$, such that (1) the associated scalar product

$$(x, y) := Q(x + y) - Q(x) - Q(y) \quad (x, y \in \Lambda)$$

is Z-bilinear. (2)

$$Q(rx) = r^2Q(x) \quad \forall r \in \mathbb{Z}, \forall x \in \Lambda$$

For a quadratic form $Q(x)$ on lattice, we can always choose a Z-basis $\{w_i\}_{i=1}^m \subset \mathbb{R}^m$ of Λ (The basis is determined by $Q(x)$ itself.). Then Q can be described by symmetric matrix A as before: for $x \in \Lambda$, whose coordinate is $t \in \mathbb{Z}^m$ under the basis, we have $Q(x) = \frac{1}{2}t^TAt$. This means, by choosing a basis of lattice, we turn the domain from lattice Λ back to $\mathbb{Z}^m$. Here we can solve the basis by A through the relation $(w_i, w_j) = a_{ij}$, which means A is Gram matrix for basis $\{w_i\}$. The scalar product is given by $(x, y) = x^TAy$.

However, the basis-free language is more convenient. To reach this goal, we first define a scalar product on Λ. We have length function on lattice λ to be

$$||x||^2 = (x, x) \quad \forall x \in \Lambda,$$

and define

$$Q(x) = \frac{1}{2}||x||^2.$$

So the **integer-value property of $Q(x)$ in $\mathbb{Z}^m$** corresponds to the requirement that **lattice in which all vectors have even length** (which is equivalent to that A is even integral (can verify by law of cosines when $m = 2$)) , then we say the lattice is **even**.

Now we can formulate a diagram to illustrate the relation between quadratic form on lattice $Q(x)$, even integral matrix A and even length metric $||\cdot||$ on lattice.

Define the **covolume** $\mathrm{Vol}(\mathbb{R}^m/\Lambda)$ of a lattice Λ to be the volume of its fundamental domain, which is computed by $\det[e_1...e_m]$ for an oriented basis $\{e_1, ..., e_m\}$, (and when $m = 2$ define its **discriminant** to be $D = -4covol(\Lambda)^2$.) We have

Proposition 3.12

$$\sqrt{detA} = Vol(\mathbb{R}^m/\Lambda) \tag{50}$$

Proof: A is Gram matrix of basis $\{e_i\}$, $a_{ij} = (e_i, e_j)$. Let B be matrix $(e_1, ..., e_m)$, then $A = B^tB$. Thus $\mathrm{Vol}(\mathbb{R}^m/\Lambda) = \det B = \sqrt{\det A}$. ■

There is a spacial case when the volume of the lattice is 1.

Definition 3.9 (*unimodular*)

When $Vol(\mathbb{R}^m/\Lambda) = 1$ (i.e. when $\Lambda \in \mathbb{R}^m$ has the same covolume as $\mathbb{Z}^m$) the lattice is called ***unimodular***

♣ Invariant of Even Unimodular Lattice

For the sake of clarity, we recall the definition of even unimodular lattice. A lattice is unimodular means its determinant is 1 or -1 (in our cases of positive definite form, it must be 1). A lattice is even means for any vectors in it, they have even length.

If the matrix A of a positive definite quadratic form Q is even integral and unimodular. Then by Theorem 3.1, Θ_Q is a modular form on Γ_0 (full modular group) of weight k and character $\chi_1 = 1$. The reason why Θ_Q is on full modular group is not trivial, we have

Proposition 3.13

The even unimodular quadratic form of even rank has level 1.

Proof: What we need to prove is: For an even matrix (integral symmetric matrix with even diagonal elements) of even rank, with determinant 1, its inverse is also a matrix like this. That is, if $A \in SL(n,\mathbb{Z})^{even} := \{M \in SL(n,\mathbb{Z}) | 2 \mid m_{ii} \forall 1 \leq i \leq n\}$, then $A^{-1} \in SL(n,\mathbb{Z})^{even}$.

Claim: If M is even matrix with **odd** rank, then $\det A$ is even.

Proof of Claim: Assume $M = (m_{ij})$ is a $k \times k$ matrix, k is odd. Then for every $i = 1, ..., k$

$$\det M = \sum_{j=1}^{k} m_{ij} A_{ij};$$

summing these equalities, we obtain:

$$k \det M = \sum_{i=1}^{k} m_{ii} A_{ii} + 2 \sum_{1 \leq i < j \leq k} m_{ij} A_{ij}.$$

Since $m_{ii} \quad (i \leq 1 \leq k)$ are even, it follows that $k\det M$ is divisible by 2, and hence so is $\det M$.

Another proof: by combinatorial definition of determinant. Notice that in a Derangement of odd numbers, there is no element of order 2. Thus, the item which doesn't contain diagonal element must has coefficient 2. Hence the determinant is divisible by 2.

For $A \in SL(n,\mathbb{Z})^{even}$, each diagonal element of A^* is determinant of even matrix with odd rank, thus A^* is even matrix by Claim. Then by $A^{-1} = (\det A)^{-1} \cdot A^*$ we get: $A^{-1} \in SL(n,\mathbb{Z})^{even}$ for n even. ■

Corollary 3.14

If Q is a quadratic form of rank $2k$ which is even and unimodular, then the theta series associated to Q is a moudular form on Γ_1.

Proof: By Proposition 3.13 we know Q has level 1, and by Theorem 3.1, we have $\Theta_Q \in M_k(\Gamma_0(1)) = M_k(SL(2,\mathbb{Z}))$. ■

Now we can reach the important consequence.

Proposition 3.15

Let $Q : \mathbb{Z}^m \to \mathbb{Z}$ be a positive definite even unimodular quadratic form in m variables. Then

(i) the rank m is divisible by 8 ,and

(ii) the number of representation of $n \in \mathbb{N}$ by Q is given for large n by the formula

$$R_Q(n) = -\frac{2k}{B_k}\sigma_{k-1}(n) + O(n^{k/2}) \quad (n \to \infty), \tag{51}$$

where $k = \frac{m}{2}$ and B_k denotes the kth Bernoulli number.

Proof: First prove that if the rank $m = 2k$ with k even, then $4|k$.

By corollary above, $\Theta_Q \in M_k(\Gamma_1)$. Thus by 2.14

$$\Theta_Q = a \cdot \mathbb{G}_k(z) + b \cdot C_k(z),$$

where $\mathbb{G}_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ and C_k are Eisenstein series and cusp form of weight k respectively.

Since $\Theta_Q = \sum_{n=0}^{\infty} R_Q(n)q^n$ and the $R_Q(0) = 1$ (because the only vector such that $Q(x) = 0$ is 0.), we get $a = -\frac{2k}{B_k}$ (B_k is the kth Bernoulli number.)

$C_k(z)$ is a cusp form. So we use Proposition 2.15 and get the asymptotic formula in (ii).

If $k \equiv 2 \pmod 4$ then B_k is positive. We have

$$\frac{R_Q(n)}{n^{k/2}} = -\frac{2k}{B_k}\frac{\sigma_{k-1}(n)}{n^{k/2}} + O(1) \to -\infty \quad (n \to \infty, k > 2)$$

When $k = 2$, we have

$$\limsup_{n\to\infty} \frac{\sigma_1(n)}{n} = +\infty \quad (\frac{\sigma_1(k!)}{k!} \geq 1 + 1/2 + ... + 1/k).$$

Thus

$$\liminf_{n\to\infty} \frac{R_Q(n)}{n^{k/2}} = -\infty.$$

Contradict to $R_Q(n) \geq 0$, hence $4|n$.

Consider other cases. If Q has odd rank m satisfying the condition, then $Q \oplus Q \oplus Q \oplus Q$ also satisfies condition, because the matrix of $Q \oplus Q \oplus Q \oplus Q$ is $diag(A, A, A, A)$ which is positive definite, even and unimodular. However its rank is $4m$, m odd, wich contradict to our conclusion above. If rank of Q is a twice odd number, then consider $Q \oplus Q$. ■

Next we introduce a important example: Λ_8 lattice.

Definition 3.10 (Λ_8 *root system*)

The Λ_8 root system is a subset of $\mathbb{R}^8$, such that

(i) each vector has coordinates all in $\mathbb{Z}$ or all in $\mathbb{Z} + \frac{1}{2}$,

(ii) the sum of coordinate of every vector is an even integer,

(iii) the sum of square of coordinate is 2.

which is:

$$\{(x_i) \in \mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8 : \sum_i x_i \equiv 0 \pmod 2, \sum_i x_i^2 = 2\} \tag{52}$$

There are 112 integer vectors in Λ_8 root system, while 128 half integer vectors. Thus Λ_8 has 240 roots in total.

Definition 3.11 (Λ_8 *lattice*)

E_8 is the $\mathbb{Z}$-submodule of $\mathbb{R}^8$ generated by E_8 root system. Which means E_8 is the root lattice of the root system.

Proposition 3.16 (*property of E_8*)

(1) Λ_8 is a integral lattice. (2) Λ_8 is unimoudular. (3) Λ_8 is even.

Proof: (1) Λ_8 integral means scalar product of any two vectors in the lattice is integer. The case when two vector are both integer is trivial. For $x, y \in \Lambda_8$,

$$(x, y) = \sum_{i=1}^{8}(x_i + \frac{1}{2})y_i = \sum_{i=1}^{8} x_i y_i + \frac{1}{2}\sum_{i=1}^{8} y_i \in \mathbb{Z},$$

or

$$(x, y) = \sum_{i=1}^{8}(x_i + \frac{1}{2})(y_i + \frac{1}{2}) = \sum_{i=1}^{8} x_i y_i + \frac{1}{2}\sum_{i=1}^{8} x_i + \frac{1}{2}\sum_{i=1}^{8} y_i + 2 \in \mathbb{Z}.$$

(2)For any $v \in \mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8$, its sum of coordinate is either even or odd. Thus,

$$\mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8 = \Lambda_8 \cup (\Lambda_8 + e_1).$$

and $|\mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8 : \Lambda_8| = 2$.

$$\mathrm{Vol}(\mathbb{R}^8/\Lambda_8) = \mathrm{Vol}[\mathbb{R}^8/(\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8)] \cdot |\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8 : \Lambda_8|$$

Now we only need to calculate $\mathrm{Vol}(\mathbb{R}^8/(\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8))$. What we know is that $|\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8) : \mathbb{Z}^8| = 2$, for the two representation of coset are 0 and $\frac{1}{2}(e_1 + ... + e_8)$

$$1 = \mathrm{Vol}(\mathbb{R}^8/\mathbb{Z}^8) = \mathrm{Vol}[\mathbb{R}^8/(\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8)] \cdot |\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8) : \mathbb{Z}^8|.$$

Thus, $\mathrm{Vol}[\mathbb{R}^8/(\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8)] = \frac{1}{2}$, and we get: $\mathrm{Vol}(\mathbb{R}^8/\Lambda_8) = 1$.

(3)For x_i integer $x_i^2 \equiv x_i \pmod 2$, while for x_i half integer $x_i^2 \equiv \frac{1}{4} \pmod 2$. Thus $||x|| = \sum_{i=1}^8 x_i^2 \equiv 0 \pmod 2$. ■

remark 26

Warning: $\{\frac{1}{2}e_i\}$ is not a basis of $\mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8$.

We can choose $\mathbb{Z}$-Basis $u_i = e_i - e_{i+1} (1 \le i \le 6)$, $u_7 = e_6 + e_7$, $u_8 = -\frac{1}{2}(e_1 + ... + e_8)$ of E_8, then every u_i has length 2 and (u_i, u_j) equals -1 or 0 for $i \neq j$. Precisely, (u_i, u_j) depend on E_8 **Dynkin diagram**, which equals to -1 if ith and jth vertices of the diagram are adjacent, and 0 if not.

Since E_8 is even unimodular lattice, the theta series of E_8 is a modular form of weight 4 on $SL(2,\mathbb{Z})$, whose Fourier series begins with 1. Thus it must be $E_4(z) = 1 - \frac{2\cdot 4}{B_4}\mathbb{G}_4(z) = 1 + 240q + 2160q^2 + ...$ Then $R_{Q[E_8]}(n) = 240\sigma_3(n)$, so for every $n \ge 1$ there are $240\sigma_3(n)$ vectors x in E_8 lattice such that $(x, x) = 2n$.

From $dim(M_4(\Gamma_1)) = 1$, we know that $R_Q(n) = 240\sigma_3(n)$ for any even unimodular quadratic form of rank 8. We will see soon that same theta series may not correspond to isomorphic lattice. And the uniqueness of theta series on rank 8 even unimodular lattice is not surprising because we know:

Proposition 3.17 (*Classification on rank 8 even unimodular lattice*)

E_8 is the only even unimodular lattice of rank 8 up to isomorphism.

In rank 16 there are two non-equivalent lattice: $E_8 \oplus E_8$ and Λ_{16} (Barnes-Wall lattice) which is not decomposable. Since the theta series of both lattices are modular form of weight 8 on $SL(2,\mathbb{Z})$, with Fourier series beginning with 1, they both equal to $E_8(z)$. So $r_{E_8\oplus E_8}(n) = r_{\Lambda_{16}}(n)$ for $n \ge 1$, **even though the two lattice are distinct.** (Their distinctness, and a great deal of further information about the relative positions of vectors of various lengths in these or in any other lattices, can be obtained by using the theory of Jacobi forms which was mentioned briefly in section 3.1 rather than just the theory of modular forms.)

In rank 24 we don't have uniqueness of theta series, because $dim M_{12}(\Gamma_1) = 2$. The even unimodular lattices of this rank were classified completely by Niemeyer in 1973. There are exactly 24 of them up to isomorphism. *There is one special one, Λ = the Leech lattice, discovered by John Leech in the mid 1960s in his study of sphere packings. It has minimum norm 4 whereas the others have minimum norm 2. The number of minimal vectors is 196560. The Leech lattice has very large automorphism group and closely related to the monster group and other sporadic simple groups. Additionally, each Niemeier lattice can be constructed from its root lattice (except for the Leech lattice which has no roots)* Some (but not all) of them have the same theta series and hence same number of vectors of any given length. (an obvious example of such pair being $E_8 \oplus E_8 \oplus E_8$ and $E_8 \oplus \Lambda_1 6$, corresponding to theta series $E_4(z) \cdot E_8(z)$). (rf. Sphere Packings, Lattices and Groups (J.H.Conway, N.J.A.Sloane), Chapter 16)

The theta series of Leech lattice is the unique modular form with Fourier expansion starting $1 + 0q + ...$ in other rank 24 even unimodular lattices. Thus it must be :

$$\Theta_{Leech}(z) = E_{12} - \frac{65520}{691}\Delta(z) = 1 + \frac{65520}{691}\sum_{n=1}^{\infty}(\sigma_{11}(n) - \tau(n))q^n = 1 + 196560q^2 + 1677312q^3 + ... \quad (53)$$

where $\Delta(z)$ is the discriminant function that is a modular form of weight 12 on $SL(2,\mathbb{Z})$. And we get $R_{Leech}(n) = \frac{65520}{691}(\sigma_{11}(n) - \tau(n))$ for $n \ge 1$. This gives a prove of Ramanujan's congruence 2.17 since $R_{Leech}(n)$ must be a integer number.

In rank 32 things become more interesting. The complete classification is not known, but we know there are more than 8×10^7 isomorphism classes. This is (as you can gauss) is also a consequence of theory of modular forms, but a far more sophisticated part. There is a fundamental theorem of Siegel:

Theorem 3.2 (*Siegel*)

The average value of the theta series associated to the quadratic forms in a single genus is always an Eisenstein series.

Specialized to case of even unimodular forms of rank $m = 2k \equiv \pmod 8$ (which forms a single genus). This theorem also says that there are only finitely many such forms up to equivalence for each k, denoting them by $Q_1, ..., Q_I$ We have relation

$$\sum_{i=1}^{I} \frac{1}{w_i} \Theta_{Q_i}(z) = \mathsf{m}_k E_l(z), \tag{54}$$

where w_i is the number fo automorphisms of the form Q_i (i.e. the number of matrices $\gamma \in SL(m, \mathbb{Z})$ such that $Q_i(\gamma x) = Q_i(x)$ for all $x \in \mathbb{Z}^m$). And m_k is give by

$$\mathsf{m}_k = \frac{B_k}{2k} \frac{B_2}{4} ... \frac{B_{2k-2}}{4k-4},$$

where B_i denotes the ith Bernoulli number.

By comparing the constant terms of equation above, we have

$$\sum_{i=1}^{I} \frac{1}{w_i} = \mathsf{m}_k. \tag{55}$$

which is called **Minkovski-Siegel mass formula**.

Some value of m_k are: $m_4 \approx 1.44 \times 10^{-9}$, $m_8 \approx 2.49 \times 10^{-18}$, $m_{12} \approx 7.49 \times 10^{-15}$ are small, but $m_{16} \approx 4.03 \times 10^7$. Since $w_i \geq 2$ for every i ($\pm Id$ are certainly automorphisms of quadratic form). So when consider classification of rank 32 even unimodular lattice, we have $|I| \times \frac{1}{2} \geq \sum_{i \in I} \frac{1}{w_i} = \mathsf{m}_{16}$, so $|I| > 8 \times 10^7$.

A further consequence of the fact that $\Theta_Q \in M_k(\Gamma_1)$ for Q even and unimodular of rank $m = 2k$ is:

Proposition 3.18

If quadratic form Q is even and unimodular of rank $m = 2k$, then the minimal value of $Q(x)$ for non-zero $x \in \Lambda$ is bounded by $r = dim M_k(\Gamma_1) = [k/12] + 1$. (So $r = dim M_k(\Gamma_1)$ is the upper bound of minimal value of $Q(x)$ for any proper lattice of rank $2k$.)

*The lattice is called **extremal** if this bound is attained, that is, the minimal value of $Q(x)$ is exactly r.*

Proof: (don't know yet) ■

Definition 3.12 (*Extermality via modular forms*)

Let M be a subspace of $M_k(\Gamma_0(l)))$ (we know that the theta series Θ_L of even lattice L is in $M_k(\Gamma_0(l)))$.

M is extremal if: the projection $M \to \mathbb{C}^d$ from $f \in M$ to its first $d = dim M$ coefficients of q-expansion is injective. Precisely:

$$f = \sum_{n \geq 0} a_n q^n \mapsto (a_0, ..., a_{d-1})$$

is injective.

The inverse image of $(1, 0, ..., 0)$ which is

$$F_M = 1 + \sum_{n \geq d} a_n q^n$$

is then called the extremal modular form in M.

remark 27

The conception "extremal" comes from Coding Theory, refer to Sphere Packings, Lattices and

Groups (J.H.Conway, N.J.A.Sloane), Chapter 7).

Consider the lattice of rank 8 and 16, we have $r = 1$. For the case E_8, any element from its root system has length 2, and E_8 is generated by element in root system, so the minimal value of $Q(x)$ is 1. For $E_8 \oplus E_8$, its generate matrix is $diag(A, A)$, where A is generate matrix of E_8, whose column vectors in $\mathbb{Z}^8 \cup (Z + \frac{1}{2})^8$ and have length 2. Thus the column vectors of $diag(A, A)$ also have length 2. Minimal value of $Q(x)$ is also 1.

For Λ_{16}, $\Theta_{\Lambda_{16}}(z) = 1 + 4320q^2 + 61440q^3 + ...$ thus the minimal value of $Q(x)$ is 1.(rf. Sphere Packings, Lattices and Groups (J.H.Conway, N.J.A.Sloane), Section 4.10)

For rank 24 we have $r = 2$. By what we state above, the only extremal lattice is the Leech lattice.

Extremal unimodular lattices are also known to exist for $m = 32, 40, 48, 56, 64$ and 80, while the case $m = 72$ is open. However, for rank large enough there is no extremal even unimodular lattice.

Theorem 3.3 (*Mallow-Odlyzko-Sloane*)

There are only finitely many non-isomorphic extremal even unimodular lattices.

Proof (sketch) : By Theorem 3.2, there are only finite equivalent classes of even unimodular lattice of given any rank. So we only need to prove there is a upper bound on the value of rank for lattice to be extremal even unimodular.

By argument (don't know yet), we find the extremal theta series has the form:

$$f_n(z) = 1 + na_n q^{n+1} + \left(\frac{nb_n}{2} - 24n(n+31)a_n\right) q^{n+2} + ... \tag{56}$$

where a_n and b_n are coefficients of $\Delta(z)^n$ in the modular function $j(z) = \frac{E_4(z)^3}{\Delta(z)}$ and $j(z)^2$, respectively, when these are expressed as Laurent series in the modular form $\Delta(z) = q - 24q^2 + 252q^3 - ...$ It is not hard to show that

$$a_n \sim An^{-3/2}C^n$$

for some constant $A = 225153.793389...$ and $C = 1/\Delta(z_0) = 69.1164201716...$, where $z_0 = 0.52352170017992...i$ is the unique zero on the imaginary axis of the function $E_2(z)$ (This is because $E_2(z)$ is the logarithmic derivative of $\Delta(z)$),

$$b_n \sim 2\lambda An^{-3/2}C^n.$$

$\lambda = j(z_0) - 720 = 163067.793145...$

It follow that the coefficient of q^{n+2} in f_n, $\left(\frac{nb_n}{2} - 24n(n+31)a_n\right) \sim AC^n n^{-1/2}(\lambda - 24(n+31)$ is negative for n large enough (roughly larger than 6800, corresponding to m roughly larger than 16300). The negative coefficient contradict to the definition of theta series, hence extremal lattices of rank large this cannot exist. ■

(reference on coding theory: Lattices and Codes (Wolfgang Ebeling))

(Property of extremal theta series: Sphere Packings, Lattices and Groups (J.H.Conway, N.J.A.Sloane), Section 7.7 Theorem 20)

♣ Drums Whose Shape One Cannot Hear

Marc Kac asked a famous question "Can one hear the shape of a drum?". Can there be two Riamannian manifolds with fixed boundary which are not isomorphic but have the same spectra of eigenvalues(Dirichlet eigenvalues) of their Laplace operator?

Isospectral Drums of 16-dimension by Milnor : We know that the two even unimodular lattice of rank 16 $\Lambda_8 \oplus \Lambda_8$ and Λ_{16} are not isomorphic, hence two Riemannian manifolds $M_1 = \mathbb{R}^{16}/(\Lambda_8 \oplus \Lambda_8)$ and $M_2 = \mathbb{R}^1 6/\Lambda_{16}$ are not isomorphic to each other. But the spectrum of Laplace operator on any torus $\mathbb{R}^n/\Lambda$ is $\{||\lambda||^2 : \lambda \in \Lambda\}$, counted with multiplicities. Since the theta series of the two lattice are the same, M_1 and M_2 have same spectrum.

Carolyn S.Gordon,David L.Webb, Scott Wolpert : The three mathematicians came up with two drums of dimension 2 that have equal areas and perimeters but different geometric shapes. They proved that the drums, each a multisided polygon, display identical spectra. This means both drum would generate the same set of normal-mode frequencies.

When physicist S. Sridhar of Northeastern University in Boston heard about the Gordon-Webb-Wolpert discovery, he decided to put it to an experimental test – and he had just the right kind of setup to do the

necessary experiment. Sridhar and his coworkers had been investigating aspects of quantum chaos [link to quantum chaos BOB] by looking at the patterns created when microwaves bounce around inside thin metal enclosures of various shapes. The same technique could be used to identify normal modes, with microwaves standing in for sound waves and severely squished cavities standing in for membranes. To test the drum theorem, the researchers constructed two cavities corresponding to one of the pairs of shapes discovered by Gordon and her colleagues. Fabricated from copper and having eight flat sides, each angular enclosure was nearly 8 centimeters long and less than 6 millimeters thick. Sending in microwaves through a tiny opening and measuring their strength over a range of frequencies at another location enabled the researchers to establish the frequencies of the normal modes of each cavity. They could also map the standing wave patterns inside the cavities.

Remarkably, the frequencies present in both spectra were practically identical. Any discrepancies between the spectra could be attributed to slight imperfections introduced during assembly of the enclosures.

Reference: Wiki: Hearing the shape of a drum
Drums That Sound Alike

4 Hecke Eigenforms and L-series

4.1 Hecke Theory

Definition 4.1 (*Hecke operator by F*)

For integer $m \geq 1$, weight k, there is a linear operator T_m from $M_k(\Gamma_1)$ to itself, which we called Hecke operator, defined by

$$T_m F(\Lambda) := \sum_{[\Lambda:\Lambda']=m} F(\Lambda'). \tag{57}$$

where we use the definition of modular form as homogeneous function F (of degree $(-k)$) on lattice $\Lambda \subset \mathbb{C}$, and the sum runs over all sublattice$\Lambda' \subset \Lambda$ of index m.

The index of Λ' over Λ is m implies that the fundamental parallelogram of Λ' is m times area of Λ.

It is obvious that the number of sublattice of given lattice Λ is finite. And $T_m F(\lambda\Lambda) = \sum F(\lambda\Lambda') = \lambda^{-k} \sum F(\Lambda')$, so $T_m F$ is also homogeneous of degree $-k$.

Translate from the language of lattice to that of functions in upper half plane by the formula we have mentioned in section 1

$$f(z) = F(\Lambda_z), \quad F(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) = \omega_2^{-k} f(\omega_1/\omega_2).$$

we find the action of T_m is given by

Definition 4.2 (*Hecke operator by f*)

$$T_m f(z) = m^{k-1} \sum_{\gamma \in \Gamma_1 \backslash M_m} (cz+d)^{-k} f(\frac{az+b}{cz+d}) \quad (\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \in \mathfrak{H}). \tag{58}$$

where M_m denotes the set of 2×2 integral matrix of determinant m. And m^{k-1} is normalizing constant (to send forms with integral Fourier coefficient to forms with integral Fourier coefficient.)

Now we explain the equivalence between two forms of definition. Firstly, to get sublattice with index m of Λ_z, we replace z and 1 by $az+b$ and $cz+d$ respectively with $ad-bc=m$. Thus we get sublattice $\Lambda' = (az+b)\mathbb{Z} + (cz+d)\mathbb{Z}$, whose covolume is m times of Λ_z's covolume. And by the second formula above, $F(\Lambda')$ is exactly the summand. (For example if Λ' has index 6, and we take $\gamma = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$, then the sublattice is generated by $2z+1$ and 3. Obviously, $\mathrm{Vol}(\Lambda') = 6\mathrm{Vol}(\Lambda)$) On the other hand, in the sum every orbit correspond to a sublattice, since by modularity of f, the summand is indeed unchanged when M is replaced by γM with $\gamma \in \Gamma_1$.

Then verify that $T_m f(z)$ is also in $M_k(\Gamma_1)$. For simplicity, we define $\gamma z_{[k]} = (cz+d)^{-k}$. By easy computation we find that

$$(\gamma_1\gamma_2) z_{[k]} = \gamma_1(\gamma_2 z)_{[k]} \cdot \gamma_2 z_{[k]}. \tag{59}$$

Then we can get:

$$T_m f(\gamma_0 z) = \sum_{\gamma\in\Gamma_1\backslash M_m} (c\gamma_0 z+d)^{-k} f(\gamma\gamma_0 z) = \sum_{\gamma\in\Gamma_1\backslash M_m} \gamma(\gamma_0 z)_{[k]} f(\gamma\gamma_0 z) = (\gamma_0 z_{[k]})^{-1} \sum_{\gamma\in\Gamma_1\backslash M_m} (\gamma\gamma_0)z_{[k]} f(\gamma\gamma_0)$$
$$= (c_0 z+d)^k \sum_{\gamma\in\Gamma_1\backslash M_m} \gamma z_{[k]} f(\gamma z) = (c_0 z+d)^k T_m f(z).$$

And it is easy to know that $T_m f(z)$ is holomorphic in $\mathfrak{H}$. It is also subexponential growth at infinity (i.e. $f(x+iy) = O(e^{Cy})$ as $y\to\infty$ and $f(x+iy) = O(e^{C/y})$ as $y\to 0$ for all $C>0$).

Next we calculate the effect of T_m on Fourier development. First determine a set of representatives of $\Gamma_1\backslash M_m$ is upper triangular matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. with $ad=m$, $0\le b<d$.

Exercise 1

A set of representation of $\Gamma_1\backslash M_m$ is upper triangular matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad=m$, $0\le b<d$.

Proof: Use T(when$|c|<2|a|$) to decrease $|a|$ and S(otherwise, change position of a and c, get the former condition again) repeatedly.Then use T to reduce b. ■

So we get:

$$T_m f(z) = m^{k-1} \sum_{a,d>0,ad=m} \frac{1}{d^k} \sum_{0\le b<d} f\left(\frac{az+b}{d}\right). \tag{60}$$

A further calculation with equation above show that $T_m f(z)$ has Fourier expansion as follows:

Proposition 4.1 (*Fourier expansion of $T_m f$*)

$$T_m f(z) = \sum_{d>0,d|m} (m/d)^{k-1} \sum_{n\ge 0,d|n} a_n q^{mn/d^2} = \sum_{n\ge 0} \left(\sum_{r|(m,n),r>0} r^{k-1} a_{mn/r^2} \right) q^n. \tag{61}$$

Proof: Firstly, the Fourier expansion

$$f\left(\frac{mz/d+b}{d}\right) = \sum_{n\ge 0} a_n q^{\frac{mn}{d^2}} e^{2\pi n\frac{b}{d}}$$

If $d\nmid n$, $\sum_{0\le b<d} e^{2\pi i n\frac{b}{d}}=0$, else $\sum_{0\le b<d} e^{2\pi i n\frac{b}{d}} = d$. Replace a by m/d in 60 and use equation above:

$$\begin{aligned}
T_m f(z) &= \sum_{d>0,d|m} (m/d)^{k-1} \frac{1}{d} \sum_{0\le b<d} \sum_{n\ge 0} a_n q^{\frac{mn}{d^2}} e^{2\pi i n\frac{b}{d}} \quad \text{(by first equation)} \\
&= \sum_{d>0,d|m} (m/d)^{k-1} \sum_{n\ge 0,d|n} a_n q^{mn/d^2}. \quad \text{(sum on } b\text{)} \\
&= \sum_{d>0,d|m} (m/d)^{k-1} \sum_{N=0}^{\infty} a_{Nd} q^{mN/d} \quad (n=Nd) \\
&= \sum_{r>0,r|m} r^{k-1} \sum_{N=0}^{\infty} a_{\frac{mN}{r}} q^{rN} \quad (r:=m/d) \\
&= \sum_{N=0}^{\infty} \left(\sum_{r|m} r^{k-1} a_{\frac{mN}{r}} \right) q^{rN} \quad \text{(exchange the order of sum)} \\
&= \sum_{n=0}^{\infty} \left(\sum_{r|m,r|n} r^{k-1} a_{\frac{mn}{r^2}} \right) q^n \quad (n=rN) = \sum_{n=0}^{\infty} \left(\sum_{r|(m,n),r>0} r^{k-1} a_{\frac{mn}{r^2}} \right) q^n
\end{aligned}$$

■

Let's calculate first two terms of the expansion of $T_m f$:

$$q^0 : \sum_{r|(m,0)} r^{k-1} a_0 = \sigma_{k-1}(m) a_0. \quad q^1 : \sum_{r|(m,1)} a_{m/r^2} = a_m$$

An important consequence of this formula is that:

Proposition 4.2 (*Commutative of Hecke operator*)

The operator T_m $(m \geq 1)$ all commute.

Proof: (this is NOT trivial)

Step 1: Prove $T_p T_q = T_q T_p$ for $(p,q) = 1$.

Assume $f \in M_k(\Gamma_1)$, $p, q \geq 1$, let $T_q f(z) = \sum_{n \geq 0} b_n q^n$, $\quad b_n = \sum_{s|(q,n)} s^{k-1} a_{\frac{qn}{s^2}}$. Thus,

$$T_p T_q f(z) = \sum_{n \geq 0} \left(\sum_{r|(p,n)} r^{k-1} b_{\frac{bn}{r^2}} \right) q^n,$$

the coefficient of q^n is

$$a_n(T_p T_q f) = \sum_{r|(p,n)} r^{k-1} \sum_{s|(q, \frac{pn}{r^2})} s^{k-1} a_{\frac{pqn}{r^2 s^2}}. \tag{62}$$

We can get $rs|(n,pq)$. (Since $r|q$, $s|p$, $rs|pq$. Since $s|\frac{pn}{r^2}$, $d = rs|\frac{pn}{r}$. If $rs \nmid n$, then rs has factor in p but not in n, while $r|n$, thus s has factor in p. However, $s|q$, so $(p,q) \neq 1$, contradiction! So, $rs|n$.) Thus, let $d = rs$

$$\begin{aligned}
a_n(T_p T_q f) &= \sum_{rs|(n,pq)} \sum_{r|(p,n)} \sum_{s|(q, \frac{pn}{r^2})} r^{k-1} s^{k-1} a_{\frac{pqn}{r^2 s^2}} \\
&= \sum_{d|(n,pq)} \sum_{r|d, r|(p,n)} \sum_{\substack{s|d, s|(q, \frac{pn}{r^2}) \\ rs=d}} (rs)^{k-1} a_{\frac{pqn}{d^2}} \\
&= \sum_{d|(n,pq)} \sum_{r|d, r|p} \sum_{\substack{s|d, s|q \\ rs=d}} (rs)^{k-1} a_{\frac{pqn}{d^2}} \quad (r|d \Rightarrow r|n) \text{ and } (s|d \Rightarrow s|n, s|\frac{pn}{r^2} \iff \frac{d}{r}|\frac{pn}{r^2} \iff d|\frac{p}{r}n) \\
&= \sum_{d|(n,pq)} d^{k-1} a_{\frac{pqn}{d^2}}
\end{aligned}$$

(Since (p,q)=1, for any d there is a unique decomposition of $d = rs$ with $r|p$ and $s|q$)

So $a_n(T_p T_q f)$ is symmetric for p and q, thus $T_p T_q = T_q T_p$ with $(p,q) = 1$. In fact we proved $T_p T_q = T_{pq}$ if $(p,q) = 1$.

Step 2: Prove that for p prime, we have

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}} \quad (r \geq 2). \quad T_1 := 1(\text{Identity operator}) \tag{63}$$

Thus T_{p^k} is a polynomial of T_p. By induction on k and l, we have $T_{p^k} T_{p^l} = T_{p^l} T_{p^k}$ for any $k, l \geq 1$.

$$a_n(T_{p^r}) = \sum_{d|(n,p^r)} d^{k-1} a_{\frac{p^r n}{d^2}} = a_{p^r n} + p^{k-1} a_{p^{r-2} n} + ... + p^{r(k-1)} a_{p^{-r} n}.$$

(The ith term correspond to $d = p^{i-1}$. And $a_{p^{r-2(i-1)} n} = 0$ if $p^{r-2(i-1)} n$ is not integral.)

And

$$a_n(T_p T_{p^{r-1}}) = \sum_{d|(n,p)} d^{k-1} a_{\frac{pn}{d^2}} (T_{p^{r-1}} f) = \sum_{d|(n,p)} d^{k-1} \sum_{e|(\frac{pn}{d^2}, p^{r-1})} e^{k-1} a_{\frac{p^r n}{e^2 d^2}} (f).$$

Then

$$\begin{aligned}
&a_n((T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}}) f) \\
&= \left(\sum_{e|(pn, p^{r-1})} e^{k-1} a_{\frac{p^r n}{e^2}} \right) + \left(p^{k-1} \sum_{e|(\frac{n}{p}, p^{r-1})} e^{k-1} a_{\frac{p^{r-2} n}{e^2}} \right) - \left(p^{k-1} \sum_{f|(n, p^{r-2})} f^{k-1} a_{\frac{p^{r-2}}{n} f^2} \right)
\end{aligned}$$

(Expand the sum on d in $a_n(T_p T_{p^{r-1}})$.)

$= a_n(T_{p^r} f)$. (Take $e = 1, p, ... p^{r-1}$ and $f = 1, p, ..., p^{r-2}$ and arrange the terms.)

Step 3: For any $m, n \in \mathbb{Z}_{\geq 1}$, by prime factorization and first two step, T_m and T_n commute. ∎

Let us consider some examples. By previous calculation:

$$\hat{a}_0 = \sigma_{k-1}(m)a_0, \quad \hat{a}_1 = a_m, ...$$

Thus, if f is a cusp form then so is $T_m f$. More specially, $S_{12}(\Gamma_1)$ is 1-dimensional and spanned by $\Delta(z)$, so $T_m\Delta(z)$ must be a mutiple of $\Delta(z)$ for any $m \geq 1$. And we know by calculation above $T_m\Delta(z) = \tau(m)q + ...$, thus

$$T_m\Delta(z) = \tau(m)\Delta(z).$$

So by Proposition 61 we get

$$\tau(m)\tau(n) = \sum_{r|(m,n)} r^{11}\tau\left(\frac{mn}{r^2}\right) \quad m, n \geq 1. \tag{64}$$

especially for $\gcd(m, n) = 1$, we have $\tau(m)\tau(n) = \tau(mn)$. proving Ramanujan's multiplicativity observations.

Generalize the argument above. Now, if $f \in M_k(\Gamma_1)$ is a simultaneous eigenfuntion of all of the $T_m(m \geq 1)$, with eigenvalues λ_m. Then we get

$$a_m = \lambda_m a_1 \quad \forall m \geq 1$$

We therefore know that if $a_1 = 0$, then the simultaneous eigenfunction f is a constant. We normalize f by $a_1 = 1$, such f is called **normalized Hecke eigenform** or **Hecke form**. Then we have

$$T_m f = a_m f. \quad (m \geq 1) \tag{65}$$

$$a_m a_n = \sum_{r|(m,n)} r^{k-1} a_{mn/r^2} \quad (m, n \geq 1). \tag{66}$$

Cusp form space of dimension 1 naturally have unique Hecke form. Those are $\Delta(z)E_{k-12}(z)$ in $S_k(\Gamma_1)$ for $k = 16, 18, 20, 22, 26$. And we also have Eisenstein series $\mathbb{G}_k$ for $k \geq 4$ satisfying

$$T_m\mathbb{G}_k = \sigma_{k-1}(m)\mathbb{G}_k, \quad \sigma_{k-1}(m)\sigma_{k-1}(n) = \sum_{r|(m,n)} r^{k-1}\sigma_{k-1}(mn/r^2). \tag{67}$$

Proof: We first prove for $m = p$ prime, then by Recursive formula of T_{p^r} 63, we can prove for $m = p^r$. Finally by $T_m T_n = T_{mn}$ when $(m, n) = 1$ and identity $\sigma_{k-1}(p^r)\sigma_{k-1}(q^s) = \sigma_{k-1}(p^r q^s)$, we get the property $\forall m \geq 1$. ■

Theorem 4.1 (*Hecke*)

$M_k(\Gamma_1)$ has a basis of normalized simultaneous eigenforms for all k, and this basis is unique.

Example: Hecke form as basis of $M_{24}(\Gamma_1)$:

$$\mathbb{G}_{24}, \quad f_1 = \Delta E_4^2 - (156 - 12\sqrt{144169})\Delta^2, \quad f_2 = \Delta E_4^2 - (156 + 12\sqrt{144169})\Delta^2$$

Finally we mention a little about Hecke's theory on other congruence groups of $SL(2, \mathbb{Z})$ of level N, for example $\Gamma_0(N)$. (1) The definition of T_m must be modified by adding a term if m and N are not coprime. (2) To find the unique Hecke form basis of $M_k(\Gamma_0(N))$, we have to decompose it as direct sum of space of "Old" and "New" forms.

4.2 L-series of Eigenforms

We have seen that $M_k(\Gamma_1)$ is spanned by normalized Hecke eigenforms $f = \sum a_m q^m$, satisfying equation 66. Specializing the equation we have

$$a_{pq} = a_p a_q \quad \text{if } \gcd(m, n) = 1, \quad a_{p^{m+1}} = a_p a_{p^m} - p^{k-1} a_{p^{m-1}} \quad (p \text{ prime}, m \geq 1) \tag{68}$$

In fact, this two case together are equivalent to the former equation 66.

Proof: Induction on the second case above (see it as case $n = 1$), we have 66 for $m = p^a, n = p^b$ for $a, b \geq 1$. Then by prime factorization on general m, n and the first case, we get the general equation. ■

The first says that the coefficient a_n are **multiplicative**, hence the **Dirichlet series**

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{69}$$

called **Hecke L-series of** f have Euler product:

$$L(f, s) = \prod_{p \text{ prime}} (1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + ...) \tag{70}$$

The second tells us:

$$\sum_{n=0}^{\infty} a_{p^n} x^n = \frac{1}{1 - a_p + p^{k-1}x^2}. \tag{71}$$

(which is the generating function of $\{a_{p^n}\}$.)

Combining these two statements we have:

Proposition 4.3 (*Hecke fundamental Euler product development*)

For normalized Hecke form $f \in M_k(\Gamma_1)$ we have

$$L(f, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}. \tag{72}$$

Example: For Eisenstein series $\mathbb{G}_k$,

$$L(\mathbb{G}_k, s) = \prod_p \frac{1}{1 - (1 + p^{k-1})p^{-s} + p^{k-1-2s}} = \prod_p \frac{1}{1 - p^{-s}} \cdot \prod_p \frac{1}{1 - p^{k-s-1}} = \zeta(s)\zeta(s - k + 1).$$

For eigenforms on $\Gamma_0(N)$, there is a similar result (the Euler factors for $p|N$ have to be modified suitably).

There's another fundamental property of general L-series(not any more just to eigenforms), they can be analytically continued in s and satisfy some functional equation.

We again restrict to Γ_1 for convenience, and only prove for cusp forms. (we omit proof for non-cusp forms since $L(f, s)$ then has poles which is messier to manage.). Since M_k is spanned by cusp forms and $\mathbb{G}_k$ ($M_k = \mathbb{C}E_k \oplus S_k$), and we have completely know the the L-series of the latter, we can extend the prove to any L-series.

Proposition 4.4

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k on Γ_1. Then the L-series $L(f, s)$ extends to an entire function $L^*(f, s) := (2\pi)^{-s}\Gamma(s)L(f, s)$. And it satisfies functional equation

$$L^*(f, k - s) = i^k L^*(f, s). \tag{73}$$

Proof: Mellin transform: $\mathcal{M}f(s) = \int_0^{\infty} t^{s-1} f(t)dt$.

Replace t by $2\pi nt$ in gamma function $\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}dt$ then multiplying a_n and summing over n, we get:

$$(2\pi)^{-s}\Gamma(s)L(f, s) = \sum_{n=1}^{\infty} a_n \int_0^{\infty} t^{s-1}e^{-2\pi nt}dt = \int_0^{\infty} t^{s-1} f(it)dt.$$

The interchange of integration and summation is due to the absolute convergence: $\sum_n \int |a_n t^{s-1}e^{-2\pi nt}|dt < \infty$ (Fubini Theorem). And fact that cusp form $f(it)$ is exponentially small for $t \to \infty$ ($f = O(e^{-2\pi t})$) and for $t \to 0$ (because $f(-1/z) = z^k f(z)$), implies that the integral converges absolutely for all $s \in \mathbb{C}$.

Hence the function $L^*(f,s)$ extends holomorphically from the half-plane $\Re(s) > 1 + k/2$ to the entire complex plane.

By sbsititution $t \to 1/t$ and equation $f(i/t) = (it)^k f(it)$ of f we obtain:

$$L^*(f, k-s) = i^k L^*(f,s). \tag{74}$$

■

remark 28

The converse of the proposition hold as well: if $a_n \quad (n \geq 1)$ are complex numbers of polynomial growth and $L^*(f,s) = (2\pi)^{-s}\Gamma(s)\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ continues analytically to the whole complex plane and satisfies the functional equation 73, then $f(z) = \sum_n a_n e^{2\pi i n z}$ is a cusp form of weight k on Γ_1.

4.3 Modular Forms and Algebraic Number Theory

We have investigated the Γ_1-equivalent classes of binary quadratic forms in 1.2, and proved that for each discriminant $D < 0$, class number $h(D)$ is finite. Further, we have a

Proposition 4.5

*If $D <$ is a square-free integral number, the class number of binary quadratic forms $h(D)$ equals the **class number of the imaginary quadratic field** $K = \mathbb{Q}(\sqrt{D})$. Precisely, there is a well-known bijection between the classes of binary quadratic forms of discriminant D and the ideal classes of K, such that:*

$$r(Q,n) = w \cdot r(\mathcal{A}, n),$$

where $r(Q,n)$ is the representation number of n by Q, $r(\mathcal{A},n)$ denotes the number of integral ideal $\mathfrak{a}$ of norm n in the corresponding ideal class $\mathcal{A}$.

Proof: (algebraic number theory; to be added, firstly need to define class number of a field.) ■

Thus we can rewrite the L-series of theta series Θ_Q:

$$L(\Theta_Q, s) = w \cdot \sum_{\mathfrak{a}\in\mathcal{A}} N(\mathfrak{a})^{-s}.$$

The sum on the right side is called "partial zeta-function", denoted by $\zeta_{K,\mathcal{A}}(s)$.

We know that the ideal classes of K forms an abelian group $Cl(K)$. Let χ be a homomorphism from $Cl(K)$ to $\mathbb{C}^*$. Define

$$L_K(s,\chi) := \sum_{\mathfrak{a} \text{ integral ideal in } K} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{\mathcal{A}\in Cl(K)} \chi(\mathcal{A})\zeta_{K,\mathcal{A}}(s).$$

It is hence the L-series of modular form $f_\chi(z) = w^{-1}\sum_{\mathcal{A}}\chi(\mathcal{A})\Theta_{\mathcal{A}}(z)$.

Since the integral ring O_K of number field K is a Dedekind domain, the integral ideal (ideal in O_K) of K is unique prime factorization. It follows that $L_K(s.\chi)$ has a Euler product, hence f_χ is a Hecke eigenform.

If $\chi = \chi_0$ is the trivial character, then $L_K(s,\chi_0) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ is called **Dedekind zeta function** of K (ref Feng. Section 4.3). We claim the factorization:$\zeta_K(s) = \zeta(s)L(s,\epsilon_D)$, where $\epsilon_D(n) = \left(\frac{D}{n}\right)$ (Kronecker symbol) and $L(s,\epsilon_D) = \sum_{n=1}^{\infty}\epsilon_D(n)/n^s$. Then

$$L_K(s,\chi_0) = \zeta(s)L(s,\epsilon_D) = \sum_{n=1}^{\infty}\frac{\sum_{d|n}\epsilon_D(d)}{n^s}.$$

And we also have

$$L_K(s,\chi_0) = \sum_{n=1}^{\infty}\sum_{\mathcal{A}\in Cl(K)}\frac{r(\mathcal{A},n)}{n^s} = w^{-1}\sum_{n=1}^{\infty}\sum_{[Q]}\frac{r(Q,n)}{n^s}.$$

Therefore, $L_K(s,\chi_0)$ is the L-series of modular form $f_{\chi_0} = w^{-1}\sum_{[Q]}\Theta_Q(q)$ (we have mentioned this above). And more importantly, we get identity (which is know to Gauss):

$$\sum_{[Q]} r(Q,n) = w\sum_{d|n}\epsilon_D(d). \tag{75}$$

Correspondingly,

$$\begin{aligned} f_{\chi_0}(z) = w^{-1}\sum_{[Q]}\Theta_Q(q) &= w^{-1}\sum_{n=0}^{\infty}\left(\sum_{[Q]} r(Q,n)\right)q^n \\ &= \frac{h(D)}{w} + \sum_{n=1}^{\infty}\left(\sum_{d|n}\epsilon_D(d)\right)q^n. \end{aligned} \tag{76}$$

which is a **Eisenstein series of weight 1** (Cf Miyake. Modular Forms. Chapter 7.2).

If the character χ has order 2, then it is called **genus character**. We claim that then $L_K(s,\chi)$ factors as $L(s,\epsilon_{D_1})L_K(s,\epsilon_{D_2})$, where $D = D_1D_2$. In this case, f_χ is also an Eisenstein series. However in other cases, f_χ is a cusp forms.

♣ Binary Quadratic Forms of Discriminant -23

4.4 Modular Forms Associated to Elliptic Curves and Other Varieties

♣ Fermat's Last Theorem

5 Modular Forms and Differential Operators

5.1 Derivatives of Modular Forms

♣ Modular Forms Satisfy Non-Linear Differential Equations

♣ Moments of Periodic Functions

5.2 Rankin-Cohen Brackets and Cohen-Kuznetsov Series

♣ Further Identities for Sums of Powers of Divisors

♣ Exotic Multiplications of Modular forms

5.3 Quasimodular forms

♣ Counting Ramified Coverings of the Torns

5.4 Linear Differential Equations and Modular Forms

♣ The Irrationality of $\zeta(3)$

♣ An Example Coming from Percolation Theory

6 Singular Moduli and Complex Multiplication

To describe the theory of complex multiplication (CM) fully needs to combine themes relating to elliptic curves, modular forms, and algebraic number theory. In this note we will discuss mostly the modular forms side, and brifly explian the notion of CM in the language of elliptic curves.

An elliptic curve E over $\mathbb{C}$ can be represented by a quotient $E = \mathbb{C}/\Lambda$ (by Weierstrass p-function), where Λ is a lattice in $\mathbb{C}$. If $\lambda\Lambda \subset \Lambda'$, then multiplication by λ induces an algebraic map from E to $E' = \mathbb{C}/\Lambda$. In particular, if $\lambda\Lambda \subset \Lambda$, then we get a map from E to itself. $\lambda \in \mathbb{Z}$ is the only possible real values of λ.

An elliptic curve $E = \mathbb{C}/\Lambda$ is said to be **admit complex multiplication** if $\lambda\Lambda \subset \Lambda$ for some non-real value of λ.

As we have seen in previous notes, there are two different ways in which elliptic curves are related to modular forms.

(i) The moduli space of elliptic curves is precisely the domain of definition of modular function on Γ_1, $\Gamma_1 \backslash \mathfrak{H}$.

(ii) The elliptic curves over $\mathbb{Q}$ are suppose (and now finally known, which is called Modularity Theorem) to have parametrizations by modular functions, and to have Hasse-Weil L-funtions which coincide with the Hecke L-series of certain cusp form of weight 2.

remark 29

In the first relation bewteen elliptic curves and modular forms, the moduli space is used to parametrize all of the isomorphic classes of some geometry object, every point of moduli space correspond to a isomorphic class of elliptic curves. (though we haven't give the precise definition of moduli space, which is a basic notion in algebra geometry.) To get isomorphic classes of elliptic curves, we need to quotient two equivalent relations on lattice: ***homothety of lattice*** *($\Lambda_1 = \lambda\Lambda_2$) to write Λ as $\mathfrak{z}\mathbb{Z} + \mathbb{Z}$, and* Γ_1***-action on*** $\mathfrak{z} \in \mathfrak{H}$*(easy to verify after action of $\gamma \in \Gamma_1$, $\gamma\mathfrak{z}\mathbb{Z} + \mathbb{Z}$ denotes the same lattice) to get the moduli space of elliptic curves $\Gamma_1 \backslash \mathfrak{H}$.*

The modularity conjecture(Taniyama-Shimura-Weil conjecture) says that every elliptic curves E is associated to a modular form f such that $L(E, s) = L(f, s)$, i.e. there L-function coincide. In 1993 Wiles announced a proof of the modularity conjecture in the semistable case, but a flaw was found in the proof, which was fixed in 1995 by Taylor and Wiles. In 2001 the full conjecture was proved for all elliptic curves over $\mathbb{Q}$ by Brueil, Conrad, Diamond, and Taylor.

The elliptic curves with CM are of special interest from both point of view. From first view, if we think of $\mathfrak{H}$ as parametrizing elliptic curves, then, if the points $\mathfrak{z} \in \mathfrak{H}$ corresponds to *an elliptic curves with CM* we call this point a **CM points**. Next we will discuss the relation between CM points and integer quadratic forms.

Proposition 6.1

$\mathfrak{z} \in \mathfrak{H}$ is a CM point $\iff$ $\mathfrak{z}$ satisfies a quadratic equation over $\mathbb{Z}$.

Proof: ($\Rightarrow$) If $\mathbb{C}/(\mathbb{Z} + \mathfrak{z}\mathbb{Z}) = \mathbb{C}/\Lambda$ is an elliptic curve with CM, then $\exists \alpha \in \mathbb{C}, \alpha\Lambda \subset \Lambda$, thus $\alpha = a + b\mathfrak{z}$ and $\alpha\mathfrak{z} = c + d\mathfrak{z}$, eliminate α we get the quadratic equation

$$b\mathfrak{z}^2 + (a - d)\mathfrak{z} - c = 0. \tag{77}$$

And if $\mathfrak{z}$ satisfy some equation $A\mathfrak{z}^2 + B\mathfrak{z} + C$, then there is a matrix $M \in M(2, \mathbb{Z})$(such as $(B, C; -A, 0)$) fix $\mathfrak{z}$, with $m = \det M$. This will be fully discussed latter.

($\Leftarrow$) Assume that $A\mathfrak{z}^2 + B\mathfrak{z} + C$ with $\gcd(A, B, C) = 1$ and $D = B^2 - 4AC < 0$. i.e. minimal polynomial of $\mathfrak{z}$. Let

$$\alpha = \frac{1}{2}(t + Bu) + Au\mathfrak{z}, \quad t, u \in \mathbb{Z}, \quad t \equiv Du \pmod 2,$$

easy to verify that $\alpha\Lambda \subset \Lambda$ (sufficient to verify only for 1 and $\mathfrak{z}$). ■

The discriminant D of the minimal polynomial of some CM point $\mathfrak{z}$ is defined as **Discriminant of CM point**. Denote by $\mathfrak{Z}_D$ the set of CM point with discriminant D. By proposition above, any $\mathfrak{z} \in \mathfrak{Z}$ associated to a $Q \in \mathfrak{Q}_D$(which defined in 1.8) by $\mathfrak{z} \mapsto$ (minimal polynomial of $\mathfrak{z}$), and on the other hand, for $Q(x, y) = Ax^2 + Bxy + Cy^2 \in \mathfrak{Q}_D$, we have $Q(x, y) \mapsto \mathfrak{z}_Q$ (root of $Q(\mathfrak{z}, 1) = 0$). Furthermore, quotient the Γ_1 equivalence, we get bijection:

$$\Gamma_1 \backslash \mathfrak{Q}_D \longleftrightarrow \Gamma_1 \backslash \mathfrak{Z}_D \tag{78}$$

In particular, $|\Gamma_1 \backslash \mathfrak{Z}_D| = h(D)$, the class number of D. We can choose a set of representatives $\{\mathfrak{z}_{D,i}\}_{1 \le i \le h(D)}$, (e.g. the set $\mathfrak{Z}_D \cap \widetilde{\mathcal{F}}_1$ corresponding to the set $\mathfrak{Q}_D^{red}$).

The basic fact of CM point $\mathfrak{z}$ is that the value of $j(\mathfrak{z})$ is then an algebraic number.(which will be proved in section 6.1) . (?)This says that an elliptic curve with CM is always defined over $\overline{\mathbb{Q}}$ (i.e. has a Weierstrass equation with algebraic coefficient).

These special algebraic numbers $j(\mathfrak{z})$ is called **singular moduli**. They have remarkalbe properties: they give explicit generators of the class fields of imaginary quadratic fields; the differences between them factor into small prime factors; their traces are themselves the coefficients of modular forms, etc. (In 6.1 and 6.2).

From the second view, we consider L-function of CM elliptic curves and associated cusp form. Both of them have very special properties: the former belongs to two important classes of Dirichlet series (Epstein zeta functions and L-series of grossen-characters), and the latter is a theta series with spherical coefficients associated to a binary quadratic form.(In 6.3 and 6.4).

6.1 Algebraicity of Singular Moduli

In this subsection we will discuss the proof, refinements, and applications of the following basic statement:

Proposition 6.2

Let $\mathfrak{z} \in \mathfrak{H}$ be a CM point. Then $j(\mathfrak{z})$ is an algebraic number.(i.e., a root of some polynomial in $\mathbb{Q}[x]$)

Before that, we first introduce properties of the modular invariant $j(z)$:

Proof: (sketch) By proposition above, $\mathfrak{z}$ satisfies quadratic equation over $\mathbb{Z}$, say $A\mathfrak{z}^2 + B\mathfrak{z} + C = 0$. There are always matrices $M \in M(2, \mathbb{Z})$ which fixes $\mathfrak{z}$ as well as having positive determinant.(so it act on the upper half-plane.)

Then the two function $j(z)$ and $j(Mz)$ are both modular function on the subgroup $\Gamma_1 \cap M^{-1}\Gamma_1 M$ (of finite index in Γ_1). We have:

Lemma 6

$j(z)$ and $j(Mz)$ are algebraically dependent over $\mathbb{C}$.

Next, by looking at the Fourier expansion at infinity, we can see that:

Lemma 7

The $P(X, Y)$ such that $P(j(z), j(Mz)) = 0$ can be chosen to have coefficients in $\mathbb{Q}$.

Finally, since M fixes $\mathfrak{z}$, the number $j(\mathfrak{z})$ is then a root of the polynomial $P(X, X) \in \mathbb{Q}[X]$, so it is algebraic. ■

♣ Strange Approximations to π

♣ Computing Class Numbers

♣ Explicit Class Field Theory for Imaginary Quadratice Fields

♣ Solution of Diophantine Equations

6.2 Norms and Traces of Singular Moduli

♣ Height of Heegner Points

♣ The Borcherds Product Formula

Periods and Taylor Expansion of Modular Forms

♣ Two Transcendence Results

♣ Hurwitz Number

♣ Generalized Hurwitz Numbers

6.3 CM Elliptic Curves and CM Modular Forms

♣ Factorization, Primality Testing, and Cryptography

♣ Central Values of Hecke L-Series

♣ Which Primes are Sums of Two Cubes ?