

COUNTING COVERS OF ELLIPTIC CURVES

Orlando Marigliano

May 8, 2015

Contents

1. Quasimodular forms	2
1.1. The space of quasimodular forms	2
2. Basic facts and definitions	6
2.1. Covering spaces	6
2.2. Complex curves	7
3. Covers of an elliptic curve	8
3.1. Connected covers	8
3.2. Covers	9
4. Classifying covers via the fundamental group	12
4.1. Marked covers	12
5. Appendix A: Calculations	13
5.1. Quasimodular forms	13

1. Quasimodular forms

This section introduces quasimodular forms as described in [2].

1.1. The space of quasimodular forms

Let $\mathcal{H} = \{\tau \in \mathbb{C}; \Im(\tau) > 0\}$ denote the upper half-plane. For $\tau \in (H)$, define $q = \exp(2\pi\tau)$ and $Y = 4\pi\Im(\tau)$. Further, let $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{C})$ denote the full modular group. Then $\mathrm{SL}_2(\mathbb{Z})$ operates on \mathcal{H} by

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}, \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).^1$$

Definition. A *modular form (of weight k)* is a holomorphic function f on \mathcal{H} satisfying the modular condition $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all τ in \mathcal{H} , which is holomorphic at infinity.

A function satisfying the modular condition is \mathbb{Z} -periodic, hence induces a map $f_\infty(\zeta)$, holomorphic for $\zeta \neq 0$, such that $f(\tau) = f_\infty(q)$. The condition that f should be holomorphic at infinity means that the function f_∞ should be holomorphic at zero.

Note that if k is odd, then any function satisfying the modular condition of k is zero.

The modular forms of weight k form a vector space, denoted by M_k . Multiplying two modular forms having the weights k and l yields a modular form of weight $k + l$, giving the space $\bigoplus_k M_k$ the structure of a graded ring, denoted by M_* .

Examples. For an even integer $k \geq 2$, the *Eisenstein series of weight k* is the function

$$E_k(\tau) = 1 - \frac{2k}{b_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n,$$

where b_k is the k -th Bernoulli number, and $\sigma_{k-1}(n) = \sum_{m|n} m^{k-1}$. By definition, these functions are holomorphic at infinity. For $k \geq 4$, the Eisenstein series of weight k is a modular form of weight k . One proves this for example by showing that for $k \geq 4$, the series E_k is a multiple of the function $G_k(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} (m\tau + n)^{-k}$, which is indeed modular of weight k .

¹To see that $\gamma\tau \in \mathcal{H}$, note that $\Im(\gamma\tau) = \Im(\tau)/|c\tau + d|^2$.

The function $\Delta = 2^{-6}3^{-3}(E_4^3 - E_6^2)$ is a modular form of weight 12. By a theorem of Jacobi, one has

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

The theory of modular forms, including the above equality, is developed in more detail in [3]. Therein, one also finds a proof of the following proposition, which characterizes the space of modular forms.

Proposition 1.1. *There is an isomorphism of graded rings $\mathbb{C}[X_4, X_6] \rightarrow M_*$ mapping X_i to E_i , where the former ring is graded by assigning to X_i the degree i . In particular, there are no nonzero modular forms of negative weight.*

Definition. An *almost holomorphic modular form* (of weight k) is a function F on \mathcal{H} of the form

$$F(\tau) = \sum_{m=0}^M f_m(\tau) Y^{-m}$$

satisfying the modular condition $F(\gamma\tau) = (c\tau + d)^k F(\tau)$, where the f_m are holomorphic functions, holomorphic at infinity.

Even though Y is \mathbb{Z} -periodic, it is not a priori clear whether the modular condition already implies that the f_m are \mathbb{Z} -periodic, which is required to justify the above definition. Nevertheless, this is a consequence of the following proposition, which allows comparing Y -coefficients.

Proposition 1.2. *Let F be a function of the form $F(\tau) = \sum_{m=0}^M f_m(\tau) Y^{-m}$, for some holomorphic f_m . If $F = 0$ on \mathcal{H} , then all the coefficients f_m are zero on \mathcal{H} .*

Proof. For the differential operator $\frac{d}{d\tau}$ one has $\frac{d}{d\tau} Y^{-m} = -2\pi i m Y^{-m-1}$ and $\frac{d}{d\tau} f_m = 0$, hence

$$0 = \frac{d}{d\tau} F(\tau) = -2\pi i \sum_{m=1}^M f_m(\tau) Y^{-m-1} = -2\pi i Y^{-2} \left(\sum_{m=0}^{M-1} f_{m+1}(\tau) Y^{-m} \right).$$

By induction this implies that the f_m are zero for $m \geq 1$, hence also $f_0 = 0$. \square

Corollary 1.3. *Let $F(\tau) = \sum_{m=0}^M f_m(\tau) Y^{-m}$ be an almost holomorphic modular form. Then the leading coefficient f_M is a modular form of weight $k - 2M$. In particular, if $f_M \neq 0$, then $2M \leq k$.*

Proof. This follows after comparing the coefficients of Y^{-M} in both sides of the modularity condition $F(\gamma\tau) = (c\tau + d)^k F(\tau)$, using the equality

$$Y^{-1}(\gamma\tau) = (c\tau + d)^2 Y(\tau)^{-1} + \frac{c(c\tau + d)}{2\pi i}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$. □

The almost holomorphic modular forms of weight k form a vector space, denoted by \widehat{M}_k . Let \widehat{M}_* denote the associated graded ring.

Definition. An element in the image of the map $\widehat{M}_k \rightarrow \mathcal{O}(\mathbb{C})$ taking an almost holomorphic modular form $F = \sum_{m=0}^M f_m Y^{-m}$ of weight k to f_0 is called a *quasimodular form of weight k* . Hence a quasimodular form is a holomorphic function on the upper plane appearing as the constant term of an almost holomorphic modular form.

Again, denote the vector space of quasimodular forms of weight k by \widetilde{M}_k and the associated graded ring by \widetilde{M}_* . The definition gives a surjective graded ring homomorphism $\widehat{M}_* \rightarrow \widetilde{M}_*$ and one has $\widehat{M}_k \cap \widetilde{M}_k = M_k$.

Example. Consider the second Eisenstein series

$$E_2(\tau) = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n,$$

where $\sigma_1(n) = \sum_{d|n} d$. For the weight 12 modular form $\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q)^{24}$, one has the identity $2\pi i E_2(\tau) = \frac{d}{d\tau} \log(\Delta(\tau))$, which is proven by a straightforward computation. Using the modularity of Δ , one then computes

$$E_2(\gamma\tau) = (c\tau + d)^2 E_2(\tau) + \frac{6c(c\tau + d)}{\pi i},$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$.

Now, since $Y^{-1}(\gamma\tau) = (c\tau + d)^2 Y(\tau)^{-1} + \frac{c(c\tau + d)}{2\pi i}$, it follows that $E_2^* = E_2 - 12/Y$ is an almost holomorphic modular form of weight 2. Hence, E_2 is a quasimodular form of weight 2.

Proposition 1.4. *The space \widetilde{M}_* of quasimodular forms satisfies the following properties.*

1. *The canonical graded homomorphism $\widehat{M}_* \rightarrow \widetilde{M}_*$ is an isomorphism.*

2. *There is an isomorphism of graded rings $M_* \otimes \mathbb{C}[X_2] \simeq \mathbb{C}[X_2, X_4, X_6] \rightarrow \widetilde{M}_*$ mapping X_i to E_i , where the former ring is graded by assigning to X_i the degree i .*
3. *Quasimodular forms are closed under taking derivatives.*

Proof. 1. The map $\widehat{M}_* \rightarrow \widetilde{M}_*$ is surjective by definition. Injectivity follows from Calculation 5.1. Given an almost holomorphic modular form $F(\tau) = \sum_{m=1}^M f_m(\tau)Y^{-m}$ with constant term zero, the strategy is to solve the modularity equation for the coefficients f_m . This way, one finds for a fixed argument τ a polynomial equation in the lower row components c, d of any transformation $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, involving the coefficients $f_m(\tau)$. By varying the transformation γ , one may force these coefficients to be zero.

2. Express the map $\mathbb{C}[X_2, X_4, X_6] \rightarrow \widetilde{M}_*$ as the composition

$$\mathbb{C}[X_2^*, X_4, X_6] \rightarrow \widehat{M}_* \rightarrow \widetilde{M}_*,$$

where the first map takes X_2^* to E_2^* and X_i to E_i , and the second map is the canonical map, which is an isomorphism by the first point above.

To prove the surjectivity of the first map, let $F(\tau) = \sum_{m=0}^M f_m(\tau)Y^{-m}$ be an almost holomorphic modular form. Then $f_M(E_2^*/12)^M$ is an almost holomorphic modular form of weight k , since f_M is modular of weight $k - 2M$, and the difference $F - f_M(E_2^*/12)^M$ has degree smaller than M . Now use induction on M .

To get injectivity, let $F = \sum_{\alpha=0}^{k/2} (E_2^*)^\alpha f_{k-2\alpha}$ be an almost holomorphic modular form of weight k , in the image of the first map, where the f_m are modular of weight m . If $F = 0$, then by comparing the coefficients of $Y^{-k/2}$ one obtains $0 = f_0$. Now it follows by induction on k that the other coefficients f_m are zero. Hence F was the image of the zero element in $M_* \otimes \mathbb{C}[X_2^*]$.

3. To prove the last statement, one verifies that $(6/\pi i)E_2' - E_2^2$ is modular of weight 4, and that if f is modular of weight k , then $(6/\pi i)f' - kE_2f$ is modular of degree $2 + k$. Now use the second point above.

□

2. Basic facts and definitions

In this section we will fix some notation and recall the definitions and basic properties of the objects of this thesis. We will follow [4].

2.1. Covering spaces

Definition. Let X be a topological space, F a set, G a group operating on both X and F . Define the fibred product $X \times_G F$ to be the topological space $(X \times F) / \sim$, where $(x, f) \sim (gx, gf)$ for all g in G .

Proposition 2.1. *Let X be a connected, locally pathwise connected, and semi-locally simply connected topological space. Let $p : \widetilde{X} \rightarrow X$ be a universal cover. Furthermore, choose a point \tilde{x}_0 of \widetilde{X} , and let x_0 be the image of \tilde{x}_0 in X . Then there is an equivalence of categories*

$$\{\text{Unbranched covers of } X\} \longrightarrow \{\pi_1(X, x_0)\text{-sets}\},$$

defined by the pair of quasi-inverse functors

$$(p_Y : Y \rightarrow X) \mapsto p_Y^{-1}(x_0) \text{ and } F \mapsto \widetilde{X} \times_{\pi_1} F.$$

Proof. One verifies by hand that the given functors are mutually quasi-inverse, by using elementary covering theory. Nonetheless, the needed isomorphisms between objects are given below.

Let F be a π_1 -set and $p_F : \widetilde{X} \times_{\pi_1} F \rightarrow X$ the associated covering. Define a map $\zeta_F : F \rightarrow p_F^{-1}(x_0)$ by sending an element f to the class of (\tilde{x}_0, f) . This map is surjective by definition, and is injective since the π_1 -action on \widetilde{X} is free.

On the other hand, let $p_Y : Y \rightarrow X$ be a cover of X . Define a map

$$\eta_Y : \widetilde{X} \times_{\pi_1} p_Y^{-1} \rightarrow Y$$

as follows. For a given class (\tilde{x}, f) , let $\beta : [0, 1] \rightarrow \widetilde{X}$ be a path starting in \tilde{x}_0 and ending in \tilde{x} . Consider the projection $p\beta$ of β to X and lift the path $p\beta$ to a path $\tilde{\beta}_f$ in Y , with starting point f . Finally, set $\eta_Y(\tilde{x}, f) = \tilde{\beta}_f(1)$. Note that since \widetilde{X} is simply connected, this is independent of the choice of the path β . Also, the map is well-defined, since $p\beta\tilde{\gamma} = p\beta$ for any lift $\tilde{\gamma}$ of a loop in X .

η_Y is surjective: for $y \in Y$, let β be a path in X with starting point $p_Y(y)$ and endpoint x_0 . Let $f = \tilde{\beta}_y(1)$, be the endpoint of the lift of β to Y with starting point y . Then y is the image of $(\tilde{\beta}_{x_0}(1), f)$ under η_Y , where $\tilde{\beta}_{x_0}$ is a lift of β to \tilde{X} with starting point \tilde{x}_0 . To see that the map is injective, given any two points $(\tilde{x}_1, f), (\tilde{x}_2, g)$ mapping to the same point in Y , define a path in \tilde{X} connecting \tilde{x}_1 to \tilde{x}_2 , and use the paths given by the definition of η_Y to construct the loop in X that will take (\tilde{x}_1, f) to (\tilde{x}_2, g) \square

Remark. In the above proposition, if X has the structure of a Riemann surface, then the first category may be taken to be the category of unbranched covers of Riemann surfaces over X . Indeed, every cover inherits a complex structure from X such that the structure map becomes holomorphic, and morphisms of covers of X are automatically holomorphic: in general, if fg and f are holomorphic, then g is.

2.2. Complex curves

Proposition 2.2. *The assignment $C \mapsto K(C)$ defines a contravariant equivalence of categories between the category of irreducible smooth curves over \mathbb{C} and the category of finitely generated, transcendence degree one, field extensions of \mathbb{C} . By definition, degree d maps of curves correspond to degree d field extensions.*

Proof. See [4] pp. 20-22. \square

Proposition 2.3 (Riemann-Hurwitz formula). *Let $\varphi: C_1 \rightarrow C_2$ be a finite, degree d map of smooth curves of genera g_1 and g_2 , respectively. Then*

$$2g_1 - 2 = d(2g_2 - 2) + \sum_{x \in C_1} (e_\varphi(x) - 1),$$

where $e_\varphi(x)$ is the ramification index of φ at x .

3. Covers of an elliptic curve

3.1. Connected covers

In the following, let \mathbb{C} be the ground field for all varieties considered.

Definition. Let E be an elliptic curve.

1. A *(degree d , genus g , connected) cover of E* is a finite, degree d morphism $p: C \rightarrow E$ of an irreducible smooth curve C of genus g onto E . Denote such a cover by (C, p) , possibly omitting the structure map p .
2. If $S = b_1, \dots, b_{2g-2}$ is a set of $2g - 2$ distinct points of E , call a cover C *simply branched over S* , if it is simply branched over each point of S . This means that for all points b of S there is exactly one point x in $p^{-1}(b)$ with ramification index $e_p(x) = 2$, the others having a ramification index of one.

It follows from the Riemann-Hurwitz formula of Proposition 2.3 that every point not in the pre-image of S has a ramification index of one. This justifies the choice of the number of points in S .

3. Two covers C_1, C_2 are to be considered isomorphic, if there is an isomorphism $C_1 \rightarrow C_2$ commuting with the respective structure maps into E . Accordingly, define the automorphism group $\text{Aut}_p(C) = \text{Aut}(C)$ of the cover (C, p) to be the group of cover isomorphisms $C \rightarrow C$.

Proposition 3.1. *Let C be a connected cover of E . Then the automorphism group of C is finite.*

Proof. By Proposition 2.2, if C is a degree d connected cover, the elements of $\text{Aut}(C)$ correspond to the automorphisms of the degree d field extension $K(C)/K(E)$, of which only finitely many exist. \square

Remark. The degree d connected covers of an elliptic curve E form a set. Indeed, they correspond by Proposition 2.2 to elements of the power set of the algebraic closure of $K(E)$.

Definition. Let E be an elliptic curve, $S = b_1, \dots, b_{2g-2}$ a set of $2g - 2$ distinct points of E .

1. Denote the set of isomorphism classes of degree d , genus g , simply branched over S , connected covers of E by $\text{Cov}(E, S)_{g,d}^\circ$.

2. Any isomorphism of two equivalent covers defines a bijection of their automorphism groups. This allows to define the *weight* of the class $[(C, p)]$ to be the number $1/|\text{Aut}_p(C)|$.
3. Define $N_{g,d}$ to be the weighted count

$$\sum_{C \in \text{Cov}(E, S)_{g,d}^\circ} \frac{1}{|\text{Aut}(C)|}.$$

The elliptic curve E and the set of points S are omitted from the notation, a priori for brevity. It will turn out that $N_{g,d}$ is finite and does not depend on the choice of E and S .

Definition. For any $g \geq 1$, define F_g to be the generating series

$$F_g(q) = \sum_{d \geq 1} N_{g,d} q^d$$

counting covers of genus g .

This thesis shall prove the following result.

Theorem 3.2 (Dijkgraaf). *Let $g \geq 2$, and for $\tau \in \mathbb{C}$ let $q(\tau) = \exp(2\pi i \tau)$. Then the function $F_g \circ q$ is a quasimodular form of weight $6g - 6$.*

The strategy to prove the theorem will involve considering a larger class of curves covering the fixed elliptic curve, also allowing “disconnected” covers. The covers in this more general sense will be easier to count.

3.2. Covers

Definition. Let E be an elliptic curve, $S = b_1, \dots, b_{2g-2}$ a set of $2g - 2$ distinct points of E .

1. A *(degree d , genus g) cover* of E is a finite, degree d morphism $p: C \rightarrow E$ of a disjoint union $C = \cup_i C_i$ of k irreducible smooth curves C_i of genus g onto E . Again, often a cover will be identified with its source C .
2. A cover C is *simply branched over S* , if it is simply branched over each point of S . Hence the cover C has $2g - 2$ ramification points.

3. We define the notion of isomorphic covers and the automorphism group $\text{Aut}_p(C)$ of a cover as before.
4. For a cover $(\cup_i C_i, p)$ we define the maps p_i to be the restrictions to the C_i of the structure map p . These are finite maps, whose degrees we denote by d_i .

Remark. By the Riemann-Hurwitz formula, the maps p_i have $2g_i - 2$ ramification points on C_i . Hence, the following relations hold:

$$\sum_i d_i = d, \text{ and } \sum_i (2g_i - 2) = 2g - 2.$$

Remark. The automorphism group of a cover $C = C_1 \cup \dots \cup C_k$ is the semidirect product

$$\text{Aut}_p(C) = \prod_i \text{Aut}_{p_i}(C_i) \rtimes \Gamma,$$

where $\Gamma \subset S_k$ is the subgroup of the permutations of the components such that each orbit is contained in an isomorphism class of connected covers over E .

Indeed, since cover isomorphisms must permute isomorphic components, there is a homomorphism of $\text{Aut}(C)$ into Γ which is the identity on Γ , viewed as a subset of $\text{Aut}(C)$, having as kernel the product $\prod_i \text{Aut}_{p_i}(C_i)$.

If the cover C is simply branched over Γ , then no two components of genus greater than one are isomorphic as connected covers, since any isomorphism would have to preserve ramification indices (see for example [4], prop. 2.6 c), but no two components share a branched point over E . In particular, if there are no components of genus one, then $\Gamma = 1$.

On the other hand, each component of genus one is unramified over E , and could be isomorphic to other components of genus one, in which case Γ is nontrivial.

Definition. Let E be an elliptic curve, $S = b_1, \dots, b_{2g-2}$ a set of $2g - 2$ distinct points of E .

1. Denote the set of isomorphism classes of degree d , genus g , simply branched over S , covers of E by $\text{Cov}(E, S)_{g,d}$.
2. Assign to an element $[(C, p)]$ of $\text{Cov}(E, S)_{g,d}$ the *weight* $1/\text{Aut}_p(C)$. This is again well-defined.

3. Define $\widehat{N}_{g,d}$ to be the weighted count of the elements of $\text{Cov}(E, S)_{g,d}$ with the weighting defined above. As before, the data E and S are omitted from the notation, since $\widehat{N}_{g,d}$ will turn out not to depend on them.

Definition. The generating functions $Z(q, \lambda)$, respectively $\widehat{Z}(q, \lambda)$, for the quantities $N_{g,d}$, respectively $\widehat{N}_{g,d}$, are defined as follows:

$$Z(q, \lambda) = \sum_{g \geq 1} \sum_{d \geq 1} \frac{N_{g,d}}{(2g-2)!} q^d \lambda^{(2g-2)} = \sum_{g \geq 1} \frac{F_g(q)}{(2g-2)!} \lambda^{(2g-2)},$$

$$\widehat{Z}(q, \lambda) = \sum_{g \geq 1} \sum_{d \geq 1} \frac{\widehat{N}_{g,d}}{(2g-2)!} q^d \lambda^{(2g-2)}.$$

Lemma 3.3. *The generating functions are related by $\widehat{Z}(q, \lambda) = \exp(Z(Q, \lambda)) - 1$.*

Proof.

□

4. Classifying covers via the fundamental group

Let E be an elliptic curve, $S = \{b_1, \dots, b_{2g-2}\}$ a set of $2g - 2$ distinct points of E . Fix a basis point $b_0 \in E \setminus S$, and denote the fundamental group $\pi_1(E \setminus S, b_0)$ by π_1 . Recall the equivalence of categories from 2.1.:

$$\{\text{Unbranched covers of } E \setminus S\} \longrightarrow \{\pi_1\text{-sets}\}.$$

The goal of this section is to use this equivalence of categories to classify those π_1 -sets giving rise to unbranched covers that, after filling adding the branched points, become the covers we are interested in, i.e. the over S simply branched, genus g , degree d covers. To obtain natural π_1 -actions on the set of d fibre points of b_0 , it is convenient to introduce markings on the set of fibres.

4.1. Marked covers

Definition. A *marked (degree d , genus g , simply branched over S) cover* of E is a triple (C, p, m) , where $(C, p) \in \text{Cov}(E, S)_{g,d}$ and $m: p^{-1}(b_0) \rightarrow \{1, \dots, d\}$ is a bijective map, the *marking* of (C, p, m) .

Two marked covers (C_1, p_1, m_1) and (C_2, p_2, m_2) are considered equivalent, if there is an isomorphism of covers $\phi: C_1 \rightarrow C_2$ such that $m_1 = m_2 \phi$. Let $\widetilde{\text{Cov}}(E, S)_{g,d}$ denote the set of equivalence classes of marked covers with respect to this relation.

Definition. Denote the group operation of π_1 on the fiber of b_0 in any cover by $(\gamma, x) \mapsto \gamma \cdot x$. Define the monodromy map

$$\text{mon}: \widetilde{\text{Cov}}(E, S)_{g,d} \rightarrow \text{Hom}(\pi_1, S_d)$$

by $\text{mon}(C, p, m)(\gamma)(i) = m(\gamma \cdot m^{-1}(i))$.

5. Appendix A: Calculations

5.1. Quasimodular forms

Calculation 5.1. This calculation follows the one found in [1]. Let $F(\tau) = \sum_{m=1}^M f_m(\tau)Y^{-m}$ be an almost holomorphic modular form, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$, and $\tau \in \mathcal{H}$. Write $j = c\tau + d$, and $a = 6cj/2\pi i$. Then $Y^{-1}(\gamma\tau) = a + j^2Y(\tau)^{-1}$. Hence,

$$\begin{aligned} F(\gamma\tau) &= \sum_{m=1}^M f_m(\gamma\tau)(a + j^2Y^{-1})^m \\ &= \sum_{m=1}^M \sum_{l=0}^m \binom{m}{l} f_m(\gamma\tau) a^{m-l} j^{2l} Y^{-l} \\ &= \sum_{m=1}^M f_m(\gamma\tau) a^m + \sum_{l=1}^M \sum_{m=l}^M \binom{m}{l} f_m(\gamma\tau) a^{m-l} j^{2l} Y^{-l}. \end{aligned}$$

On the other hand,

$$F(\gamma\tau) = \sum_{l=1}^M f_l(\tau) j^k Y^{-l},$$

by the modularity condition. By comparing the coefficients of Y^{-l} , one obtains the equalities

$$\sum_{m=1}^M f_m(\gamma\tau) a^m = 0 \quad (1)$$

and

$$j^k f_l(\tau) = \sum_{m=l}^M \binom{m}{l} f_m(\gamma\tau) a^{m-l} j^{2l}.$$

Rewriting the second equality yields

$$f_l(\gamma\tau) = f_l(\tau) j^{k-2l} - \sum_{m=l+1}^M \binom{m}{l} f_m(\gamma\tau) a^{m-l}. \quad (2)$$

The latter may be solved recursively, starting by f_M , to get equalities of the form

$$f_l(\gamma\tau) = (\text{a polynomial in the } f_{\geq l}(\tau), j \text{ and } c). \quad (3)$$

The first two equalities are

$$\begin{aligned} f_M(\gamma\tau) &= f_M(\tau) j^{k-2M} \\ f_{M-1}(\gamma\tau) &= f_{M-1}(\tau) j^{k-2M+2} - \text{const} \cdot f_M(\tau) j^{k-2M+1} c. \end{aligned}$$

In general, a straightforward inductive argument shows that in the summands of the expression (2) for $f_l(\gamma\tau)$, the variable j appears with a power lower than or equal to $k - 2l$. Now let r be the greatest index such that $f_r \neq 0$. Equation (1) finally gives, after substituting back the expressions for j and a and using (2) for $l = r$, the relation

$$\begin{aligned} 0 &= \kappa_1 f_r(\gamma\tau)(c\tau + d)^r c^r + \sum_{l=r+1}^M \kappa_3 f_l(\gamma\tau)(c\tau + d)^l c^l \\ &= \kappa_1 f_r(\tau)(c\tau + d)^{k-r} c^r - \\ &\quad - \sum_{m=r+1}^M \kappa_2 \binom{m}{r} f_m(\gamma\tau)(c\tau + d)^{m-r} c^{m-r} + \sum_{l=r+1}^M \kappa_3 f_l(\gamma\tau)(c\tau + d)^l c^l, \end{aligned}$$

where the κ_i are some nonzero constants. To obtain a contradiction, choose a point τ in the upper half-plane and consider the last relation as a polynomial equation in c and d , letting $P(c, d)$ denote the right-hand side of the equation. First look for the possible coefficients of monomials of the form $c^r d^{\geq 1}$. This excludes the third summand from the picture, since there c will always appear with a power greater than r . Next look for the possible coefficients of the monomial $c^r d^{k-r}$. As seen when recursively solving the equations for $f_l(\gamma\tau)$, the second summand will include only terms where $(c\tau + d)$ appears with a power lower than $k - r$. Hence the coefficient of $c^r d^{k-r}$ in $P(c, d)$ is $\kappa_1 f_r(\tau)$.

Now, if $c \in \mathbb{Z}$, then there are infinitely many $d \in \mathbb{Z}$ such that $P(c, d) = 0$. Indeed, there are infinitely many d with $\gcd(c, d) = 1$. For these d , find $a, b \in \mathbb{Z}$ such that $ad - bc = 1$. Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, it follows that $P(c, d) = 0$. Similarly, for all $d \in \mathbb{Z}$, there are infinitely many c such that $P(c, d) = 0$. It thus follows that $P(c, d) = 0$ holds for all $c, d \in \mathbb{C}$. These remarks may be summarized by the statement that the set of all c, d belonging to the lower row of some matrix in $\mathrm{SL}_2(\mathbb{Z})$ is Zariski-dense in \mathbb{C}^2 .

Concluding, since P is zero as a function on \mathbb{C}^2 , it is also zero as a polynomial, hence the coefficient $\kappa_1 f_r(\tau)$ is zero. Since τ was arbitrary, one finds $f_r = 0$, a contradiction.

References

- [1] S. Bloch A. Okounkov. The character of the infinite wedge representation.
- [2] M. Kaneko D. Zagier. A generalized jacobi theta function and quasimodular forms.
- [3] J. P. Serre. *A Course in Arithmetic*.
- [4] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2nd edition, 2009.