Counting Covers of Elliptic Curves

Orlando

May 1, 2015

Contents

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 $\mathcal{H}$ satisfyting $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all τ in $\mathcal{H}$, and growing at most polynomially in $1/Y$ as $Y \to 0$.

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 $\bigoplus_k \mathrm{M}_k$ the structure of a graded ring, denoted by M_*.

Example. 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 $\sigma_{k-1}(n) = \sum_{m|n} m^{k-1}$. 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 $G_k(\tau) = \sum_{(a,b) \in \mathbb{Z}^2 \smallsetminus (0,0)} (a\tau + b)^{-k}$, which is indeed modular of weight k.

The theory of modular forms is developed in more detail in [Serre]. There one also finds a proof for the following proposition, which characterizes the space of modular forms.

Proposition 1. *There is an isomorphism of graded rings $\mathbb{C}[X_4, X_6] \to M_*$ mapping X to E_4 and Y to E_6, where the former ring is graded by assigning to X_i the degree i.*

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

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 [3].

2.1. Complex Curves

Proposition 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 [3] pp. 20-22. □

Proposition 3 (Riemann-Hurwitz formula)**.** *Let $\varphi\colon C_1 \to C_2$ be a finite, degree d map of smooth curves of genera g_1 and g_2, respectively. Then*

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

where $\mathrm{e}_\varphi(x)$ 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 $p\colon C \to E$ 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 $S = b_1, \ldots, b_{2g-2}$ 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 exacly one point x in $p^{-1}(b)$ with ramification index $\mathrm{e}_p(x) = 2$, the others having a ramification index of one.

   It follows from the Riemann-Hurwitz formula of Proposition 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 $C_1 \to C_2$ commuting with the respective structure maps into E. Accordingly, define the automorphism group $\mathrm{Aut}_p(C) = \mathrm{Aut}(C)$ of the cover (C, p) to be the group of cover isomorphisms $C \to C$.

Proposition 4. *Let C be a connected cover of E. Then the automorphism group of C is finite.*

Proof. By Proposition 2, if C is a degree d connected cover, the elements of $\mathrm{Aut}(C)$ correspond to the automorphisms of the degree d field extension $K(C)/K(E)$, of which only finitely many exist. □

Remark. The degree d connected covers of an elliptic curve E form a set. Indeed, they correspond by Proposition 2 to elements of the power set of the algebraic closure of $K(E)$.

Definition. Let E be an elliptic curve, $S = b_1, \ldots, b_{2g-2}$ 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 $\mathrm{Cov}(E, S)^\circ_{g,d}$.
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 $1/|\mathrm{Aut}_p(C)|$.
3. Define $N_{g,d}$ to be the weighted count

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

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 5 (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, $S = b_1, \ldots, b_{2g-2}$ a set of $2g-2$ distinct points of E.

1. A *(degree d, genus g,) cover* of E is a finite, degree d morphism $p \colon C \to E$ 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 $\mathrm{Aut}_p(C)$ 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 $C = C_1 \cup \cdots \cup C_k$ is the semidirect product

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

where $\Gamma \subset \mathrm{S}_k$ 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 $\mathrm{Aut}(C)$ into Γ which is the identity on Γ, viewed as a subset of $\mathrm{Aut}(C)$, having as kernel the product $\prod_i \mathrm{Aut}_{p_i}(C_i)$.

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 [3], 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, $S = b_1, \ldots, b_{2g-2}$ 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 $\mathrm{Cov}(E, S)_{g,d}$.
2. Assign to an element $[(C, p)]$ of $\mathrm{Cov}(E, S)_{g,d}$ the *weight* $1/\mathrm{Aut}_p(C)$. This is again well-defined.
3. Define $\hat{N}_{g,d}$ to be the weighted count of the elements of $\mathrm{Cov}(E, S)_{g,d}$ with the weighting defined above. As before, the data E and S are omitted from the notation, since $\hat{N}_{g,d}$ will turn out not to depend on them.

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

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

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

Lemma 6. *The generating functions are related by* $\hat{Z}(q, \lambda) = \exp(Z(Q, \lambda)) - 1$.

Proof. □

4. Appendix A: Calculations

4.1. Quasimodular Forms

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

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

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

$$\sum_{i=1}^{M} f_i(\gamma\tau) a^i = 0 \tag{1}$$

and

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

Rewriting the second equality yields

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

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

$$f_l(\gamma\tau) = (\text{a polynomial in the } f_{\geq l}(\tau)\ ,\ j \text{ and } c). \tag{2}$$

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

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

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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, 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 this 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. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2nd edition, 2009.