SINGULAR MODULI FOR A DISTINGUISHED NON-HOLOMORPHIC MODULAR FUNCTION

VALERIO DOSE, NATHAN GREEN, MICHAEL GRIFFIN,
TIANYI MAO, LARRY ROLEN, AND JOHN WILLIS

Abstract. Here we study the integrality properties of singular moduli of a special non-holomorphic function $\gamma(z)$ which was previously studied by Siegel [10], Masser [8], Bruinier, Sutherland, and Ono [3]. Similar to the modular $j$-invariant, $\gamma$ has algebraic values at any CM-point. We show that primes dividing the denominators of these values must have absolute value less than that of the discriminant and are not split in the corresponding quadratic field. Moreover we give a bound for the size of the denominator.

1. Introduction and statement of results

We first recall the famous modular $j$-function given explicitly by

$$j(\tau) := \frac{1 + 240 \sum_{n=1}^{\infty} \sum_{d|n} d^3 q^n}{q \prod_{n=1}^{\infty} (1 - q^n)^24} = q^{-1} + 744 + 196884q + 2149370q^2 + \ldots$$

where $q := e^{2\pi i \tau}$. The term singular moduli classically refers to values of the $j$-function at quadratic irrationalities, which for the remainder of this paper we will refer to as CM-points. These numbers are at the center of the beautiful subject known as complex multiplication, and they enjoy numerous important properties. More specifically, these singular moduli are algebraic integers, and they generate ring class fields for imaginary quadratic fields. Their minimal polynomials are therefore important in the study of explicit class field theory. These polynomials are known as the Hilbert class polynomial of discriminant $D$, and are defined as

$$H_D(j; X) := \prod_{Q \in SL_2(\mathbb{Z}) \setminus Q_D} (X - j(\alpha_Q)) \in \mathbb{Z}[X]$$

(for example, see [11] Ch. 6 and [9] Ch. 7). Here, $Q_D$ is the set of reduced, primitive, integral, binary quadratic forms of a fixed discriminant $D$; for a representative quadratic form $Q$, $\alpha_Q$ is the root of $Q(x, 1)$ in the upper half-plane. Gross and Zagier in [5] further give exact factorization formulas for the constant terms of $H_D(j; X)$ when the discriminant is fundamental, explaining the fact that they seem to be highly factorizable integers.
Analogous “class polynomials” may be defined for non-holomorphic modular functions. A natural first example is the function $\Psi(z)$ defined as follows:

\begin{equation}
\Psi(z) := \frac{E^*_2(z)E_4(z)}{E_6(z)},
\end{equation}

where

\begin{equation}
E^*_2(z) := 1 - \frac{3}{\pi \text{Im}(z)} - 24 \sum_{n=1}^{\infty} \sum_{d|n} dq^n
\end{equation}

is the usual weight 2 non-holomorphic Eisenstein series and where

\begin{equation}
E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \sum_{d|n} d^4 q^n, \quad E_6(z) := 1 - 504 \sum_{n=1}^{\infty} \sum_{d|n} d^6 q^n
\end{equation}

are the usual weight 4 and weight 6 Eisenstein series, respectively. This function has algebraic values at CM-points (see [11, Ch. 2]) and was previously studied by Siegel in [10] in connection with computing CM-values for $j'(z)$. Following Masser we will also define the normalized modular function

\begin{equation}
\gamma(z) := \frac{\Psi(z)}{6j(z)} - \frac{7j(z) - 6912}{6j(z)(j(z) - 1728)}.
\end{equation}

This function was important in [6] and [3], and its singular moduli were first studied in Masser ([8, App. 1]).

As mentioned above, for any level 1 modular function $f$ we may define an analogue of the “class polynomial”,

\begin{equation}
H_D(f; X) := \prod_{Q \in \text{SL}_2(\mathbb{Z}) \backslash \mathbb{Q}_D} (X - f(\alpha_Q)) \in \mathbb{Q}[X].
\end{equation}

We will generally refer to these polynomials simply as class polynomials. It is suspected, but not yet proven, that for some nonholomorphic modular functions, including $\Psi$ and $\gamma$, these polynomials generate the appropriate ring class fields. The following table gives the class polynomials $H_D(\gamma; X)$ and $H_D(\Psi; X)$ for several small discriminants:
Several phenomena are apparent from this table. For example, the denominators appear to be “highly factorizable.” In fact, it appears that the primes appearing in the denominators are bounded by the size of the discriminant. This suggests that a Gross-Zagier type phenomenon occurs, but now for the denominators of the constant terms of the class polynomials rather than for the constant terms as a whole. Based on numerics, Ono and Sutherland proposed the following:

**Conjecture 1** (Ono-Sutherland). Let $D$ be a negative discriminant, not equal to $-4$. Then if $p > -D$ or if $p$ splits in $\mathbb{Q}(\sqrt{D})$, we have that $H_D(\gamma; X)$ and $H_D(\Psi; X)$ are $p$-integral.

We remark that throughout the paper, when we refer to a split, inert or ramified prime, we mean that the prime is such in the appropriate quadratic field for the discriminant in question. Our main result is the proof of this conjecture.

**Theorem 1.1.** The conjecture of Ono and Sutherland is true.

**Remark.** The relation between $\Psi$ and $\gamma$ given in equation (1.6) will play a crucial role in the proof of Theorem 1.1. The fact that the denominators in $H_D(\Psi; X)$ are in general simpler than those in $H_D(\gamma; X)$ should be apparent from (1.6). In particular $\Psi$ is, in many ways, a more basic modular function than is $\gamma$. 
The paper is organized as follows. In §2 we review relevant background information including the formulas of Masser on singular moduli for \(\gamma(z)\), the formula of Gross and Zagier. In §3 we complete the proof of 1.1 by combing the cited results in §2 along with results from the theory of reduced binary quadratic forms, basic elliptic curve theory, and Deuring lifting theory.

ACKNOWLEDGMENTS

This project was completed as part of the Arizona Winter School. The authors wish to thank the organizers of the winter school for their generous support. The authors also wish to thank Ken Ono for his advisement throughout the project. We are also grateful to Andrew Sutherland for providing SAGE code and extensive numerical data which supported the conjectures studied here.

2. Nuts and bolts

Here we review some important facts which we need in the proof of Theorem 1.1

2.1. Masser’s Formulas. Our starting point is an elegant formulation due to Masser in [8, App. 1]. His careful study of \(\Psi\) and \(\gamma\) yields two formulas for singular moduli of these functions in terms of modular polynomials and elliptic curves which we require. The first concerns the function \(\gamma(z)\). We begin by reviewing the definition of the classical modular polynomial \(\Phi_D\).

Definition 2.1. We say that two matrices \(B_1\) and \(B_2\) are equivalent if \(B_1 = X \cdot B_2\) for some \(X \in \text{SL}_2(\mathbb{Z})\).

It is well-known that there are only finitely many equivalence classes of primitive integer matrices of determinant \(-D\). Write \(M_1, M_2, \ldots, M_n\) for representatives of these equivalence classes and suppose \(M_1\) is such that \(\alpha_Q = M_1\alpha_Q\), where the action of a matrix on a complex number is given by Möbius transformation.

Definition 2.2. We write \(\Phi_D(X, Y)\) for the classical modular polynomial, i.e. the polynomial such that

\[
\Phi_D(j(z), Y) = \prod_{i=1}^{n}(Y - j(M_i z)).
\]

By [2], Theorem 1 of Section 3.4, the polynomial \(\Phi_D(X, Y)\) is symmetric in \(X\) and \(Y\) and has coefficients that are rational integers. In particular, we can expand \(\Phi_D(X, Y)\) in a power series about \(X = Y = j(\alpha_Q)\) as

\[
\Phi(X, Y) = \sum_{\mu, \nu} \beta_{\mu, \nu}(X - j(\alpha_Q))^\mu(Y - j(\alpha_Q))^\nu,
\]

where \(\beta_{\mu, \nu} = \beta_{\nu, \mu}\). We write \(\beta = \beta_{0,1} = \beta_{1,0}\).
We define $Q$ to be special if there is more than one equivalence class of matrices $M$ such that $M\alpha_Q = \alpha_Q$. This can only happen if $-D = 3d^2$ for some integer $d$ (see [8, App. 1]).

**Lemma 2.1** (Masser). If $Q$ is not special, we have $\beta \neq 0$ and

\begin{equation}
\gamma(\alpha_Q) = \frac{\beta_{0,2} - \beta_{1,1} + \beta_{2,0}}{\beta}.
\end{equation}

If $Q$ is special, we have $\beta \neq 0$ and

\begin{equation}
\gamma(\alpha_Q) = \frac{\beta_{4,0} - \beta_{3,1} + \beta_{2,2} - \beta_{1,3} + \beta_{0,4}}{\beta}.
\end{equation}

**Proof.** See [8, App. 1] (in particular, the equations on page 118). \hfill \Box

By definition, the $\beta_{\mu,\nu}$ are algebraic integers. Thus, to study integrality of $\gamma(\alpha_Q)$ it suffices to study the primes dividing $\beta$. From the definition of $\beta$, we have

\begin{equation}
\beta = \prod_{i=2}^{n}(j(\alpha_Q) - j(M_i\alpha_Q)).
\end{equation}

We will later use this result to eliminate split primes by studying lifting of isomorphisms of elliptic curves over $\mathbb{F}_p$ to $\mathbb{Q}$.

In order to show that large primes cannot divide the denominators of our class polynomials, and to study bounds for the powers of primes appearing, we will find another formula of Masser convenient.

**Lemma 2.2** (Masser). Let $\tau$ be a CM point of discriminant $D$ for $4 < -D$ and $A, B, C$ integers such that $A\tau^2 + B\tau + C = 0$. Then we have that

\begin{equation}
\Psi(\tau) = -\frac{g_2S}{g_3A(2C + B\tau)}.
\end{equation}

Here, $g_2$ and $g_3$ are the usual invariants of the associated CM-elliptic curve (the non-normalized Eisenstein series), and $S$ is the sum of $C\tau$-division values of the Weierstrass $\wp$-function (We note that Masser defines the coefficients such that $C\tau^2 + B\tau + A = 0$).

### 2.2. The Gross-Zagier Formula.

Gross and Zagier [5] give an exact formula for the factorizations of the constant terms of the Hilbert class polynomials $H_D(j; X)$ when $D$ is fundamental. In fact their result is more general. For two coprime discriminants $D_1, D_2$, let $w_i$ be the number of roots of unity in the quadratic order of discriminant $d_i$ for $i = 1, 2$. Consider the norm of difference of singular moduli defined by

\begin{equation}
J(D_1, D_2) := \left( \prod (j(\tau_1) - j(\tau_2)) \right)^{\frac{4}{w_1w_2}},
\end{equation}
where \( \text{disc}(\tau_i) = D_i \) and \( \tau_i \) run through representatives of \( \text{SL}_2(\mathbb{Z}) \backslash \mathcal{Q}_{D_i} \). Then for primes \( \ell \) with \( \left( \frac{D_1 D_2}{\ell} \right) \neq -1 \) define

\[
\epsilon(\ell) := \begin{cases} 
\left( \frac{D_1}{\ell} \right) & \text{if } (D_1, \ell) = 1 \\
\left( \frac{D_2}{\ell} \right) & \text{if } (D_2, \ell) = 1
\end{cases}
\]

We extend this definition to natural numbers by setting \( \epsilon(\prod_i \ell_i^{n_i}) := \prod_i \epsilon(\ell_i)^{n_i} \) if \( \left( \frac{D_1 D_2}{\ell_i} \right) \neq -1 \) for all \( i \). Their main result is the following factorization.

**Theorem 2.1** (Gross-Zagier [5]). Suppose \( (D_1, D_2) = 1 \) are negative fundamental discriminants. Then

\[
J(D_1, D_2)^2 = \pm \prod_{x, n, n' \in \mathbb{Z} \atop n, n' > 0 \atop x^2 + 4nn' = -D_1 D_2} n^{\epsilon(n')}.
\]

We are particularly interested in the following corollary.

**Corollary 2.3** (Gross-Zagier [5]). For \( \ell \) a rational prime dividing \( J(D_1, D_2)^2 \), we have that \( \left( \frac{D_1}{\ell} \right) \neq 1 \), \( \left( \frac{D_2}{\ell} \right) \neq 1 \), and \( \ell < \frac{D_1 D_2}{4} \).

For our proof, we will need a generalization to the case when \( D_1 \) and \( D_2 \) are distinct, but not necessarily coprime. Lauter and Viray [7] prove a generalized Gross-Zagier type formula for exactly this case. In particular, their Corollary 1.3 implies as a special case the following:

**Theorem 2.2** (Lauter-Viray, Corollary of Corollary 1.3 of [7]). Suppose \( D_2 = -3 \) or \( -4 \), and \( D_1 \) is a negative discriminant not equal to \( D_2 \). Then for \( \ell \) a rational prime dividing \( J(D_1, D_2) \), we have \( \ell \leq -D_1 \).

### 3. Proof of Theorem 1.1

The proof of Theorem 1.1 involves two pieces. We first show in Section 3.1 that split primes do not appear in the denominators of \( H_D(\gamma; X) \) and \( H_D(\Psi; X) \). Then in Section 3.2 we bound the size of prime divisors.


The aim of this section is to prove the following:

**Theorem 3.1.** Let \( D \) be a negative discriminant not \(-4\). If \( p \) splits in \( \mathbb{Q}(\sqrt{D}) \), we have that \( H_D(\gamma; x) \) and \( H_D(\Psi; x) \) are \( p \)-integral.

**Proof.** We prove the result for \( \gamma \). By (1.6) and Theorem 2.2 it applies to \( \Psi \) as well. When \( D = -3 \), the result reduces to a calculation. Thus we may assume \( D < -3 \). We begin with Masser’s result, given in Lemma 2.1. As each \( \beta_{\mu, \nu} \) is an algebraic integer, it suffices in both the special and the non-special case to show that split primes cannot divide \( \beta_{0,1} = \beta \). By the expression for \( \beta \) as a product of differences of \( j \)-values (2.5), it suffices to show that if \( p \) is a split prime and \( p \) is a prime above \( p \) in \( \mathbb{Q}(\sqrt{D}) \) that \( j(\alpha_Q) \neq j(\alpha_Q') \)
(mod $p$) for $\alpha_Q$ not SL$_2(\mathbb{Z})$-equivalent to $\alpha_Q'$. This is exactly the situation of Lemma 3.2 of [6], which is also stated in Theorem 13.21 of [4], and is essentially a result of Deuring lifting theory.

3.2. Large Primes. In order to finish the proof of Theorem 1.1, it suffices to show the following:

**Theorem 3.2.** Let $D$ be a negative discriminant not $-4$, and $p$ a prime such that $p > -D$. Then $H_D(\gamma; x)$ and $H_D(\Psi; x)$ are $p$-integral.

**Proof.** We prove the result for $\Psi$. By (1.6) and Theorem 2.2, it applies to $\gamma$ as well. As above, the case when $D = -3$ is a calculation. We may therefore assume $D < -3$. By (1.6), it suffices to consider primes dividing the denominators of singular moduli for $\Psi(z)$ and $j(z) \cdot (j(z) - 1728)$. Suppose $\ell > -D$ is a rational prime. By Theorem 2.2, the factor $j(z)(j(z) - 1728)$ is not divisible by $\ell$, as it is well-known that

$$j(i) = 1728, \quad j(e^{2\pi i/3}) = 0.$$ (3.1)

Thus, it suffices to show that $\ell$ does not divide the denominator of $\Psi(\tau)$. For this, we use Masser’s formula for $\Psi(\alpha_Q)$ given in Lemma 2.2. We will first consider the term $A(2C + B\tau)$ which appears in the denominator of (2.6). A short calculation shows that $(2C + B\tau)$ has norm $\frac{-DC}{A}$. Every integral, binary quadratic form is SL$_2(\mathbb{Z})$-equivalent to a unique form with “smallest” coefficients, which we refer to as the reduced form. We recall that an integral, binary quadratic form $Q = [A, B, C] = AX^2 + BXY + CY^2$ of negative discriminant is reduced if $|B| \leq A \leq C$ and if $B \geq 0$ whenever $A = |B|$ or $A = C$. Masser’s formula requires $A, B, C > 0$. If $B > 0$, we may use this form and the inequalities quickly give us the bounds

$$B \leq A \leq \sqrt{-\frac{D}{3}}, \quad \text{and} \quad C \leq -\frac{D}{3},$$ (3.2)

which implies that the norm of $A(2C + B\tau)$ is bounded by $\frac{D^2}{3}$.

If the reduced form has $B < 0$, we may transform the reduced form $Q$ by $\left( \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right)$, which changes the sign of $B$ and swaps $A$ and $C$.

If $B = 0$, we have that $-D = 4AC$, and so we have improved bounds

$$A < \frac{\sqrt{-D}}{2} \quad \text{and} \quad C \leq -\frac{D}{4},$$ (3.3)

which is easily shown to be sufficient after a short calculation.

Now $g_2$ and $g_3$ correspond to our model of the elliptic curve determined by $\tau$, and may be varied by scaling the model. Hence, using that

$$j(\tau)\Delta = 12^3 \cdot g_2^3 \quad \text{and} \quad (j(\tau) - 1728) \cdot \Delta = g_3^2,$$ (3.4)
we see that for an appropriate choice of $\Delta$, we may take $g_2$ and $g_3$ to be algebraic integers divisible only by primes dividing $12j(\tau)(j(\tau) - 1728)$. By Theorem 2.2 above, this gives the desired bound for the size of the primes.

It remains only to control the denominators from the term $S$. Having chosen $g_2$ and $g_3$ as above, we have by Lemma 4 of [1] that the numbers $(AC)^2\wp(\tau)$ are algebraic integers. However we have already bounded the primes dividing $AC$. This concludes the proof. □

REFERENCES
