PRINCIPAL MODULI AND CLASS FIELDS

DAVID COX, JOHN McKAY, AND PETER STEVENHAGEN

Abstract. We study the values taken by $\Gamma_0(n)$-modular functions at elliptic points of order 2 for the Fricke group $\Gamma_0(n)^\dagger$. In the case of a principal modulus ('Hauptmodul') for $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$, we determine the class fields generated by these values.

1. Introduction

The Fricke group $\Gamma_0(n)^\dagger$ of level $n > 1$ is the subgroup of $\mathrm{PSL}_2(\mathbb{R})$ generated by the congruence subgroup $\Gamma_0(n) \subset \mathrm{PSL}_2(\mathbb{Z})$ and the Fricke involution $w_n = \sqrt{n}\begin{pmatrix} 0 & -\frac{1}{n} \\ 1 & 0 \end{pmatrix}$, which acts on the upper half plane $\mathfrak{h}$ by $w_n(\tau) = \frac{-1}{n\tau}$. As explained in [2, Section 4], $\Gamma_0(n)^\dagger$ is a subgroup of the full normalizer $\Gamma_0(n)^+$ of $\Gamma_0(n)$ in $\mathrm{PSL}_2(\mathbb{R})$, which may be generated over $\Gamma_0(n)$ by a finite number of Atkin-Lehner involutions. The subgroup $\Gamma_0(n)$ has index 2 in $\Gamma_0(n)^\dagger$, and the elements of the coset $\Gamma_0(n)^\dagger \setminus \Gamma_0(n)$ are the matrices $\sqrt{n}\begin{pmatrix} A & \frac{B}{n} \\ C & D \end{pmatrix} \pmod{\pm 1}$ with $A, B, C, D \in \mathbb{Z}$ satisfying $nAD - BC = 1$. Such a matrix is elliptic of order 2 if and only if it has trace 0, i.e., if it is represented by

$$\alpha = \sqrt{n}\begin{pmatrix} A & \frac{B}{n} \\ C & -A \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \tag{1.1}$$

with $nA^2 + BC = -1$. We always pick α in (1.1) in such a way that we have $B < 0$ and $C > 0$. Then the fixed point of α in $\mathfrak{h}$ is the element

$$\tau_\alpha = \frac{nA + \sqrt{-n}}{nC} \in \mathfrak{h}, \tag{1.2}$$

which is a zero of the polynomial

$$f_\alpha = nCX^2 - 2nAX - B \in \mathbb{Z}[X] \tag{1.3}$$

1991 *Mathematics Subject Classification.* Primary 10D12, 11R37; Secondary 11G15, 20D08, 20H10.

of discriminant $4n(nA^2 + BC) = -4n$. As B is coprime to nA, the polynomial f_α is irreducible in $\mathbb{Z}[X]$ unless B and C are both even. In the latter case we have $n = (-1 - BC)\frac{1}{A^2} \equiv 3 \bmod 4$, and $\frac{1}{2}f_\alpha$ is irreducible in $\mathbb{Z}[X]$ of discriminant $-n$. It follows (cf. [3, Thm. 7.7]) that the complex lattice

$$I_\alpha = [\tau_\alpha, 1] = \frac{1}{nC}[nA + \sqrt{-n}, nC] \subset \mathbb{C} \tag{1.4}$$

corresponding to the fixed point of α is an invertible ideal for the quadratic order $\mathcal{O}_\alpha = \{\lambda \in \mathbb{C} : \lambda I_\alpha \subset I_\alpha\}$, which has discriminant $-n$ if B and C are both even, and discriminant $-4n$ otherwise. More explicitly, we have

$$\mathcal{O}_\alpha = \begin{cases} \mathbb{Z}[\frac{-n+\sqrt{-n}}{2}] & \text{for } n \equiv 3 \bmod 4,\ B \text{ and } C \text{ even} \\ \mathbb{Z}[\sqrt{-n}] & \text{otherwise.} \end{cases} \tag{1.5}$$

The goal of this paper is to study the Galois theoretic properties of the values $f(\tau_\alpha)$ over $\mathbb{Q}(\tau_\alpha)$ when f is a $\Gamma_0(n)$-modular function and α is an elliptic element of order 2 in $\Gamma_0(n)^\dagger \setminus \Gamma_0(n)$. If f is modular for the full modular group $\mathrm{PSL}_2(\mathbb{Z})$ and has rational q-expansion, i.e., if f is an element of the field $\mathbb{Q}(j)$ of modular functions of level 1, then the classical theory of complex multiplication tells us that if $f(\tau_\alpha)$ is finite, then it is contained in the ring class field of the order $\mathcal{O}_\alpha$. This class field is an abelian extension of $\mathbb{Q}(\tau_\alpha) = \mathbb{Q}(\sqrt{-n})$, and its Galois group over $\mathbb{Q}(\tau_\alpha)$ is canonically isomorphic under the Artin isomorphism to the ideal class group $C(\mathcal{O}_\alpha)$ of the order $\mathcal{O}_\alpha$. We will write σ_α for the automorphism corresponding to the ideal class $[I_\alpha] \in C(\mathcal{O}_\alpha)$.

For $f \in \mathbb{Q}(j)$ of level 1 as above, it is a classical result that we have $\sigma_\beta\big(f(\tau_\alpha)\big) = f(\tau_\gamma)$ when α, β and γ are elliptic elements as in (1.1) satisfying $\mathcal{O}_\alpha = \mathcal{O}_\beta = \mathcal{O}_\gamma$ and $[I_\alpha I_\beta^{-1}] = [I_\gamma] \in C(\mathcal{O}_\alpha)$.

Our main result below shows that $\Gamma_0(n)$-modular functions behave like level 1 functions when evaluated at the elliptic points of order 2 of the Fricke group $\Gamma_0(n)^\dagger$. The proof given in Section 3 uses the Shimura reciprocity law [11, Thm. 6.31] as explained in [5, 12].

Theorem 1.1. *Fix $n > 1$ and let f be a $\Gamma_0(n)$-modular function with rational q-expansion at ∞. Also let α be an elliptic element of order 2 in $\Gamma_0(n)^\dagger \setminus \Gamma_0(n)$ as in (1.1), and assume that f is defined at τ_α. Then:*

(1) *$f(\tau_\alpha)$ lies in the ring class field of $\mathcal{O}_\alpha$.*
(2) *Let β, γ be elliptic elements as in (1.1) with $\mathcal{O}_\alpha = \mathcal{O}_\beta = \mathcal{O}_\gamma$, and suppose $[I_\alpha I_\beta^{-1}] = [I_\gamma] \in C(\mathcal{O}_\alpha)$. Then we have*

$$\sigma_\beta\big(f(\tau_\alpha)\big) = f(\tau_\gamma).$$

Our motivation for proving Theorem 1.1 goes back to the special case where f is a principal modulus ('Hauptmodul') of the kind that arises in the moonshine conjectures for the monster group [2] and its generalizations to replicable functions [4]. These principal moduli are known to correspond to genus zero subgroups of $\mathrm{PSL}_2(\mathbb{R})$ that lie between $\Gamma_0(n)$ and its normalizer $\Gamma_0(n)^+$ for some n. In Section 4 we apply Theorem 1.1 to this situation, and explain how our results relate to those of Chen and Yui [1]. The main corollary, which is proved in Section 4, is the following.

Corollary 1.2. *Fix $n > 0$ and let f be a principal modulus with rational q-expansion at ∞ for either $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$. Suppose that f is defined at the fixed point τ_α from (1.2). Then $\mathbb{Q}(\tau_\alpha, f(\tau_\alpha))$ is the ring class field of the order $\mathcal{O}_\alpha$.*

2. Ideals, Quadratic Forms, and Conjugacy Classes

This section collects what we need about the ideals I_α arising in (1.4) and their classes in $C(\mathcal{O}_\alpha)$. While part of this material is well known (see [7, 8]), we include the details for the convenience of the reader.

In (1.3), we denoted by f_α the quadratic polynomial in $\mathbb{Z}[X]$ having the fixed point τ_α of the elliptic element α as one of its zeroes. Its homogeneous form

$$F_\alpha(x, y) = nCx^2 - 2nAxy - By^2 \in \mathbb{Z}[x, y] \tag{2.1}$$

is a binary quadratic form of discriminant $-4n$. Since we take $B < 0$ and $C > 0$, the form F_α is positive definite. Depending on the case we are in in (1.5), either F_α or $\frac{1}{2}F_\alpha$ is primitive of discriminant $\mathrm{disc}(\mathcal{O}_\alpha) \in \{-n, -4n\}$. Under the standard bijection [3, Thm. 7.7] between the set of $\mathrm{SL}_2(\mathbb{Z})$-orbits of primitive positive definite binary quadratic forms of discriminant $\mathrm{disc}(\mathcal{O}_\alpha)$ and the class group $C(\mathcal{O}_\alpha)$, this primitive form corresponds to the ideal class $[I_\alpha] \in C(\mathcal{O}_\alpha)$.

Lemma 2.1. *Let α and α' be as in* (1.1)*. Then the quadratic forms F_α and $F_{\alpha'}$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent if and only if α and α' are conjugate in $\Gamma_0(n)^\dagger$. If α and α' are conjugate in $\Gamma_0(n)^\dagger$, there exists $\delta \in \Gamma_0(n)$ with $\delta^{-1}\alpha\delta = \alpha'$.*

Proof. Let M_α denote the matrix representing the form α from (2.1):

$$M_\alpha = \begin{pmatrix} nC & -nA \\ -nA & -B \end{pmatrix} = \sqrt{n}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\alpha.$$

Since every $\delta \in \mathrm{SL}_2(\mathbb{Z})$ satisfies

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\delta^t\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \delta^{-1},$$

we have

$$\delta^t M_\alpha \delta = M_{\alpha'} \Longleftrightarrow \delta^{-1}\alpha\delta = \alpha'.$$

When F_α and $F_{\alpha'}$ are equivalent via $\delta \in \mathrm{SL}_2(\mathbb{Z})$, working modulo n gives

$$\delta^t\begin{pmatrix} 0 & 0 \\ 0 & -B \end{pmatrix}\delta \equiv \begin{pmatrix} 0 & 0 \\ 0 & -B' \end{pmatrix} \bmod n.$$

If $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, this easily implies

$$-Bc^2 \equiv -Bcd \equiv 0 \bmod n.$$

Since $\gcd(B, n) = \gcd(c, d) = 1$ (because $\det(\alpha) = \det(\delta) = 1$), we see that $c \equiv 0 \bmod n$, so that $\delta \in \Gamma_0(n)$. Then the above equivalence implies that α and α' represent conjugate elements in $\Gamma_0(n)^\dagger$.

Conversely, suppose we have $\alpha' = \pm\delta^{-1}\alpha\delta$ (remember that conjugacy classes are computed in $\Gamma_0(n)^\dagger \subset \mathrm{PSL}_2(\mathbb{R})$). If δ represents an element of $\Gamma_0(n)$, then the above equivalence shows that F_α and $\pm F_{\alpha'}$ are properly equivalent, and the sign must be $+$ since F_α and $F_{\alpha'}$ are positive definite. The final statement of the lemma says that this is the only case we need to consider. Indeed, if δ represents an element of $\Gamma_0(n)^\dagger \setminus \Gamma_0(n)$, then $\alpha^{-1}\delta$ represents an element of $\Gamma_0(n)$ since $\Gamma_0(n)$ has index 2 in $\Gamma_0(n)^\dagger$, and we may replace δ by $\alpha^{-1}\delta$:

$$\alpha' = \pm\delta^{-1}\alpha\delta = \pm(\alpha^{-1}\delta)^{-1}\alpha(\alpha^{-1}\delta).$$

This completes the proof of the lemma. $\square$

It follows from Lemma 2.1 that $\Gamma_0(n)$-modular functions have a well-defined value on the $\Gamma_0(n)^\dagger$-orbits of the fixed points in (1.2), and that elliptic elements α, β in (1.1) with $\mathcal{O}_\alpha = \mathcal{O}_\beta$ are conjugate in $\Gamma_0(n)^\dagger$ if and only if σ_α and σ_β coincide on the ring class field of $\mathcal{O}_\alpha$.

Our main result (Theorem 1.1) gives a Galois action in terms of Artin automorphisms σ_α corresponding to the ideal classes $[I_\alpha]$. It is therefore useful to know that every ideal class in $C(\mathcal{O}_\alpha)$ is of this form.

Lemma 2.2. *Let n be a positive integer and fix $\mathcal{O}$ to be either $\mathbb{Z}[\sqrt{-n}]$ or $\mathbb{Z}[\frac{n+\sqrt{-n}}{2}]$, where in the latter case we assume $n \equiv 3 \bmod 4$. Then the ideals $I_\alpha = \frac{1}{nC}[nA + \sqrt{-n}, nC]$ from(1.4) with $\mathcal{O}_\alpha = \mathcal{O}$ represent all ideal classes in the ideal class group $C(\mathcal{O})$.*

Proof. It suffices to show that a primitive positive definite quadratic form G of discriminant $D = -4n$, or $D = -n$ with $n \equiv 3 \bmod 4$, is properly equivalent to F_α or $\frac{1}{2}F_\alpha$ respectively. By [3, Lemmas 2.3 and 2.25], we may assume that $G(x,y) = ax^2 + bxy + cy^2$ has $\gcd(c, D) = 1$.

First suppose that $D = -4n$. Since b is even in this case, we can find an integer k such that

$$ck \equiv -b/2 \bmod n.$$

Using this k to replace $G(x,y)$ with the equivalent form

$$G(x, y + kx) = (a + bk + ck^2)x^2 + (b + 2kc)xy + cy^2, \tag{2.2}$$

we may assume that b is divisible by $2n$. Then $-4n = b^2 - 4ac$ and $\gcd(c, -4n) = 1$ imply that a is divisible by n. It follows that G is of the form F_α, as desired.

Next assume $D = -n$ and $n \equiv 3 \bmod 4$. Then we can find k such that

$$2ck \equiv -b \bmod n.$$

Using this k and (2.2), we may assume that b is divisible by n. Since n is odd, $-n = b^2 - 4ac$ and $\gcd(c, -n) = 1$ imply that a is divisible by n. Then $G = \frac{1}{2}F_\alpha$ follows easily. $\square$

For $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$, the form $F_\alpha = nx^2 + y^2$ corresponding to the principal ideal generated by $\tau = \frac{-1}{\sqrt{-n}}$ is in the unit class in $C(\mathcal{O})$. For $\mathcal{O} = \mathbb{Z}[\frac{-n+\sqrt{-n}}{2}]$, we can start from $G(x,y) = \frac{n+1}{4}x^2 + xy + y^2$ in the unit class and apply the proof of (2.2) (with $k = \frac{n-1}{2}$) to obtain the element $F_\alpha(x,y) = \frac{n(n+1)}{4}x^2 + nxy + y^2$ in the unit class. It corresponds to the principal ideal generated by $\tau = \frac{-2n+2\sqrt{-n}}{n(n+1)}$. Note that in both cases, $\tau\mathcal{O}$ is the lattice $[\tau, 1]$.

3. Proof of the Main Theorem

We now prove Theorem 1.1 using the method explained in [12].

Let f be a modular function for $\Gamma_0(n)$ with rational q-expansion and assume that f is defined at the fixed point τ_α from (1.2). Our first task is to show that $f(\tau_\alpha)$ lies in the ring class field of $\mathcal{O}_\alpha$. We first do this when the corresponding ideal I_α is in the unit class in $C(\mathcal{O}_\alpha)$. This leads to the following special choice for $\tau = \tau_\alpha$ and in each of the two cases for $\mathcal{O} = \mathcal{O}_\alpha$ provided by (1.5).

	n	α	τ	$\mathcal{O}$
Case 1	arbitrary	$\sqrt{n}\begin{pmatrix} 0 & -\frac{1}{n} \\ 1 & 0 \end{pmatrix}$	$\frac{-1}{\sqrt{-n}}$	$\mathbb{Z}[n\tau]$
Case 2	$n \equiv 3 \bmod 4$	$\sqrt{n}\begin{pmatrix} 1 & -\frac{2}{n} \\ \frac{n+1}{2} & -1 \end{pmatrix}$	$\frac{-2n+2\sqrt{-n}}{n(n+1)}$	$\mathbb{Z}[\frac{n(n+1)}{4}\tau]$

Standard results in complex multiplication imply that $f(\tau)$ lies in the maximal Abelian extension K^{ab} of $K = \mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-n})$. Class field theory describes the absolute abelian Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ as the surjective image under the Artin map of the group $\widehat{K}^* = (K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^*$ of finite K-ideles. In order to show that $f(\tau)$ lies in the ring class field $H_{\mathcal{O}}$ of $\mathcal{O}$, it suffices to show that every automorphism of K^{ab} over $H_{\mathcal{O}}$ leaves $f(\tau)$ invariant. As $\mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$ is the image under the Artin map of the subgroup $\widehat{\mathcal{O}}^* = (\mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^* \subset \widehat{K}^*$, we need to show that the Artin symbol any idele $x \in \widehat{\mathcal{O}}^*$ leaves $f(\tau)$ invariant.

Shimura's reciprocity law tells us how (the Artin symbol of) the idele $x \in \widehat{\mathcal{O}}^*$ acts on $f(\tau)$: we have

$$f(\tau)^x = f^{g_\tau(x^{-1})}(\tau), \tag{3.1}$$

where $g_\tau : \widehat{\mathcal{O}}^* \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the map that sends $x \in \widehat{\mathcal{O}}^*$ to the transpose of the matrix of multiplication by x on the free $\widehat{\mathbb{Z}}$-module $\widehat{\mathbb{Z}}\tau + \widehat{\mathbb{Z}}$ with respect to the basis $\{\tau, 1\}$. From the irreducible polynomial of τ in $\mathbb{Z}[X]$ one easily computes g_τ as in [12, (3.3)] to be

$$g_\tau(x) = g_\tau(a + bn\tau) = \begin{pmatrix} a & -b \\ nb & a \end{pmatrix} \tag{3.2}$$

for the order $\mathcal{O} = \mathbb{Z}[n\tau]$ in Case 1, and

$$g_\tau\big(a + b\tfrac{n(n+1)}{4}\tau\big) = \begin{pmatrix} a - nb & -b \\ \frac{n(n+1)}{4}b & a \end{pmatrix} \tag{3.3}$$

for the order $\mathcal{O} = \mathbb{Z}[\frac{n(n+1)}{4}\tau]$ in Case 2. In both cases, the matrix $g_\tau(x)$ is upper triangular modulo n for every choice of $x \in \widehat{\mathcal{O}}^*$. This means that modulo n, it is a product

$$M_1 M_2 = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} M_2 \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where M_2 is the reduction modulo n of a matrix from $\Gamma_0(n)$. But M_2 acts trivially on f since f is a modular function for $\Gamma_0(n)$, and M_1, which acts on f via its Fourier coefficients, also acts trivially since the q-expansion is rational. It follows that f is invariant under $\widehat{\mathcal{O}}^*$, so that

$f(\tau)$ lies in the desired ring class field $H_{\mathcal{O}}$. In particular, the class group $C(\mathcal{O})$, which is naturally isomorphic to the Galois group $\mathrm{Gal}(H_{\mathcal{O}}/K)$ under the Artin map, now acts on $f(\tau)$.

Our next task is to show that for elliptic elements β and γ satisfying $\mathcal{O}_\beta = \mathcal{O}_\gamma = \mathcal{O}$ and $[I_\beta^{-1}] = [I_\gamma] \in C(\mathcal{O})$, the Galois action of σ_β on $f(\tau)$ is in each of the two cases given by

$$\sigma_\beta(f(\tau)) = f(\tau_\gamma). \tag{3.4}$$

This shows that we have $\sigma_\gamma(f(\tau_\gamma)) = f(\tau)$ for all $f(\tau_\gamma)$ with γ as in (1.1) having $\mathcal{O}_\gamma = \mathcal{O}$. In particular, all these values $f(\tau_\gamma)$ are conjugate over K as soon as one of them is known to be finite, and one easily derives the second statement in (1.1) from (3.4). We may therefore finish the proof of (1.1) by proving (3.4).

To prove (3.4), we apply (3.1) once more, with $x \in \widehat{K}^*$ an $\widehat{\mathcal{O}}$-generator of $\widehat{I}_\gamma = I_\gamma \otimes \widehat{\mathbf{Z}}$ and $g_\tau : \widehat{K}^* \to \mathrm{GL}_2(\widehat{\mathbb{Q}})$ the natural $\mathbb{Q}$-linear extension of the map $g_\tau : \widehat{\mathcal{O}}^* \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ we had before. As in [12, Section 6], we let $M \in \mathrm{GL}_2^+(\mathbb{Q})$ be the transpose of a matrix mapping the lattice $[\tau, 1] = \tau\mathcal{O}$ to the lattice τI_γ. Write $I_\gamma = \frac{1}{nC}[nA+\sqrt{-n}, nC]$ as in (1.4). In Case 1 we have $\tau\sqrt{-n} = -1$, so

$$\tau I_\gamma = \tau[\tfrac{nA+\sqrt{-n}}{nC}, 1] = [\tfrac{nA\tau-1}{nC}, \tau],$$

and we can take $M \in \mathrm{GL}_2^+(\mathbb{Q})$ to be

$$M = \begin{pmatrix} A/C & -1/nC \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1/C & A/C \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1/n \\ 1 & 0 \end{pmatrix}.$$

In Case 2 our element τ satisfies $\tau(n + \sqrt{-n}) = -2$, so we have

$$\tau I_\gamma = \tau[\tfrac{nA+\sqrt{-n}}{nC}, 1] = [\tfrac{n(A-1)\tau-2}{nC}, \tau]$$

and we can take the matrix $M \in \mathrm{GL}_2^+(\mathbb{Q})$ to be

$$M = \begin{pmatrix} (A-1)/C & -2/nC \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2/C & (A-1)/C \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1/n \\ 1 & 0 \end{pmatrix}.$$

By construction, we have $M(\tau) = \tau_\gamma$ in both cases. Note that at this point we use the fact that the lattice $[\tau, 1]$ is a principal $\mathcal{O}$-ideal.

Further M and $g_\tau(x)$ are transposes of matrices mapping the $\widehat{\mathbb{Z}}$-module $\widehat{\mathbb{Z}}\tau + \widehat{\mathbb{Z}} \subset \widehat{K}$ onto $\widehat{I_\gamma}$, so the matrix $g_\tau(x)M^{-1}$ is in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ as its transpose fixes $\widehat{\mathbb{Z}}\tau + \widehat{\mathbb{Z}}$. We can now compute

$$\sigma_\beta(f(\tau)) = f^{g_\tau(x)}(\tau) = f^{g_\tau(x)M^{-1}}(M(\tau)) = f^{g_\tau(x)M^{-1}}(\tau_\gamma) \tag{3.5}$$

by evaluating $g_\tau(x)M^{-1} \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ modulo the level n of f. All we need to know for this are the p-components x_p of a generator $x \in \widehat{K}^*$ of $\widehat{I_\gamma}$ for the primes p dividing n. Finding a generator x_p of the $(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$-ideal $I_\gamma \otimes \mathbb{Z}_p$ is easy at primes $p|n$, since for these p the identity $BC = -1 - nA^2$ implies that C is a unit in $\mathbb{Z}_p$. This yields

$$\begin{aligned} I_\gamma \otimes_{\mathbb{Z}} \mathbb{Z}_p &= \tfrac{nA+\sqrt{-n}}{nC}\mathbb{Z}_p + \mathbb{Z}_p = (A - \tfrac{1}{\sqrt{-n}})\mathbb{Z}_p + \mathbb{Z}_p \\ &= \tfrac{-1}{\sqrt{-n}}\mathbb{Z}_p + \mathbb{Z}_p = \tfrac{-1}{\sqrt{-n}}\mathbb{Z}_p[\sqrt{-n}]. \end{aligned} \tag{3.6}$$

In Case 1 we have $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p[\sqrt{-n}]$ and we can choose $x_p = \frac{-1}{\sqrt{-n}} = \tau$ for all $p|n$. Applying (3.2) then yields

$$g_\tau(x_p) = \begin{pmatrix} 0 & -1/n \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

at all $p|n$, so $g_\tau(x)M^{-1}$ has upper triangular reduction

$$\begin{pmatrix} 1/C & A/C \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} C & -A \\ 0 & 1 \end{pmatrix}$$

modulo n. It therefore leaves f invariant, and (3.5) reduces to (3.4).

In Case 2 only odd primes can divide n, so again we have $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p[\sqrt{-n}]$ for p dividing n, and we may take $x_p = \frac{n+1}{4}\tau = \frac{1+\sqrt{-n}}{2}\frac{-1}{\sqrt{-n}}$ since $\frac{1+\sqrt{-n}}{2}$ is a p-adic unit if p divides n. Applying (3.3) now yields

$$g_\tau(x_p) = \begin{pmatrix} -1 & -1/n \\ \frac{n+1}{4} & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & \frac{n+1}{4} \end{pmatrix} \begin{pmatrix} 0 & -1/n \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

at all $p|n$, so $g_\tau(x)M^{-1}$ has upper triangular reduction

$$\begin{pmatrix} 1 & -1 \\ 0 & \frac{n+1}{4} \end{pmatrix} \begin{pmatrix} 2/C & (A-1)/C \\ 0 & 1 \end{pmatrix}^{-1}$$

modulo n. As in Case 1, we find that $g_\tau(x)M^{-1}$ leaves f invariant. This finishes the proof of Theorem (1.1).

By Lemma 2.2, Theorem 1.1 furnishes a complete description of the Galois theoretic properties of $f(\tau_\alpha)$ over $\mathbb{Q}(\tau_\alpha)$. This will be particularly useful in the cases in the next section, where we know exactly which elements in $\mathrm{PSL}_2(\mathbb{R})$ fix f.

4. Principal moduli

A modular function f for a discrete group $G \subset \mathrm{PSL}_2(\mathbb{R})$ commensurable with $\mathrm{PSL}_2(\mathbb{Z})$ is a *principal modulus* (in German: *Hauptmodul*) if it generates the field of all modular functions for G. This implies $G\backslash\mathfrak{h}^* \simeq \mathbb{P}^1$ via f. In particular, G has genus 0.

Corollary 1.2, which we will prove now, states that if the modular function f in Theorem 1.1 is a principal modulus for $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$, then we get a primitive element of the ring class field.

Proof of Corollary 1.2. The case $n = 1$ is obvious, so we may assume $n > 1$. Lemma 2.2 shows that the ideals I_α represent all ideal classes in $C(\mathcal{O}_\alpha)$. Then Lemma 2.1 and the correspondence between ideals and quadratic forms imply that we get $|C(\mathcal{O}_\alpha)|$ different $\Gamma_0(n)^\dagger$-inequivalent points of the form τ_α. If f is a principal modulus for $\Gamma_0(n)^\dagger$, it follows that the complex numbers $f(\tau_\alpha)$ have $|C(\mathcal{O}_\alpha)|$ distinct values as we vary α, and the same is true if f is a principal modulus for $\Gamma_0(n)$ since $\Gamma_0(n)^\dagger$-inequivalent points are automatically $\Gamma_0(n)$-inequivalent. Thus the minimal polynomial of $f(\tau_\alpha)$ over $\mathbb{Q}(\tau_\alpha)$ has degree $|C(\mathcal{O}_\alpha)|$ by Theorem 1.1. The theorem follows since this is the degree of the ring class field over $\mathbb{Q}(\tau_\alpha)$. $\square$

It is well known that $\Gamma_0(n)$ has genus 0 for the 15 numbers

$$n = 1\text{–}10, 12, 13, 16, 18, 25. \tag{4.1}$$

Turning to $\Gamma_0(n)^\dagger$, Ogg [10] showed that $\Gamma_0(n)^\dagger$ has genus 0 for the following 37 values of $n > 1$ (we exclude $n = 1$ since $\Gamma_0(1)^\dagger = \Gamma_0(1)$):

$$n = 2\text{–}21, 23\text{–}27, 29, 31, 32, 35, 36, 39, 41, 47, 49, 50, 59, 71. \tag{4.2}$$

However, in order to use Corollary 1.2 for either $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$, we also need to know that the group has a principal modulus with a rational q-expansion. As we are dealing with a finite list of groups, one can simply check the tables in [2], which give explicit formulas for principal moduli in all cases when $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$ has genus 0. These all have rational q-expansions. Alternatively, as S. Norton pointed out to us, Theorem 1 of [9] easily implies the existence of a principal modulus with rational q-expansion whenever $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$ has genus 0. It follows that Corollary 1.2 applies to all values of n in (4.1) for $\Gamma_0(n)$ and (4.2) for $\Gamma_0(n)^\dagger$.

The primitive elements for the ring class fields obtained from principal moduli are often much smaller than those provided by the j-function. For example, take f to be the function listed as 71A in [2, p. 337], which is a principal modulus for the Fricke group $\Gamma_0(71)^\dagger$. There are 14 elliptic fixed points of order 2 for $\Gamma_0(71)^\dagger$, of which seven are of discriminant -71 and seven are of discriminant $-4 \cdot 71 = -284$. This is in accordance with the fact that the two quadratic orders having these discriminants have class number 7. In both cases the corresponding ring class field is the Hilbert class field H of $\mathbb{Q}(\sqrt{-71})$.

When $n = 71$, the two special elliptic points of order 2 used in the proof of Theorem 1.1 are

$$\tau_{-284} = \frac{-1}{\sqrt{-71}} \quad \text{and} \quad \tau_{-71} = \frac{-71 + \sqrt{-71}}{71 \cdot 36}.$$

corresponding to the orders of discriminant -284 and -71 respectively. One can compute that the minimal polynomial of $f(\tau_{-284})$ is

$$h_{-284} = x^7 - 7x^5 - 11x^4 + 5x^3 + 18x^2 + 4x - 11,$$

while the minimal polynomial of $f(\tau_{-71})$ is

$$h_{-71} = x^7 + 4x^6 + 5x^5 + x^4 - 3x^3 - 2x^2 + 1.$$

Each of these polynomials is a small generating polynomial for H over $\mathbb{Q}(\sqrt{-71})$ and compares favorably with the polynomial

$$w_{-71} = x^7 - 2x^6 - x^5 + x^4 + x^3 + x^2 - x - 1$$

found by Weber [13, Vol. III, p. 723] (this is the minimal polynomial of $\mathfrak{f}(\sqrt{-71})/\sqrt{2}$, where $\mathfrak{f}$ is the Weber function defined on page 114 of [13, Vol. III]). If β is a root of w_{-71}, then an easy calculation shows that

$$\begin{aligned} \beta^2 - 1 - \beta^{-1} \ &\text{ is a root of } h_{-284} \\ -\beta^6 + 3\beta^5 - 2\beta^4 + 1 \ &\text{ is a root of } h_{-71}. \end{aligned}$$

Note that the values $f(\tau_{-71})$ and $f(\tau_{-284})$ are in this case *integral*, a general phenomenon for which we currently do not have a proof. For the importance of h_{-284} and h_{-71} for the Schwarzian differential equation satisfied by f, see [6].

As we mentioned in the introduction, the moonshine conjectures for the monster group provide us with principal moduli for genus zero subgroups of $\mathrm{PSL}_2(\mathbb{R})$ in the form of so-called McKay-Thompson series. Their singular values have been studied by Chen and Yui in [1]. They restrict to fundamental McKay-Thompson series, i.e., the series T_g associated to a conjugacy class g of the monster group that is the principal modulus for a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ whose level n equals the order of g. If T_g is fundamental, $\tau \in \mathfrak{h}$ is a CM-point and $\mathcal{O} = \mathbb{Z}[a\tau]$ is the multiplier ring of $[\tau, 1]$, they prove the following in [1, Theorem 3.7.5]:

(1) If T_g is a principal modulus for $\Gamma_0(n)$, then $\mathbb{Q}(\tau, T_g(\tau))$ is the ring class field of the order of index $\frac{n}{\gcd(a,n)}$ in $\mathcal{O}$.
(2) If T_g is a principal modulus for $\Gamma_0(n)^\dagger$ with n prime and coprime to a, then $\mathbb{Q}(\tau, T_g(\tau))$ is the ring class field of the order of index n in $\mathcal{O}$.

Applying the first part of this theorem to $T_g(\tau_\alpha)$, one can prove Corollary 1.2 when T_g is a principal modulus for $\Gamma_0(n)$. So for $T_g(\tau_\alpha)$, the Chen-Yui result covers all numbers in (4.1). On the other hand, if T_g is a principal modulus for $\Gamma_0(n)^\dagger$, then the hypothesis $\gcd(a, n) = 1$ means that the second part of Theorem 3.7.5 doesn't apply to $T_g(\tau_\alpha)$. So for $T_g(\tau_\alpha)$, the Chen-Yui result covers none of the numbers in (4.2). The integrality results in [1] for the numbers $T_g(\tau)$, although interesting in their own right, do not apply to the fixed points $\tau = \tau_\alpha$ in this paper. Numerical computations do however suggest that $T_g(\tau_\alpha)$ is an algebraic integer, so this question deserves further study.

Acknowledgements

The research of the second author is partially supported by NSERC. The first author is grateful to Heng Huat Chan for bringing [5, 12] to his attention, and the second author would like to thank Simon Norton for suggesting the relevance of [9].

References

[1] I. Chen and N. Yui, 'Singular values of Thompson series', *Groups, Difference Sets, and the Monster* (*Columbus, OH, 1993*) (eds K. T. Arasu, J. F. Dillon, K. Harada, S. Sehgal and R. Solomon), Ohio State Univ. Math. Res. Inst. Publ. 4 (de Gruyter, Berlin, 1996), pp. 255–326.

[2] J. H. Conway and S. P. Norton, 'Monstrous moonshine', *Bull. Lond. Math. Soc.* 11 (1979) 308–339.

[3] D. Cox, *Primes of the Form* $x^2 + ny^2$ (John Wiley & Sons, Inc., New York, 1989).

[4] C. J. Cummins and S. P. Norton, 'Rational Hauptmoduls are replicable', Can. J. Math. 47 (1995) 1201–1218.

[5] A. Gee and P. Stevenhagen, 'Generating class fields using Shimura reciprocity', *Algorithmic number theory* (*Portland, OR, 1998*) (ed J. Buhler), Lecture Notes in Comput. Sci. 1423 (Springer-Verlag, Berlin, 1998), pp. 441–453.

[6] J. Harnad and J. McKay, 'Modular solutions to equations of generalized Halphen type', *Proc. R. Soc. Lond.* A 456 (2000) 261–294.

[7] H. Helling, 'On the commensurability class of the rational modular group', *J. London Math. Soc.* 2 (1970) 67–72.

[8] C. Maclachlan, 'Groups of units of zero ternary quadratic forms', *Proc. Roy. Soc. Edinburgh Sect. A* 88 (1981) 141–157.

[9] S. P. Norton, 'Non-monstrous moonshine', *Groups, Difference Sets, and the Monster* (*Columbus, OH, 1993*) (eds K. T. Arasu, J. F. Dillon, K. Harada, S. Sehgal and R. Solomon), Ohio State Univ. Math. Res. Inst. Publ. 4 (de Gruyter, Berlin, 1996), pp. 433–441.

[10] A. Ogg, 'Hyperelliptic modular curves', *Bull. Soc. Math. France* 102 (1974) 449–462.

[11] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* (Princeton U. Press, Princeton, NJ, 1971).

[12] P. Stevenhagen, 'Hilbert's 12th problem, complex multiplication, and Shimura reciprocity', *Class field theory—its centenary and prospect* (*Tokyo, 1998*) (ed K. Miyake), Adv. Stud. in Pure Math. 30 (Math. Soc. Japan, Tokyo, 2001), pp. 161–176.

[13] H. Weber, *Lehrbuch der Algebra*, 2nd Edition (Vieweg, Braunschweig, 1908; Chelsea, New York, 1961.)

Department of Mathematics and Computer Science, Amherst College, Amherst, MA 01002-5000, USA

E-mail address: dac@cs.amherst.edu

Department of Mathematics and Statistics, 1455 de Maisonneuve West, Concordia University, Montréal, Québec, H3G 1M8, Canada

E-mail address: mckay@cs.concordia.ca

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

E-mail address: psh@math.leidenuniv.nl