Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Number Theory 128 (2008) 1989–2009
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

On modular forms for some noncongruence subgroups of $SL_2(\mathbb{Z})$

Chris A. Kurth, Ling Long *

Department of Mathematics, Iowa State University, Ames, IA 50011, USA

Received 28 March 2007; revised 15 October 2007

Available online 28 January 2008

Communicated by James Cogdell

Abstract

In this paper, we consider modular forms for finite index subgroups of the modular group whose Fourier coefficients are algebraic. It is well known that the Fourier coefficients of any holomorphic modular form for a congruence subgroup (with algebraic coefficients) have bounded denominators. It was observed by Atkin and Swinnerton-Dyer that this is no longer true for modular forms for noncongruence subgroups and they pointed out that unbounded denominator property is a clear distinction between modular forms for noncongruence and congruence modular forms. It is an *open question* whether genuine noncongruence modular forms (with algebraic coefficients) always satisfy the unbounded denominator property. Here, we give a partial positive answer to the above open question by constructing special finite index subgroups of $SL_2(\mathbb{Z})$ called character groups and discuss the properties of modular forms for some groups of this kind.

1. Introduction

In [BLS64] Bass, Lazard, and Serre proved that any finite index subgroup of $SL_n(\mathbb{Z})$ with $n > 2$ is congruence in the sense that it contains the kernel of a modulo q homomorphism $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/q\mathbb{Z})$ for some natural number q. The story is quite different when $n = 2$. In the 19th century, the existence of noncongruence subgroups of the modular group $PSL_2(\mathbb{Z})$ was in question until the affirmative results of Fricke [Fri86] and Pick [Pic86]. Around the 1960s more noncongruence subgroups were constructed [Rei58,New65,Ran67, etc.]. In [Mil69a,

* Corresponding author.
E-mail addresses: kurthc@iastate.edu (C.A. Kurth), linglong@iastate.edu (L. Long).

doi:10.1016/j.jnt.2007.10.007

Mil69b], Millington showed there is a one-to-one correspondence between finite index subgroups of $PSL_2(\mathbb{Z})$ and legitimate finite permutation groups described in [Mil69b, Theorem 1]. Using Millington's correspondence, Hsu [Hsu96] gave a concrete method of identifying congruence subgroups. Indeed noncongruence subgroups predominate congruence subgroups in $PSL_2(\mathbb{Z})$ [ASD71,Sto84]. In [ASD71], Atkin and Swinnerton-Dyer initiated a serious investigation on the properties of noncongruence modular forms using computers. Among other important observations and theorems, Atkin and Swinnerton-Dyer pointed out that the Fourier coefficients of certain noncongruence modular forms have unbounded denominators, which is a clear distinction between the noncongruence and congruence modular forms.

Let Γ be a noncongruence subgroup and Γ^c its congruence closure, namely, the smallest congruence subgroup containing Γ. Let (UBD) refer to the following condition on Γ:

Let f be an arbitrary holomorphic integral weight $k \geqslant 2$ modular form for Γ but not for Γ^c with algebraic Fourier coefficients at infinity. Then the Fourier coefficients of f have unbounded denominators.

A natural and interesting open question is:

Does every noncongruence subgroup satisfy the condition (UBD)?

To the authors best knowledge, all data about the known genuine noncongruence modular forms supports a positive answer to the above question. It should be made clear to the readers that this paper is solely about the unbounded denominator property of the coefficients of noncongruence modular forms and that Atkin and Swinnerton-Dyer congruences will not be addressed here, but will be discussed in a coming paper by Atkin and the second author [AL07]. For research in this direction, the readers are referred to the original paper by Atkin and Swinnerton-Dyer [ASD71], several important papers by Scholl [Sch85,Sch88, etc.], and some more recent papers [LLY05, ALL08,Lon07]. All groups considered here are of finite index in $SL_2(\mathbb{Z})$ unless otherwise specified.

Unlike the approach of Atkin and Swinnerton-Dyer in [ASD71], which is mainly concerned with subgroups of $PSL_2(\mathbb{Z})$ with small indices, Li, Long, and Yang [LLY05] considered modular forms for a noncongruence subgroup defined as follows:

Definition 1. Given a finite index subgroup Γ^0 of $PSL_2(\mathbb{Z})$, a normal subgroup Γ of Γ^0 is called a *character group* of Γ^0 if Γ^0/Γ is abelian. I.e. there exists a homomorphism

$$\varphi : \Gamma^0 \to G, \tag{1}$$

where G is a finite abelian group (written multiplicatively) such that $\Gamma = \ker \varphi$.

From now on such a homomorphism φ will be fixed.

Definition 2. Let Γ be the kernel of $\varphi : \Gamma^0 \to G$ with G abelian. We say Γ is a character group of type I if there is a parabolic element $\gamma \in \Gamma^0$ such that $\varphi(\gamma) \neq 1$. If all parabolic elements γ of Γ^0 have $\varphi(\gamma) = 1$ we say Γ is a character group of type II, and additionally if all parabolic and elliptic elements of Γ^0 map to 1 we say Γ is of type II(A).

For example given any positive prime number p, $\Gamma^1(p)$ is a type II character group of $\Gamma^0(p)$ (cf. Example 17). The main difference between character groups of these two types lies in their cusp widths and the general concept of *level* introduced by Wohlfahrt [Woh64] which extends the classical level definition for congruence subgroups by Klein. For any finite index subgroup of $SL_2(\mathbb{Z})$, its level is the least common multiple of all cusp widths of the group. For index-n type II character groups Γ of Γ^0, each cusp c of Γ^0 splits into n different cusps, say $c_1, \ldots, c_n$ in Γ. The cusp width of each c_i is the same as the cusp width of c in Γ^0. Therefore, the level of Γ remains the same as the level of Γ^0. However, this is not true for type I character groups in general. Also note that any genus 0 subgroup Γ^0 can be generated by parabolic and elliptic elements only. Hence there does not exist any nontrivial type II(A) character group of Γ^0. Later in this paper we will consider those Γ^0 whose genus is 1 so that results on elliptic curves can be applied. The main result of this paper is the following theorem which gives a partial positive answer to the open question above.

Theorem 3. *Let Γ^0 be any genus* 1 *congruence subgroup. If there exists a prime number p such that every index-p type* II(A) *character group of Γ^0 satisfies the condition* (UBD)*, then there exists a positive constant c depending on Γ^0 such that for any $X \gg 0$,*

$$\#\bigl\{\textit{Type } \mathrm{II(A)} \textit{ char. group } \Gamma \textit{ of } \Gamma^0 \bigm| \bigl[\Gamma^0 : \Gamma\bigr] < X,\ \Gamma \textit{ satisfies } \mathrm{(UBD)}\bigr\} > c \cdot X^2. \tag{2}$$

In comparison, we will shown in Lemma 28 that

$$\lim_{X\to\infty} \frac{\#\{\text{type II(A) char. group } \Gamma \text{ of } \Gamma^0 \mid [\Gamma^0 : \Gamma] < X\}}{X^2} = \frac{\pi^2}{12}. \tag{3}$$

The result stated in Theorem 3 can be generalized to other genus cases where the power of X will be changed accordingly, however we will work with the genus 1 case here. We will justify in this paper that it is computationally feasible to verify the conditions for the above theorem. In particular, we consider the type II(A) character groups of $\Gamma^0(11)$ as Atkin's calculations in [Atk67] on modular functions for $\Gamma_0(11)$ (which can be easily turned into modular functions for $\Gamma^0(11)$) will be very useful to us. We will show the conclusion of Theorem 3 holds for $\Gamma^0(11)$.

This paper is organized in the following way. In Section 2 we give a general discussion on the unbounded denominator property in general. It followed by Section 3 where we will restrict ourselves to the (UBD) property satisfied by character groups. In particular we will present an unbounded denominator criterion for a single function in Lemma 11 and a criterion for the (UBD) property of groups in Proposition 14. In Section 4, we will conclude that almost all nontrivial type II character groups of the standard congruence subgroups are noncongruence. In Section 5, we will construct modular functions for type II(A) character groups in genus 1 and prove our main result, Theorem 3. In Section 6, we will study modular functions for type II noncongruence character groups of $\Gamma^0(11)$ and show Theorem 3 holds for this group. In the last section, we will briefly describe type I character groups of $\Gamma^0(11)$.

2. Notation and unbounded denominator property in general

We first recall some useful notation and results in [Shi71]. An element γ in $PSL_2(\mathbb{Z})$ is said to be parabolic (respectively elliptic or hyperbolic) if $|\mathrm{tr}\,\gamma| = 2$ (respectively < 2 or > 2). We assume Γ^0 is a congruence subgroup of $PSL_2(\mathbb{Z})$ and Γ a finite index subgroup of Γ^0. Denote by $M_k(\Gamma)$ the space of weight k holomorphic modular forms for Γ. For any field K, let $K(\Gamma)$ denote the field consisting of meromorphic modular functions for Γ with coefficients in K. In particular, $\mathbb{C}(\Gamma)$ is a finite algebraic extension of $\mathbb{C}(\Gamma^0)$. The modular curve X_Γ is defined over an algebraic closure of $\mathbb{Q}$. We use standard notation for some well-known congruence subgroups of $PSL_2(\mathbb{Z})$ with a given level n. For example

$$\Gamma^0(n) = \left\{ \gamma \in SL_2(\mathbb{Z}) \,\middle|\, \gamma = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod n \right\} \Big/ \pm I_2;$$

likewise we will use $\Gamma^1(n)$, $\Gamma_0(n)$, and $\Gamma(n)$ to denote other standard congruence subgroups.

In order to discuss the bounded or unbounded denominator property satisfied by integral weight meromorphic modular forms for Γ, we will restrict ourselves to a suitable algebraic number field K rather than $\mathbb{C}$ itself. For simplicity, we use (FS-A) to refer to the following condition satisfied by a modular form f:

All the Fourier coefficients of f at infinity are algebraic.

If $\mathbb{C}(\Gamma)$ is generated over $\mathbb{C}$ by some transcendental generators $f_1, \ldots, f_n$ where each f_i has coefficients in K, then $K(\Gamma) = K(f_1, \ldots, f_n)$. For any field extension K_1 of K,

$$K_1(\Gamma) = K(\Gamma) \otimes_K K_1. \tag{4}$$

If f satisfies (FS-A), we use (FS-B) to refer to the following condition:

The Fourier coefficients of f at infinity have bounded denominators.

Namely, there is an algebraic number M such that the Fourier coefficients of $M \cdot f$ are all algebraically integral. In the following discussion, we will assume K is a large number field. Let

$$R_K(\Gamma) := \left\{ f \in K(\Gamma) \,\middle|\, f \text{ is holomorphic on } X_\Gamma \text{ with possibly a pole at infinity} \right\}.$$

It is a ring and its fraction field is $K(\Gamma)$. The following observation is very crucial to our discussion.

Observation 1. Elements in $K(\Gamma)$ satisfying (FS-B) are closed under addition, subtraction, multiplication, and hence form a subring of $R_K(\Gamma)$ which will be denoted by $B_K(\Gamma)$. I.e.

$$B_K(\Gamma) := \left\{ f \in R_K(\Gamma) \,\middle|\, f \text{ satisfies (FS-B)} \right\}.$$

Moreover, for any formal power series f whose leading coefficient is 1 and Fourier coefficients are all algebraically integral (such as a normalized newform), $1/f$ also satisfies (FS-B).

Lemma 4. *The ring $R_K(\Gamma^0)$ is a subset of $B_K(\Gamma)$.*

Proof. It is known that any congruence cuspform which satisfies (FS-A) also satisfies (FS-B) (cf. [Shi71, Section 3.5]). Given $f \in R_K(\Gamma^0)$ one can pick a normalized newform F_1 for Γ^0 and a large positive integer N such that $f \cdot F_1^N$ is a cuspform for Γ^0; hence $f \cdot F_1^N$ satisfies (FS-B) and so does f as $1/F_1^N$ also satisfies (FS-B). We conclude that $B_K(\Gamma)$ contains $R_K(\Gamma^0)$. $\square$

Let

$$K_B(\Gamma) := \text{the fraction field of the ring } B_K(\Gamma).$$

By the above lemma, $K_B(\Gamma)$ is a field extension over $K(\Gamma^0)$.

To end this section, we will introduce our key idea in checking whether a group Γ satisfies (UBD).

Proposition 5. *Let Γ be a finite index subgroup of a congruence subgroup Γ^0. Then Γ satisfies* (UBD) *if and only if $B_K(\Gamma) = K(\Gamma^0)$.*

Proof. If Γ does not satisfy (UBD), then there exist an integer j and a holomorphic modular form $f \in M_j(\Gamma) \setminus M_j(\Gamma^0)$ which satisfies (FS-A) and (FS-B). One can construct a function $f' \in R_K(\Gamma) \setminus R_K(\Gamma^0)$ which also satisfies (FS-A) and (FS-B). To see this we first fix some weight j' normalized nonconstant newform F_1 for Γ^0 with Fourier coefficients in K. For a large enough n one can find a weight $nj' - j$ holomorphic modular form F_2 for Γ^0 satisfying (FS-A) and a $F_3 \in R_K(\Gamma^0)$ such that $f' = f \cdot F_2 \cdot F_3/F_1^n \in R_K(\Gamma)$. The functions f, $1/F_1^n$, F_2, and F_3 satisfy (FS-B), and so does f'. Since $F_2 \cdot F_3/F_1^n$ is invariant under the action of Γ^0 and f is not, so $f' \notin R_K(\Gamma^0)$. Therefore $R_K(\Gamma^0) \subsetneq R_K(\Gamma^0)[f'] \subseteq B_K(\Gamma)$ which contradicts the assumption.

Conversely, it is easy to see if $K(\Gamma^0) \subsetneq B_K(\Gamma)$ then Γ does not satisfy (UBD). $\square$

3. Unbounded denominator property for character groups

Now we assume Γ^0 is a congruence subgroup of $PSL_2(\mathbb{Z})$ and Γ a character group of Γ^0.

Lemma 6. *(Cf. [Shi71, Section 2.1].) If Γ is a normal subgroup of Γ^0, then $\mathbb{C}(\Gamma)$ is Galois over $\mathbb{C}(\Gamma^0)$ with the Galois group $\mathrm{Gal}(\mathbb{C}(\Gamma)/\mathbb{C}(\Gamma^0))$ being isomorphic to Γ^0/Γ.*

For any $\gamma \in \Gamma^0$ and $g(z) \in \mathbb{C}(\Gamma)$, γ acts on $g(z)$ via the stroke operator

$$g(z)|_\gamma = g(\gamma z).$$

Lemma 7. *Normal field extensions of $\mathbb{C}(\Gamma^0)$ which are contained in $\mathbb{C}(\Gamma)$ are in one-to-one correspondence with normal subgroups of Γ^0 containing Γ.*

Proof. By the Galois correspondence, there is a bijection between normal intermediate fields between $\mathbb{C}(\Gamma)$ and $\mathbb{C}(\Gamma^0)$ and normal subgroups of Γ^0/Γ. By one of the isomorphism theorems, normal subgroups of Γ^0/Γ are in one-to-one correspondence with normal subgroups of Γ^0 which contain Γ. $\square$

Lemma 8. *If Γ is normal in Γ^0 and Γ^0/Γ is a finite abelian group, then any group Γ' sitting between Γ^0 and Γ is normal in Γ^0.*

Proof. Assume $\Gamma' = \bigcup_i \delta_i \Gamma$. Then for any $\gamma \in \Gamma^0$,

$$\gamma \Gamma' \gamma^{-1} = \bigcup_i \gamma \delta_i \Gamma \gamma^{-1} = \bigcup_i \delta_i \gamma \Gamma \gamma^{-1} = \bigcup_i \delta_i \Gamma = \Gamma'. \qquad \square$$

Corollary 9. *If Γ is any finite index character group of Γ^0, then any intermediate group Γ' sitting between Γ^0 and Γ is also a character group of Γ^0. In particular, if Γ is of type* I (*respectively* II, *or* II(A)), *Γ' is of the same type.*

Observation 2. Let Γ be a character group of Γ^0. By the Fundamental Theorem of Finite Abelian Groups, Γ^0/Γ is isomorphic to a direct sum of several cyclic groups. Hence Γ is the intersection of several character groups Γ_i of Γ^0 with Γ^0/Γ_i cyclic. We will restrict ourselves to character groups with cyclic quotients in the sequel.

Lemma 10. *If Γ is a character group of Γ^0 with cyclic quotient of order n, then there is a modular function f for Γ^0 such that $\mathbb{C}(\Gamma) = \mathbb{C}(\Gamma^0)(\sqrt[n]{f})$.*

Proof. Since $\mathrm{Gal}(\mathbb{C}(\Gamma)/\mathbb{C}(\Gamma^0))$ is isomorphic to $\Gamma^0/\Gamma = \langle a\Gamma\rangle$ for some coset $a\Gamma$, there exists a modular function $g \in \mathbb{C}(\Gamma)$ such that $g|_a = e^{2\pi i/n} g$. Let $f = g^n \in \mathbb{C}(\Gamma^0)$. Then $\mathbb{C}(\Gamma)$ is a splitting field of $x^n - f \in \mathbb{C}(\Gamma^0)[x]$. □

Later in this paper, we will discuss the Fourier coefficients of $\sqrt[n]{f}$. It should be made clear to the readers that the first nonzero coefficient of $\sqrt[n]{f}$ can be determined up to a multiple of an nth root of unity. Once the first nonzero coefficient is chosen, the other coefficients of $\sqrt[n]{f}$ can be computed recursively. Consequently, $\sqrt[n]{f}$ is well defined up to a multiple of an nth root of unity. Therefore, despite the choice of such a root of unity, the bounded or unbounded denominator property of $\sqrt[n]{f}$ is well defined. In this paper, we will always assume, either explicitly or implicitly, a branch is fixed when we take nth root.

Next, we provide the following simple criterion for detecting whether $\sqrt[p]{f}$ satisfies (FS-B) for a given $f \in K(\Gamma^0)$ and for p prime. Note that any nonzero power series f in w can be easily normalized, up to multiplying a power of w, into the form $f = \sum_{m\geqslant 0} a_m w^m$ with $a_0 \neq 0$.

Let $\mathcal{O}_K$ be the ring of integers in K, which is a Dedekind domain. For any $a, b \in \mathcal{O}_K$ and prime ideal $\wp$ of $\mathcal{O}_K$, let $\mathrm{ord}_\wp(a/b) := \mathrm{ord}_\wp(a) - \mathrm{ord}_\wp(b)$.

Lemma 11. *Let K be a number field, p be any prime number and*

$$f = a_0 + \sum_{m\geqslant 1} a_m w^m, \quad a_m \in K,\ a_0 \neq 0$$

such that for every m, a_m is $\wp$-integral for any prime ideal $\wp$ in $\mathcal{O}_K$ above p. Expand $\sqrt[p]{f} = \sum_{m\geqslant 0} b_m w^m$ formally (*we fix a branch for the pth root of a_0*). *If there exists at least one b_m such that* $\mathrm{ord}_\wp(b_0) - \mathrm{ord}_\wp(b_m) > \frac{\mathrm{ord}_\wp(a_0)}{p}$, *then*

$$\limsup_{m\to\infty} -\mathrm{ord}_\wp(b_m) \to \infty.$$

In other words, the sequence $\{b_m\}$ has unbounded denominators.

Proof. Assume $\{-\mathrm{ord}_\wp(b_m) + \mathrm{ord}_\wp(b_0)\}_{m\geqslant 0}$ has an upper bound, say

$$\max\bigl\{-\mathrm{ord}_\wp(b_m) + \mathrm{ord}_\wp(b_0)\bigr\} = C$$

which is larger than $\frac{\mathrm{ord}_\wp(a_0)}{p}$ by our assumption. Let m_0 be the smallest positive integer such that $-\mathrm{ord}_\wp(b_m)+\mathrm{ord}_\wp(b_0)=C$. Consider the m_0p's coefficient of $(\sum(b_m/b_0)q^m)^p=\sum(a_m/a_0)q^m$. We first note that $\mathrm{ord}_\wp(a_0)\geqslant \mathrm{ord}_\wp(a_0)-\mathrm{ord}_\wp(a_{m_0p})$. The m_0p's coefficient of $(\sum(b_m/b_0)q^m)^p$ is

$$\prod_{m_1,\dots,m_p\in\mathbb{Z}_{\geqslant 0},\, m_1+\cdots+m_p=m_0\cdot p} b_{m_j}/b_0.$$

If at least one of $m_i<m_0$, then by the choice of m_0 we have $-\mathrm{ord}_\wp(b_{m_j}/b_0)<-\mathrm{ord}_\wp(b_{m_0}/b_0)$, hence by a standard p-adic analysis

$$-\mathrm{ord}_\wp(a_{m_0\cdot p}/a_0)=-\mathrm{ord}_\wp(b_{m_0}/b_0)^p=-p\cdot\mathrm{ord}_\wp(b_{m_0}/b_0).$$

So we derive a contradiction

$$\mathrm{ord}_\wp(a_0)\geqslant -\mathrm{ord}_\wp(a_{m_0\cdot p}/a_0)=-p\cdot\mathrm{ord}_\wp(b_{m_0}/b_0)>\mathrm{ord}_\wp(a_0). \qquad \square$$

Example 12. (See [ASD71, 4.2.1].) Let

$$\eta(z)=q^{1/24}\prod_{n\geqslant 1}(1-q^n),\quad q=e^{2\pi i z}. \tag{5}$$

The function

$$\xi(z)=\left(\frac{\eta(z)}{\eta(13z)}\right)^2=q^{-1}(1-2q-q^2+\cdots)\in\mathbb{Z}[q^{-1},q]]$$

is a Hauptmodul of the congruence subgroup $\Gamma_0(13)$. Clearly, for any integer $m>2$,

$$\xi^{1/m}(z)=q^{-1/m}\left(1-\frac{2}{m}q+\cdots\right).$$

By the above lemma, the coefficients of $\xi^{1/m}(z)$ have unbounded denominators. The function $\xi^{1/m}(z)$ is a Hauptmodul of a genus zero noncongruence type I character group of $\Gamma^0(13)$.

Lemma 13. *Assume Γ^0 is a genus larger than 0 finite index subgroup of $PSL_2(\mathbb{Z})$ and Γ is a character group of Γ^0. If $R_K(\Gamma)=R_K(\Gamma^0)[g]$ for some g satisfying $g^n=f$ where $f\in R_K(\Gamma^0)$, then $B_K(\Gamma)\neq K(\Gamma^0)$ implies $B_K(\Gamma)$ contains at least one element of the form g^{n+m} for some integer $m\in[1,\dots,n-1]$.*

Proof. Given any $r=\sum_{i=1}^s a_i g^{n_i}\in B_K(\Gamma)$ with $s\geqslant 1$, $a_i\neq 0$ for all i, and $1\leqslant n_1<\cdots<n_s<n$, we will show that $g^{n_i+n}\in B_K(\Gamma^0)$ for some $i\in[1,\dots,s]$ by mathematical induction. When $s=1$, it follows from Lemma 39 in Appendix A.

We now assume $s\geqslant 2$. Let H_1 be a weight 2 normalized newform for Γ^0 so $1/H_1$ satisfies (FS-A) and (FS-B). One can choose $H_2\in R_K(\Gamma^0)$ such that the weight -2 meromorphic modular form $E=H_2/H_1$ and the weight 0 modular function $\frac{E}{f}\cdot\frac{df}{dz}$ for Γ^0 are holomorphic on X_Γ with possibly a pole of finite order at the cusp infinity. It is easy to see E satisfies both

(FS-A) and (FS-B). It is well known that for any nonconstant meromorphic weight 0 modular form F for a finite index subgroup of $SL_2(\mathbb{Z})$, $\frac{dF}{dz}$ is a meromorphic weight 2 modular form for the same group. Thus, $\mathcal{D} = E\frac{d}{dz}$ is a linear mapping on both $R_K(\Gamma^0)$ and $B_K(\Gamma)$ as it preserves the (FS-B) property. Moreover $\mathcal{D}g^i = \frac{i}{n}\frac{\mathcal{D}f}{f}g^i$. So

$$\mathcal{D}\left(\sum_{i=1}^{s} a_i g^{n_i}\right) = \sum_{i=1}^{s} b_i g^{n_i}, \quad \text{where } b_i = \mathcal{D}a_i + a_i \cdot \frac{n_i}{n}\frac{\mathcal{D}f}{f}.$$

If $\frac{b_i}{a_i} = \frac{b_j}{a_j}$ for some $1 \leqslant i < j \leqslant s$, then $\mathcal{D}\ln\frac{a_i}{a_j} = \mathcal{D}\ln f^{(n_j - n_i)/n}$. This is impossible as $0 < n_j - n_i < n$ and hence $f^{(n_j-n_i)/n}$ is not in $K(\Gamma^0)$. So

$$(b_s - a_s\mathcal{D})r = \sum_{i=1}^{s-1}(b_s a_i - a_s b_i)g^{n_i} \in B_K(\Gamma)$$

and it is not zero. Therefore, by induction, we know $g^{n_i+n} \in B_K(\Gamma^0)$ for some $i \in [1, \dots, s]$. $\square$

Combining Proposition 5 and Lemma 13, we derive the following explicit method to verify whether a character group Γ of a genus larger than 0 congruence subgroup Γ^0 satisfies (UBD).

Proposition 14. *Assume Γ^0 is a genus larger than 0 congruence subgroup of $PSL_2(\mathbb{Z})$, Γ is a character group of Γ^0, and $R_K(\Gamma) = R_K(\Gamma^0)[g]$ for some g satisfying $g^n = f$ where $f \in R_K(\Gamma^0)$. If none of g^m for $m \in [n+1, \dots, 2n-1]$ satisfies* (FS-B) *then Γ satisfies* (UBD).

From now on we will confine ourselves to character groups of this type unless otherwise specified. By the Galois correspondence (cf. Lemma 6), $K_B(\Gamma) \otimes_K \mathbb{C}$, which is an intermediate field between $\mathbb{C}(\Gamma)$ and $\mathbb{C}(\Gamma^0)$, corresponds to a character group of Γ^0 containing Γ. We denote the corresponding character group by B_Γ, i.e.

$$B_\Gamma := \text{the character group of } \Gamma^0 \text{ such that } \mathbb{C}(B_\Gamma) = K_B(\Gamma) \otimes_K \mathbb{C}.$$

This group will be one of the key players in our future discussion. We rephrase the (UBD) condition in terms of B_Γ as follows:

Proposition 15. *The group Γ satisfies* (UBD) *if and only if $B_\Gamma = \Gamma^0$.*

Proof. By Proposition 5, Γ satisfies (UBD) if and only if $B_K(\Gamma) = K(\Gamma^0)$. By Lemma 13, $B_K(\Gamma) = K(\Gamma^0)$ if and only if $B_\Gamma = \Gamma^0$. $\square$

4. Noncongruence character groups of type II

Definition 16. A homomorphism $\varphi : \Gamma^0 \to G$ (G can be non-abelian) is said to be of type II if it sends all parabolic elements in Γ^0 to the identity of G.

Lemma 17. *Let p be a prime, then $\Gamma^1(p)$ is a type* II *character group of $\Gamma^0(p)$.*

Proof. Let φ be the following homomorphism

$$\varphi : \Gamma^0(p) \to (\mathbb{Z}/p\mathbb{Z})^\times/\pm 1$$
$$\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a \bmod p)/\pm 1.$$

Then $\ker\varphi = \Gamma^1(p)$. Assume $\gamma = \pm\left(\begin{smallmatrix} a & bp \\ c & \pm 2-a \end{smallmatrix}\right)$ is a parabolic element in $\Gamma^0(p)$. So $\det\gamma = 1$ implies that

$$a \cdot (\pm 2 - a) = 1 \bmod p,$$

hence $a = \pm 1 \bmod p$. Thus $\varphi(\gamma) = 1$ for every parabolic element $\gamma \in \Gamma^0(p)$. □

Proposition 18. *Let φ be a homomorphism of type* II *from $\Gamma^0(n)$ to another finite group* (*not necessarily abelian*) *whose kernel Γ does not contain $\Gamma^1(n)$. Then Γ is noncongruence.*

Proof. Let Γ be the kernel of such a type II homomorphism $\varphi : \Gamma^0(n) \to G$ (as we have mentioned in the introduction, the level of Γ remains n). Now we assume that Γ is a congruence subgroup. Since both $\Gamma^1(n)$ and Γ contain $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, the generator of the stabilizer of 0, so does $\Gamma \cap \Gamma^1(n)$. Therefore the cusp width of $\Gamma \cap \Gamma^1(n)$ at 0 is 1 (while the cusp width of $\Gamma(n)$ at 0 is n). It follows $[\Gamma \cap \Gamma^1(n) : \Gamma(n)] \geqslant n$. On the other hand we have

$$\begin{aligned} n = \left[\Gamma^1(n) : \Gamma(n)\right] &= \left[\Gamma^1(n) : \Gamma \cap \Gamma^1(n)\right]\left[\Gamma \cap \Gamma^1(n) : \Gamma(n)\right] \\ &\geqslant \left[\Gamma^1(n) : \Gamma \cap \Gamma^1(n)\right] n. \end{aligned}$$

Hence $[\Gamma^1(n) : \Gamma \cap \Gamma^1(n)] = 1$ and $\Gamma^1(n) \subset \Gamma$. □

Using a similar argument, one can obtain that

Proposition 19. *Let φ be any nontrivial homomorphism of type* II *from either $\Gamma^1(n)$ or $\Gamma(n)$ to another finite group with kernel Γ. Then Γ is noncongruence.*

5. Modular functions for type II(A) character groups in genus 1

In this section, we fix Γ^0 to be a genus one subgroup of $PSL_2(\mathbb{Z})$, so that the modular curve X_{Γ^0} for Γ^0 is an elliptic curve. We will use O to denote the identity (or the origin) of the elliptic curve. In such a setting, one can apply well-known results on elliptic curves (cf. [Sil86]). Let $\mathrm{Div}^0(X_{\Gamma^0})$ denote the set of all degree zero divisors on the elliptic curve X_{Γ^0}. For any $f \in \mathbb{C}(\Gamma^0)$, let

$$\mathrm{div}(f) = \sum_P n_P(f)(P),$$

where $n_P(f) = \mathrm{ord}_P(f)$ is the order of vanishing of f at P. Then $\mathrm{div}(f)$ is a finite sum such that $\sum_P n_P = 0$. Recall that two divisors D_1, D_2 of X_{Γ^0} are said to be *equivalent* and are denoted by $D_1 \sim D_2$ if $D_1 - D_2 = \mathrm{div}(f)$ for some $f \in \mathbb{C}(\Gamma^0)$.

There is a natural homomorphism $\pi : \Gamma^0 \to H_1(X_{\Gamma^0}, \mathbb{Z})$, the first homology group of X_{Γ^0} with coefficients of $\mathbb{Z}$. For simplicity, we will simply denote $H_1(X_{\Gamma^0}, \mathbb{Z})$ by G^0 (written additively). Let $\varphi : \Gamma^0 \twoheadrightarrow G$ be any surjective homomorphism. By Definition 2, the group $\Gamma = \ker\varphi$ being a type II(A) character group is equivalent to the existence of a surjective homomorphism $\widetilde{\varphi} : H_1(X_{\Gamma^0}, \mathbb{Z}) \twoheadrightarrow G$ such that $\varphi = \widetilde{\varphi} \circ \pi$. Under our assumption on genus being 1, G^0 is a rank-2 free $\mathbb{Z}$-module, i.e. a rank-2 lattice.

Lemma 20. *Let Γ^0 be a genus* 1 *finite index subgroup of the modular group, then type* II(A) *character groups Γ of Γ^0 are in one-to-one correspondence with rank* 2 *sublattices $\widetilde{\Gamma}$ of G^0.*

Proof. The correspondence is $\Gamma = \ker\varphi \leftrightarrow \ker\widetilde{\varphi} = \widetilde{\Gamma}$. □

$$\begin{tikzcd}
1 \arrow[r] \arrow[dr] & \Gamma \arrow[r] \arrow[d, "\pi"'] & \Gamma^0 \arrow[r, "\varphi"] \arrow[d, "\pi"] & G \\
 & \widetilde{\Gamma} \arrow[r] & G^0 \arrow[ur, "\widetilde{\varphi}"'] &
\end{tikzcd}$$

Diagram 1.

From now on we will fix the notation that $\widetilde{\Gamma}$ refers to a finite index subgroup of G^0.

Corollary 21. *Let p be a prime number and Γ^0 be a genus* 1 *finite index subgroup of $PSL_2(\mathbb{Z})$. There are $p+1$ non-isomorphic index-p type* II(A) *character groups of Γ^0.*

Proof. The rank-2 lattice G^0 has $p+1$ non-isomorphic index-p sublattices. □

Lemma 22. *Assume Γ is a type* II(A) *character group of Γ^0 with $\Gamma^0/\Gamma \cong \mathbb{Z}/n\mathbb{Z}$. Then X_Γ also has genus* 1*. The natural projection map $\pi_n : X_\Gamma \to X_{\Gamma^0}$ is a degree n isogeny of elliptic curves.*

Proof. Cf. the Hurwitz genus formula [Sil86, Chapter II, Theorem 5.9]. □

By Lemma 10, $\mathbb{C}(\Gamma) = \mathbb{C}(\Gamma^0)(\sqrt[n]{f})$ for some $f \in \mathbb{C}(\Gamma^0)$. Since $\pi_n : X_\Gamma \to X_{\Gamma^0}$ is an unramified cover, $\operatorname{div}(g) = \sum n_P(f)(P)$ where $n \mid n_P(f)$. Let $g = \sqrt[n]{f}$. We use $\operatorname{div}(g)$ to denote the divisor $\sum \frac{n_P(f)}{n}(P)$ which is in $\operatorname{Div}^0(\Gamma^0)$. By [Sil86, Chapter III, Proposition 3.4] there exists a unique point P on X_{Γ^0} such that

$$\operatorname{div}(g) \sim (P) - (O),$$

where O stands for the origin of the elliptic curve X_{Γ^0}. We fix the cusp infinity to be the origin of X_{Γ^0} in the following discussion. Since $\operatorname{div}(g^n) = \operatorname{div}(f)$ is a principle divisor, we know P is an n-torsion point of X_{Γ_0} by Abel's Theorem. Hence one can pick $f = f_P$ to be a modular function for Γ^0 satisfying

$$\operatorname{div}(f_P) = -n \cdot (O) + n \cdot (P). \tag{6}$$

Lemma 23. *If X_{Γ^0} has an algebraic model defined over a number field K_0 and $\mathbb{C}(\Gamma^0) = K_0(\Gamma^0) \otimes_{K_0} \mathbb{C}$, then for any type* II(A) *character group Γ of Γ^0 with $\Gamma^0/\Gamma \cong \mathbb{Z}/n\mathbb{Z}$, $\mathbb{C}(\Gamma)$ is generated over $\mathbb{C}(\Gamma^0)$ by a single element g whose Fourier coefficients at infinity are in a fixed number field K above K_0. Moreover, $g^n \in K(\Gamma^0)$.*

Proof. Assume $\mathrm{div}(g) \sim (P) - (O)$ and by the above assumption the coordinates of P on the elliptic curve X_{Γ^0} are algebraic numbers. Let x and y be the local variables of X_{Γ^0} which have only one pole at infinity of degree 2 and 3, respectively. Namely x corresponds to the Weierstrass $\wp(z)$-function of the elliptic curve and y corresponds to $\wp'(z)$ (cf. [Kob93, Chapter I, Section 6]). We may assume the Fourier coefficients of x and y at infinity are in a number field K_0. So $R_{K_0}(\Gamma^0) = K_0[x, y]$. Then f_P can be expressed as a polynomial in x and y whose coefficients can be determined by the condition (6). Hence the coefficients of $F(x, y)$ can be determined by solving a system of algebraic equations. Then we can pick K to be a large enough number field which contains coefficients of $F(x, y)$ and all primitive nth roots. By our construction, $f_P \in K(\Gamma^0)$. $\square$

In summary, if Γ^0 has genus 1 and Γ is a type II(A) character group of Γ^0 with cyclic quotient then

$$R_K(\Gamma) = R_K\left(\Gamma^0\right)\left[\sqrt[n]{f_P}\,\right] \tag{7}$$

for some $f_P \in R_K(\Gamma^0)$. So we can apply the results of Lemma 13 and Propositions 14 and 15. We conclude that there is an intermediate group B_Γ between Γ^0 and Γ which corresponds to modular functions in $K(\Gamma)$ satisfying (FS-B).

In the following discussion, for a fixed prime number p we will construct all non-isomorphic index-p type II(A) character groups of Γ^0.

Lemma 24. *Given two functions g_1 and g_2 in $R_K(\Gamma)$, assume* $\mathrm{div}(g_1) \sim (P_1) - (O)$ *and* $\mathrm{div}(g_2) \sim (P_2) - (O)$*. They generate the same finite field extension over $\mathbb{C}(\Gamma^0)$ which corresponds to a type* II(A) *character group if and only if $\langle P_1\rangle = \langle P_2\rangle$ as finite abelian subgroups of X_{Γ^0}.*

Proof. By our previous assumptions, the orders of P_1 and P_2 in X_{Γ^0} are both n.

If $g_1 \in \mathbb{C}(\Gamma^0)(g_2)$, then $(P_2) - (O) \in \langle (P_1) - (O)\rangle$, thus $P_2 \in \langle P_1\rangle$. So $\mathbb{C}(\Gamma^0)(g_1) = \mathbb{C}(\Gamma^0)(g_2)$ implies $\langle P_1\rangle = \langle P_2\rangle$.

Conversely, if $\langle P_1\rangle = \langle P_2\rangle$ then $P_2 = kP_1$, for some integer k such that $\gcd(k, n) = 1$. So $\mathrm{div}(g_1^k/g_2) = k(P_1) - (kP_1) - (k-1)(O)$ is principle. Hence $g_2 \in \mathbb{C}(\Gamma^0)(g_1)$. Similarly, $g_1 \in \mathbb{C}(\Gamma^0)(g_2)$. Therefore g_1 and g_2 generate the same field. $\square$

The following proposition follows from the previous discussions.

Proposition 25. *Let Γ^0 be a genus* 1 *congruence subgroup of $PSL_2(\mathbb{Z})$ and p be a prime number. Let P and Q be two linearly independent p-torsion points of X_{Γ^0}, then each function $\sqrt[p]{f}_P$, $\sqrt[p]{f_{Q+iP}}$, $i = 1, \ldots, p$, generates a degree p field extension of $\mathbb{C}(\Gamma^0)$ which corresponds to an index-p type* II(A) *character group of Γ^0. Moreover, any two* II(A) *character groups obtained this way are non-isomorphic.*

Next, we start to estimate the number of type II(A) character groups of Γ^0 satisfying the condition (UBD). We let

$$B_{\mathrm{II(A)}} = \bigcap_{\Gamma} B_\Gamma, \tag{8}$$

where Γ runs through all type II(A) character groups of Γ^0. By Observation 2, it is also the intersection of all character groups of Γ^0 with cyclic quotient. The next lemma shows $B_{\mathrm{II(A)}}$ is crucial to the discussion of the (UBD) condition.

Lemma 26. *Let Γ^0 be a genus* 1 *congruence subgroup of $PSL_2(\mathbb{Z})$ and Γ be an arbitrary type* II(A) *noncongruence character group Γ of Γ^0. If*

$$B_{\mathrm{II(A)}} \cdot \Gamma = \Gamma^0, \tag{9}$$

then Γ satisfies the condition (UBD).

Proof. The group B_Γ contains both $B_{\mathrm{II(A)}}$ and Γ. Since $B_{\mathrm{II(A)}} \cdot \Gamma$ is the smallest subgroup of Γ^0 containing both $B_{\mathrm{II(A)}}$ and Γ, it is contained in B_Γ. So

$$\Gamma^0 \supset B_\Gamma \supset B_{\mathrm{II(A)}} \cdot \Gamma = \Gamma^0$$

and thus $B_\Gamma = \Gamma^0$. The claim then follows from Proposition 15. □

For simplicity, we write B for $B_{\mathrm{II(A)}}$ below.

Lemma 27. *If there exists a prime number p such that for every index-p type* II(A) *character group Γ of Γ^0, $B \cdot \Gamma = \Gamma^0$, then $[\Gamma^0 : B] < \infty$.*

Proof. We will stick to previous notation (cf. Diagram 1 and Lemma 20). Let $\widetilde{B} = \pi(B) \subset G^0$. Since $B \cdot \Gamma = \Gamma^0$, we have $\widetilde{B} + \widetilde{\Gamma} = G^0$. Because $\widetilde{\Gamma}$ is a proper subgroup of G^0, $\widetilde{B}$ is not trivial. To achieve the claim it suffices to show that the rank of $\widetilde{B}$ is 2. We will rule out the other remaining possibility: $\widetilde{B}$ has rank 1.

Assume $\widetilde{B}$ has rank 1 and, up to picking a new basis for G^0, we may assume $\widetilde{B} = \langle na \rangle$ for some integer $n > 0$. Hence $\widetilde{B} + \langle a, pb \rangle = \langle a, pb \rangle$ where $\langle a, pb \rangle = \widetilde{\Gamma}$ is an index-p subgroup of G^0. Let Γ be the index-p type II(A) character group of Γ^0 corresponding to $\widetilde{\Gamma}$. Correspondingly we have $B \cdot \Gamma = \Gamma$ which contradicts the assumption. □

We now fix a set of generators $\{a, b\}$ for the lattice Γ^0 and consider sublattices $\widetilde{\Gamma}$ of G^0. By a standard argument using modules over $\mathbb{Z}$, we know each such $\widetilde{\Gamma}$ can be written uniquely as $\langle la + nb, mb \rangle$ for some nonnegative integers l, n, m where $0 \leqslant n < m$ and $l > 0$. Hence finite subgroups of G^0 are in one-to-one correspondence with triples (l, n, m) of nonnegative integers satisfying $0 \leqslant n < m$ and $l > 0$.

We first give an estimation for the number of type II(A) character groups of Γ^0 as follows.

Lemma 28.

$$\lim_{X \to \infty} \frac{\#\{\mathrm{II(A)}\ \textit{type char. group}\ \Gamma\ \textit{of}\ \Gamma^0 \mid [\Gamma^0 : \Gamma] < X\}}{X^2} = \frac{\pi^2}{12}. \tag{10}$$

Proof. Let X be a large positive integer. Let

$$S(X) := \#\{\text{II(A) type char. group } \Gamma \text{ of } \Gamma^0 \mid [\Gamma^0 : \Gamma] < X\}.$$

Computing $S(X)$ boils to counting the number of triples of nonnegative integers (l, m, n) such $l \cdot m < X, 0 \leqslant n < m$. Let l be a fixed positive integer smaller than X, then m can be any positive integer no bigger than $\lceil \frac{X}{l} \rceil$, the greatest integer not exceeding $\frac{X}{l}$, and n can be any nonnegative integer smaller than m, so there are altogether

$$S(X) = \sum_{l=1}^{X-1} \sum_{m=1}^{\lceil \frac{X}{l} \rceil - 1} m = \sum_{l=1}^{X-1} \frac{\lceil \frac{X}{l} \rceil (\lceil \frac{X}{l} \rceil - 1)}{2}. \tag{11}$$

So

$$\sum_{l=1}^{X-1} \left(\frac{1}{2l^2} - \frac{3}{2lX} + \frac{1}{X^2} \right) \leqslant \sum_{l=1}^{X-1} \frac{(\frac{1}{l} - \frac{1}{X})(\frac{1}{l} - \frac{2}{X})}{2}$$
$$\leqslant \frac{S(X)}{X^2} \leqslant \sum_{l=1}^{X-1} \frac{\frac{1}{l}(\frac{1}{l} - \frac{1}{X})}{2} = \sum_{l=1}^{X-1} \left(\frac{1}{2l^2} - \frac{1}{2lX} \right). \tag{12}$$

Since

$$\lim_{X \to \infty} \sum_{l=1}^{X-1} \frac{1}{lX} \leqslant \lim_{X \to \infty} \frac{1 + \ln X}{X} = 0 \quad \text{and} \quad \lim_{X \to \infty} \sum_{l=1}^{X-1} \frac{1}{X^2} = 0$$

hence

$$\lim_{X \to \infty} \frac{S(X)}{X^2} = \lim_{X \to \infty} \sum_{l=1}^{X-1} \frac{1}{2l^2} = \frac{1}{2} \zeta(2) = \frac{\pi^2}{12}, \tag{13}$$

where $\zeta(2)$ is the value of the classical Riemann zeta function at 2. □

Lemma 29. *Assume $\widetilde{B} = \langle sa + ub, vb \rangle$ with such a triple (s, u, v). Then $\widetilde{\Gamma} + \widetilde{B} = G^0$ if and only if*

$$\gcd(s, l) = 1 = \gcd(v, m, sn - ul). \tag{14}$$

Proof. $\widetilde{\Gamma} + \widetilde{B} = G^0$ if and only if the lattice $\langle la + nb, mb, sa + ub, vb \rangle = \langle a, b \rangle$. It is equivalent to the invariant factors of $\langle la + nb, mb, sa + ub, vb \rangle$ are 1 and 1. Then we apply [Jac85, Theorem 3.9] to obtain (14). □

Next we give an estimation for the number of type II(A) character groups Γ of Γ^0 satisfying $\Gamma \cdot B = \Gamma^0$. By Lemma 26, those Γ satisfy the condition (UBD).

Lemma 30. *Assume Γ^0 is a genus 1 congruence subgroup and $[\Gamma^0 : B] < \infty$. There exists a positive constant c depending on Γ^0 such that*

$$\lim_{X\to\infty} \frac{\#\{\text{II(A)}\ \textit{type char. group}\ \Gamma\ \textit{of}\ \Gamma^0 \mid [\Gamma^0 : \Gamma] < X,\ \Gamma \cdot B = \Gamma^0\}}{S(X)} > c. \tag{15}$$

Proof. It is equivalent to consider finite index subgroups $\widetilde{\Gamma}$ of G^0 such that $\widetilde{\Gamma} + \widetilde{B} = G^0$. By the previous lemma, it boils down to counting the number of triples (l, n, m) satisfying $0 \leqslant n < m$, $l > 0$, and (14). Now we count the number of triples such that $0 \leqslant n < m$, $l > 0$, $m \cdot l < X$ and $\gcd(s, l) = 1 = \gcd(v, m)$. We further assume $l = 1$ and $X/2 < m < X$. The problem has been reduced to counting the number of couples (m, n) such that

$$X/2 < m < X, \quad (s, m) = 1, \quad 0 \leqslant n \leqslant m.$$

Between $X/2$ and X there are about $\frac{\phi(s)}{2s} X$ integers coprime to s, where $\phi(s)$ is the Euler number of s. So there exists a constant $c_1 > 0$ depending on s such that there are at least $c_1 \cdot X$ positive integers within $(X/2, X)$ satisfying $(s, m) = 1$. Therefore there are at least $\frac{c_1}{2} \cdot X^2$ triples of nonnegative integers (l, n, m) satisfying the conditions above. The statement of the lemma then follows from 28. $\square$

Proof of Theorem 3. Let Γ^0 be a genus 1 congruence subgroup and p be a prime number. Each index-p type II(A) character group Γ of Γ^0 satisfies $R_K(\Gamma) = R_K(\Gamma^0)[\sqrt[p]{f_P}\,]$ for some function $f_P \in R_K(\Gamma^0)$ (cf. (6) and (7)). If all $p+1$ non-isomorphic index-p type II(A) character groups of Γ^0 satisfy (UBD), then Lemma 27 implies $B_{\mathrm{II(A)}} = \bigcap_\Gamma B_\Gamma$ is a finite index subgroup of Γ^0. Our main result, Theorem 3, then follows from Lemma 30. $\square$

6. Character groups of $\Gamma^0(11)$ of type II

In this section, we show that it is computationally feasible to verify the conditions of Theorem 3 by working with type II(A) character groups of $\Gamma^0(11)$. We choose $\Gamma^0(11)$ as the integrality of the Fourier coefficients of two basic modular functions for $\Gamma^0(11)$ is known due to a result of Atkin [Atk67].

6.1. *The group* $\Gamma^0(11)$

The group $\Gamma^0(11)$ has genus 1 and is torsion free. A fundamental domain for $\Gamma^0(11)$ is shown in Fig. 1. A set of generators of $\Gamma^0(11)$ can be chosen as two parabolic elements γ_∞ and γ_0 and two hyperbolic elements A_1 and B_1 subject to only one relation:

$$\gamma_\infty \gamma_0 A_1 B_1 A_1^{-1} B_1^{-1} = I_2.$$

Since $\Gamma^0(11)$ does not have any elliptic elements, every type II character group of $\Gamma^0(11)$ is automatically of type II(A).

The modular curve $X_{\Gamma^0(11)}$ has an equation (cf. [Cre97])

$$X_{\Gamma^0(11)}\colon\ y^2 + y = x^3 - x^2 - 10x - 20. \tag{16}$$

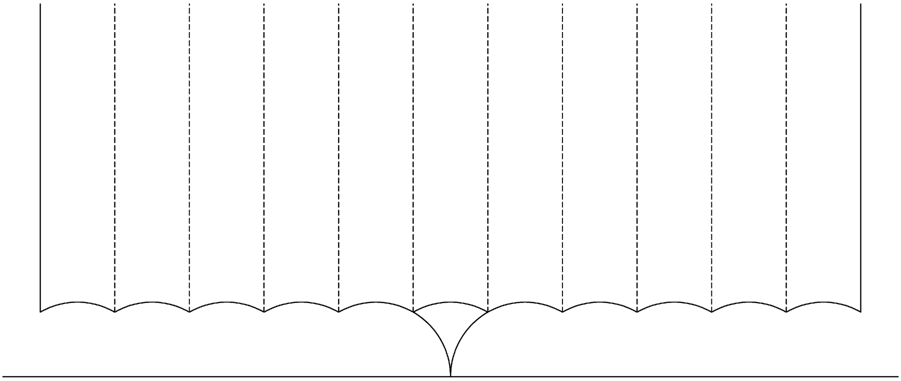

Fig. 1. Fundamental domain for $\Gamma^0(11)$.

It is known [Kob93, III, Proposition 19] that the unique (up to a scalar) holomorphic differential 1-form on $X_{\Gamma^0(11)}$ is

$$\frac{dx(z)}{2y(z)+1} = c \cdot \eta(z)^2\eta(z/11)^2\,dz. \tag{17}$$

One can easily determine that $c = 1$. From (16) and (17), we have

$$\begin{aligned} x(z) &:= w^{-2} + 2w^{-1} + 4 + 5w + 8w^2 + w^3 + 7w^4 - 11w^5 + 10w^6 - 12w^7 - 18w^8 + \cdots, \\ y(z) &:= w^{-3} + 3w^{-2} + 7w^{-1} + 12 + 17w + 26w^2 + 19w^3 + 37w^4 - 15w^5 - 16w^6 \\ &\quad - 67w^7 + \cdots, \end{aligned}$$

where $w = e^{2\pi i z/11}$.

Lemma 31. *The Fourier coefficients of x and y at infinity are in $\mathbb{Z}$.*

Proof. In [Atk67], Atkin gave a system of modular functions $\{G_n(z)\}$ on $X_{\Gamma_0(11)}$ (and $\{G_n(z/11)\}$ on $X_{\Gamma^0(11)}$) with integral coefficients and only one pole of order n at infinity and a zero at $z = 0$ with maximal multiplicities. According to Lemma 4 of [Atk67], one can obtain that

$$\begin{aligned} x &= G_2(z/11) + 16, \\ y &= G_3(z/11) + 6G_2(z/11) + 60. \end{aligned}$$

Therefore x and y have integral coefficients. □

Corollary 32. *The x and y coordinates for $z = 0$ are* 16 *and* 60.

6.2. Index-2 type II character groups of $\Gamma^0(11)$

By direct verification, we can describe the index-2 type II character groups of $\Gamma^0(11)$ as follows.

Lemma 33. *There are three distinct surjective homomorphisms* $\varphi : \Gamma^0(11) \to \{\pm 1\}$ *of type* II.

- *If* $\varphi(A_1) = -1$, $\varphi(B_1) = 1$, *then* $\ker \varphi$ *is generated by*

$$\left\{A_1^2, B_1, \gamma_0, \gamma_\infty, A_1\gamma_0 A_1^{-1}, A_1\gamma_\infty A_1^{-1}\right\}$$

  subject to the relation

$$(\gamma_0\gamma_\infty)\left(A_1\gamma_0\gamma_\infty A_1^{-1}\right)\left(A_1^2 B_1 A_1^{-2} B_1^{-1}\right) = I_2.$$

- *If* $\varphi(A_1) = 1$, $\varphi(B_1) = -1$, *then* $\ker \varphi$ *is generated by*

$$\left\{A_1, B_1^2, \gamma_0, \gamma_\infty, B_1\gamma_0 B_1^{-1}, B_1\gamma_\infty B_1^{-1}\right\}$$

  subject to the relation

$$\left(B_1\gamma_0\gamma_\infty B_1^{-1}\right)(\gamma_0\gamma_\infty)\left(A_1 B_1^2 A_1^{-1} B_1^{-2}\right) = I_2.$$

- *If* $\varphi(A_1) = -1$, $\varphi(B_1) = -1$, *then* $\ker \varphi$ *is generated by*

$$\left\{A_1^2, B_1 A_1, \gamma_0, \gamma_\infty, A_1\gamma_0 A_1^{-1}, A_1\gamma_\infty A_1^{-1}\right\}$$

  subject to the relation

$$(\gamma_0\gamma_\infty)\left(A_1\gamma_0\gamma_\infty A_1^{-1}\right)\left(\left(A_1^2\right)(BA_1)\left(A_1^2\right)^{-1}(BA_1)^{-1}\right) = I_2.$$

Making the change of variables

$$x := \frac{1}{\sqrt[3]{4}} X + \frac{1}{3}, \quad y := \frac{1}{2} Y - \frac{1}{2},$$

Eq. (16) will be changed to

$$Y^2 = X^3 - \frac{31}{3}\sqrt[3]{2^4} X - \frac{2501}{27}.$$

Let α_i, $1 \leqslant i \leqslant 3$, be the three roots of $X^3 - \frac{31}{3}\sqrt[3]{2^4}X - \frac{2501}{27}$. Then $X - \alpha_i$ is a meromorphic function on $X_{\Gamma^0(11)}$ and

$$\operatorname{div}(X - \alpha_i) = 2(P_i) - 2(O),$$

where the (X, Y) coordinates for P_i are $(\alpha_i, 0)$. Let $\beta_i = \sqrt[3]{4}/3 + \alpha_i$. Then

$$f_{P_i} = X - \alpha_i = \sqrt[3]{4}x - \beta_i = \sqrt[3]{4}w^{-2} + 2\sqrt[3]{4}w^{-1} + \cdots. \tag{18}$$

By Lemma 11, we derive that the coefficients of $(\sqrt{f_{P_i}})^3$ have unbounded denominators for $i = 1, 2, 3$. By Lemma 13, $B_K(\Gamma) = R_K(\Gamma^0(11))$ and hence $B_\Gamma = \Gamma^0(11)$. By Proposition 5, we have

Theorem 34. *Theorem* 3 *holds for* $\Gamma^0(11)$.

6.3. Index-5 character groups of $\Gamma^0(11)$ of type II

In this subsection, we consider index-5 type II character groups of $\Gamma^0(11)$. Note that $\Gamma^1(11)$ is one of these groups and the Mordell–Weil group of $X_{\Gamma^0(11)}$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Let $P = [5,5]$ and $Q = [-\frac{1}{2} + \frac{11}{10}\sqrt{5}, -\frac{1}{2} + \frac{11}{10}\sqrt{-25-2\sqrt{5}}]$. They generate all 5-torsion points of $X_{\Gamma^0(11)}$. (In particular, $3P = [16,60]$ corresponds to the point $z = 0$ on $X_{\Gamma^0(11)}$.) The x-coordinates of $Q + iP$, $1 \leqslant i \leqslant 4$, are the roots of the monic polynomial $x^4 + x^3 + 11x^2 + 41x + 101$ and hence are all integral. Similarly, the y-coordinates of $Q + iP$, $1 \leqslant i \leqslant 4$, are also integral.

By an explicit calculation using Maple, it is found that (cf. (6))

$$f_P = xy - 4x^2 + 30x - 4y - 55.$$

Hence the Fourier coefficients of the expansion of f_P in terms of w are all 5-integral. When $i = 1,2,3,4$, the coefficients of f_{Q+iP}, as a polynomial in x and y, are in a larger number field K. However, by checking the denominators, one concludes that the Fourier coefficients of the expansion of f_{Q+iP} in terms of w are all $\wp$-integral for any prime $\wp$ in K above 5.

Corollary 35. *The w-expansions of all above functions are $\wp$-integral for any prime $\wp$ above* 5.

More explicitly, we have

$$\begin{aligned}
f_P &= w^{-5} + w^{-4} - 3w^{-3} + 13w^{-2} + 20w^{-1} - 23 + \cdots, \\
f_{Q+P} &= w^{-5} + w^{-4} + \frac{23 + \sqrt{5} + i(3+\sqrt{5})\sqrt{25+2\sqrt{5}}}{4} w^{-3} + \cdots, \\
f_{Q+2P} &= w^{-5} + w^{-4} + \frac{99 - 33\sqrt{5} + i(23+3\sqrt{5})\sqrt{25+2\sqrt{5}}}{44} w^{-3} + \cdots, \\
f_{Q+3P} &= w^{-5} + w^{-4} + \frac{99 - 33\sqrt{5} - i(23+3\sqrt{5})\sqrt{25+2\sqrt{5}}}{44} w^{-3} + \cdots, \\
f_{Q+4P} &= w^{-5} + w^{-4} + \frac{23 + \sqrt{5} - i(3+\sqrt{5})\sqrt{25+2\sqrt{5}}}{4} w^{-3} + \cdots.
\end{aligned}$$

Hence one can apply Lemma 11 and conclude that the coefficients of $(\sqrt[5]{f_P(w)})^j$ and $(\sqrt[5]{f_{Q+iP}(w)})^j$, $1 \leqslant i \leqslant 4$, $j = 6,7,8,9$, have unbounded denominators. By Lemma 13, the corresponding character groups satisfy (UBD).

Theorem 36. *There are* 6 *index*-5 *type* II(A) *character groups in* $\Gamma^0(11)$. *Among them, one is* $\Gamma^1(11)$ *and the other* 5 *are noncongruence. Moreover every one of these noncongruence subgroups satisfies the condition* (UBD).

The following conjecture is equivalent to the condition (UBD) being held by all type II(A) character groups of $\Gamma^0(11)$.

Conjecture 37. *For* $\Gamma^0(11)$, $B_{\mathrm{II(A)}} = \Gamma^1(11)$.

7. Character groups of $\Gamma^0(11)$ of type I

By Lemma 3 of [Atk67], the following modular function for $\Gamma^0(11)$

$$G_5(z) = \left(\frac{\eta(z/11)}{\eta(z)}\right)^{12} = w^{-5}\left(1 - 12w + 54w^2 - 88w^3 - 99w^4 + \cdots\right) \tag{19}$$

satisfies

$$\operatorname{div}(G_5) = 5(P_0) - 5(O),$$

where $P_0 = [16, 60]$ is a 5-torsion point of $X_{\Gamma^0(11)}$. Since P_0 corresponds to the point $z = 0$ as we have mentioned earlier, O and P_0 correspond to the two cusps of $\Gamma^0(11)$.

Let Γ be a type I character group of $\Gamma^0(11)$ with $\Gamma^0(11)/\Gamma \cong \mathbb{Z}/n\mathbb{Z}$. Then $\mathbb{C}(\Gamma) = \mathbb{C}(x, y)(\sqrt[n]{f})$ for some $f \in \mathbb{C}(\Gamma^0(11)) = \mathbb{C}(x, y)$. Consider

$$\operatorname{div}(f) = n_{P_0}(f)(P_0) - n_O(f)(O) + \sum_{i=1}^{l} n_i(f)(P_i),$$

where each P_i is different from O or P_0. Since the covering map $X_\Gamma \to X_{\Gamma^0(11)}$ only ramifies at the cusps, $n \mid n_i$, $1 \leqslant i \leqslant l$. As P_0 is a 5-torsion point, we have

$$\operatorname{div}\left(f^5\right) = \operatorname{div}\left(G_5^{n_{P_0}(f)}\right) + \left(\sum_{i=1}^{l} 5n_i(f)(P_i) + \left(5n_{P_0}(f) - 5n_O(f)\right)(O)\right).$$

If $5 \nmid n$, then $\sqrt[n]{f}$ and $\sqrt[n]{f^5}$ will generate the same field extension over $\mathbb{C}(\Gamma^0(11))$. Hence we may assume $f = (G_5)^{n_0} \cdot f'$ for some integer n_0 and $f' \in \mathbb{C}(\Gamma^0(11))$ such that $\mathbb{C}(\Gamma^0(11))(\sqrt[n]{f'})$ corresponds to an index-$5n$ type II character group of $\Gamma^0(11)$.

In particular we consider the case when $f' = 1$ and $5 \nmid n$. In this case we may assume $n_0 = 1$. Let Γ_n denote the character group whose field of modular functions is generated by $\sqrt[n]{G_5}$ over $\mathbb{C}(\Gamma^0(11))$. By using the genus formula again, Γ_n has genus n. When $n \neq 1, 2, 3, 4, 6, 12$ and $5 \nmid n$, the coefficients of $\sqrt[n]{G_5}$ have unbounded denominators and hence Γ_n is a type I character group of $\Gamma^0(11)$ which satisfies the condition (UBD). Moreover, $\sqrt[5]{G_5}$ corresponds to an index-5 type II character group.

Remark 38. When $n = 2, 3, 4, 6, 12$, $\sqrt[n]{G_5}$ is an eta quotient. It is clear that it is a congruence modular function. Hence Γ_n is congruence when n is divisible by 12. By the classification of Cummins and Pauli on congruence subgroups with genus no larger than 24 [CP03], we know when $n = 2, 3, 4, 6, 12$, the corresponding character groups are $22A^2$, $33A^3$, $44A^4$, $66B^6$, $132A^{12}$ in the notation of Cummins and Pauli.

Acknowledgments

The authors are indebted to Prof. A.O.L. Atkin. The authors would like to thank him for his communications through which we have refined our approach. Atkin has provided another proof of the integrality of the Fourier coefficients of x and y used in Section 5. The authors also thank Prof. Frits Beukers, James Cogdell, Wenching Winnie Li, and Siu-Hung Ng for their enlightening communications and constructive suggestions. Prof. Helena Verrill's Fundamental Domain Drawer was used to generate the fundamental domain in this paper. The authors are grateful to the referee whose comments led to a significantly improved presentation of this paper. The second author would further thank the National Center for Theoretical Sciences in Taiwan for hosting her visit in summer 2007 during when the paper was revised.

Appendix A

To abuse notation, in the following discussion we will continue to say a formal power series $f \in K[w^{-1}, w]]$ satisfies (FS-B) if its coefficients have bounded denominators. We assume K is a large number field and use $\mathcal{O}_K$ to denote the ring of algebraic integers in K. For any formal power series $f \in \mathcal{O}_K[w^{-1}, w]]$ let $C(f)$ be the ideal of $\mathcal{O}_K$ generated by the coefficients of f. This a generalization of concept of content for polynomials with algebraically integral coefficients. Since $\mathcal{O}_K$ is a Dedekind domain, we apply Gauss Lemma to conclude that

$$C(f \cdot g) = C(f) \cdot C(g) \tag{20}$$

for any $f, g \in \mathcal{O}_K[w^{-1}, w]]$.

Lemma 39. *Let n_1 and n be positive integers satisfying $n_1 < n$ and K be a large number field containing all primitive roots of 1 of order less or equal to n. If $h(w)$ and $g(w)$ are in $K[w^{-1}, w]]$ such that $h(w)$, $g^n(w)$, and $h(w) \cdot g^{n_1}(w)$ all have bounded denominators, then so do the coefficients of $g^{n_1+n}(w)$.*

Proof. We may assume n_1 and n are relatively prime. Otherwise, we can use g^d for g and n/d (respectively n_1/d) for n (respectively n_1).

We may further assume that

$$h(w) = \sum_{m \geqslant 1} c_m w^m, \quad c_1 \neq 0$$

and $h, hg^{n_1+n}, g^n \in \mathcal{O}_K[w]]$. Note that the derivative of hg^{n_1+n} respect to w satisfies (FS-B). Since

$$\frac{d}{dw}\left(hg^{n_1+n}\right) = \frac{dh}{dw} \cdot g^{n_1+n} + \frac{n_1+n}{n} \cdot \frac{df}{dw} \cdot \left(hg^{n_1}\right),$$

it follows $\frac{dh}{dw} \cdot g^{n_1+n}$ also satisfies (FS-B). Let $h^{[1]} := h$. Then

$$h^{[2]} := w\frac{dh}{dw} - h = \sum_{m \geqslant 2} c_m(m-1)w^m$$

has algebraically integral coefficients and its product with g^{n_1+n} satisfies (FS-B). We repeat above process by replacing $h^{[1]}$ by $h^{[2]}$ and remark that the coefficients of $\frac{dh^{[2]}}{dw}$ have a common factor of 2. So

$$h^{[3]} := \frac{w}{2}\frac{dh^{[2]}}{dw} - h^{[1]} = \sum_{m \geqslant 3} c_m \frac{(m-2)(m-1)}{2} w^m \in \mathcal{O}_K[w]].$$

By iteration, we construct

$$h^{[k]} := c_k w^k + \sum_{m>k} c_m \binom{m-1}{k-1} w^m \in \mathcal{O}_K[w]]. \tag{21}$$

By induction $h^{[k]} \cdot g^{n_1+n}$ satisfies (FS-B) for any positive integer k.

By the way $h^{[k]}$ is constructed, we know there exist integer multiples of $h^{[k]}g^{n_1+n}$ which have coefficients in $\mathcal{O}_K$. Now we assume α_k is the smallest positive integer such that $\alpha_k h^{[k]} g^{n_1+n} \in \mathcal{O}_K[w]]$ and will show there exists an integer M such that $M h^{[k]} g^{n_1+n} \in \mathcal{O}_K[w]]$ for all integers k. By (20) we have

$$C\left(\alpha_k h^{[k]} \cdot h \cdot g^{n_1+n}\right) = (\alpha_k) C\left(h^{[k]}\right) \cdot C\left(h \cdot g^{n_1+n}\right) = C(h) \cdot C\left(\alpha_k h^{[k]} \cdot g^{n_1+n}\right).$$

In particular, for any positive integer d which divides α_k and satisfies $(d, C(h)) = \mathcal{O}_K$, then $(d) \subset C(\alpha_k h^{[k]} \cdot g^{n_1+n})$. Hence $\frac{\alpha_k}{d} h^{[k]} g^{n_1+n} \in \mathcal{O}_K[w]]$. By our choice of α_k, $d = 1$. Now let p be a rational prime number such that $(p, C(h)) \neq \mathcal{O}_K$ and let

$$e_p = \max\left\{\operatorname{ord}_{\wp} C(f)\right\}_{\text{all prime ideals } \wp \text{ in } \mathcal{O}_K \text{ above } p}.$$

If $p^{e_p+1} \mid \alpha_k$ then $C(h)C(\alpha_k h^{[k]} \cdot g^{n_1+n}) \subset (p^{e_p+1})$. Comparing the degrees of the prime ideals $\wp$ above p, we derive $(p) \subset C(\alpha_k h^{[k]} \cdot g^{n_1+n})$ which contradicts the choice of α_k. So $\operatorname{ord}_p \alpha_k \leqslant e_p$. We can take $M = \prod_p p^{e_p}$. Then $M h^{[k]} g^{n_1+n} \in \mathcal{O}_K[w]]$ for all k.

By (21), for any positive N, there exist rational integers β_j, $2 \leqslant j \leqslant N$, such that

$$M\left(h + \sum_{m \geqslant 2}^{N} \beta_m h^{[m]}\right) = M c_1 w + \sum_{m>N} b_m w^m \in \mathcal{O}_K[w]].$$

If $g^{n_1+n} = \sum_{m \geqslant m_0} a_m w^m$, then by our choice of M

$$M\left(h + \sum_{m \geqslant 2} \beta_m h^{[m]}\right) g^{n_1+n} = \sum_{m \geqslant m_0}^{m_0+N} M c_1 a_m w^{m+1} + \cdots \in \mathcal{O}_K[w]].$$

Since this is true for any N, we know $M c_1 g^{n_1+n} \in \mathcal{O}_K[w^{-1}, w]]$. □

References

[Atk67] A.O.L. Atkin, Proof of a conjecture of Ramanujan, Glasg. Math. J. 8 (1967) 14–32.

[ASD71] A.O.L. Atkin, H.P.F. Swinnerton-Dyer, Modular forms on noncongruence subgroups, in: Combinatorics, Univ. California, Los Angeles, CA, 1968, in: Proc. Sympos. Pure Math., vol. XIX, Amer. Math. Soc., Providence, RI, 1971, pp. 1–25.

[ALL08] A.O.L. Atkin, W.C. Li, L. Long, On Atkin and Swinnerton-Dyer congruence relations (2), Math. Ann. 340 (2) (2008) 335–358.

[AL07] A.O.L. Atkin, L. Long, On Atkin and Swinnerton-Dyer congruences of some noncongruence cuspforms, preprint, 2007.

[BLS64] H. Bass, M. Lazard, J.-P. Serre, Sous-groupes d'indice fini dans $\mathbf{SL}(n, \mathbf{Z})$, Bull. Amer. Math. Soc. 70 (1964) 385–392.

[Cre97] J.E. Cremona, Algorithms for Modular Elliptic Curves, second ed., Cambridge Univ. Press, Cambridge, 1997.

[CP03] C.J. Cummins, S. Pauli, Congruence subgroups of $\mathrm{PSL}(2, \mathbb{Z})$ of genus less than or equal to 24, Experiment. Math. 12 (2) (2003) 243–255, http://www.math.tu-berlin.de/~pauli/congruence/.

[Fri86] R. Fricke, Über die Substitutionsgruppen, welche zu den aus dem Legendre'schen Integralmodul $k^2(w)$ gezogenen Wurzeln gehören (Mit einer Figurentafel), Math. Ann. 28 (1886) 99–118.

[Hsu96] T. Hsu, Identifying congruence subgroups of the modular group, Proc. Amer. Math. Soc. 124 (5) (1996) 1351–1359.

[Jac85] N. Jacobson, Basic Algebra. I, second ed., W.H. Freeman and Company, New York, 1985.

[Kob93] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, second ed., Springer-Verlag, New York, 1993.

[LLY05] W.C. Li, L. Long, Z. Yang, On Atkin and Swinnerton-Dyer congruence relations, J. Number Theory 113 (1) (2005) 117–148.

[Lon07] L. Long, On Atkin and Swinnerton-Dyer congruence relations (3), math.NT/0701310, 2007.

[Mil69a] M.H. Millington, On cycloidal subgroups of the modular group, Proc. London Math. Soc. (3) 19 (1969) 164–176.

[Mil69b] M.H. Millington, Subgroups of the classical modular group, J. London Math. Soc. (2) 1 (1969) 351–357.

[New65] M. Newman, Normal subgroups of the modular group which are not congruence subgroups, Proc. Amer. Math. Soc. 16 (1965) 831–832.

[Pic86] G. Pick, Über gewisse ganzzahlige lineare Substitutionen, welche sich nicht durch algebraische Congruenzen erklären lassen, Math. Ann. 28 (1886) 119–124.

[Ran67] R.A. Rankin, Lattice subgroups of free congruence groups, Invent. Math. 2 (1967) 215–221.

[Rei58] I. Reiner, Normal subgroups of the unimodular group, Illinois J. Math. 2 (1958) 142–144.

[Sch85] A.J. Scholl, Modular forms and de Rham cohomology; Atkin–Swinnerton-Dyer congruences, Invent. Math. 79 (1) (1985) 49–77.

[Sch88] A.J. Scholl, The l-adic representations attached to a certain noncongruence subgroup, J. Reine Angew. Math. 392 (1988) 1–15.

[Shi71] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan, vol. 11, Iwanami Shoten Publ., Tokyo, 1971, Kanô Memorial Lectures, No. 1.

[Sil86] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[Sto84] W.W. Stothers, Level and index in the modular group, Proc. Roy. Soc. Edinburgh Sect. A 99 (1–2) (1984) 115–126.

[Woh64] K. Wohlfahrt, An extension of F. Klein's level concept, Illinois J. Math. 8 (1964) 529–535.