1-1-2009

On modular forms for some noncongruence subgroups of SL2() II

Chris Kurth
Iowa State University

Ling Long
Iowa State University

Recommended Citation
Kurth, C., & Long, L. (2009). On modular forms for some noncongruence subgroups of SL2() II. *Bulletin of the London Mathematical Society, 41* (4), 589-598. https://doi.org/10.1112/blms/bdp061

ON MODULAR FORMS FOR SOME NONCONGRUENCE SUBGROUPS OF $\mathrm{SL}_2(\mathbb{Z})$ II

CHRIS KURTH AND LING LONG

Abstract. In this paper we show two classes of noncongruence subgroups satisfy the so-called unbounded denominator property. In particular, we establish our conjecture in [KL08] which says that every type II noncongruence character group of $\Gamma^0(11)$ satisfies the unbounded denominator property.

1. Introduction

It is well-known that the modular group $\mathrm{SL}_2(\mathbb{Z})$ fails to satisfy the so-called congruence property. As a matter of fact, the majority of finite index subgroups of the modular group are noncongruence. Identifying congruence subgroups of the modular group is a fundamental question. Although there are explicit algorithms available for this purpose [LLT95, Hsu96], they require very specific data of the group and hence are not always effective. Another plausible approach is via the modular forms for these groups. For instance, if a finite index subgroup Γ of the modular group has genus 0, then knowing that any of its Hauptmoduls is congruence (in the sense that it is invariant under a congruence subgroup) is sufficient to conclude that Γ is congruence. For many interesting cases, the coefficients of these Hauptmoduls are algebraic or combinatorial. A classical example is that the Fourier coefficients of the modular j-function are related to the dimensions of the irreducible representations of the monster group. Consequently, these Hauptmoduls have algebraically integral Fourier coefficients. A general belief is that a meromorphic modular form with algebraically integral Fourier coefficients must be congruence. It is worth mentioning that if this is the case then the graded dimension of any C_2-cofinite, holomorphic vertex operator algebra over $\mathbb{C}$ is a congruence modular function (cf. [DLM00] and [MK08, Section 4]).

In this paper, we will restrict ourselves to a class of noncongruence subgroups, called noncongruence character groups, which are closely related to congruence subgroups. A group Γ is called a character group of another finite index group Γ^0 of the modular group if Γ is normal in Γ^0 with finite abelian quotient. By the definition, there is a surjective homomorphism

$$\phi : \Gamma^0 \twoheadrightarrow G \tag{1}$$

such that $\Gamma = \ker \phi$ for some finite abelian group G. Note that there exists another surjective homomorphism $\pi : \Gamma^0 \twoheadrightarrow H_1(X_{\Gamma^0}, \mathbb{Z})$, the first homology group of the compactified modular curve X_{Γ^0} for Γ^0 (cf. [Man72, Prop. 1.6]). In [KL08], we

2000 *Mathematics Subject Classification.* 11F11.

Both authors are supported in part by the NSA grant #H98230-08-1-0076.

distinguish two types of character groups based on the level structures. A character group Γ of Γ^0 is said to be of *type II* if the modular curve for Γ is a finite covering of X_{Γ^0} unramified at the cusps. Otherwise the group Γ is said to be of *type I*. In particular, a character group Γ of Γ^0 is said to be of *type II(A)* if ϕ factors through the kernel of π; and is said to be be *type I(A)*, if the modular curve for Γ is a finite covering of X_{Γ^0} unramified outside of the cusps of X_{Γ^0} and $\pi(\ker\phi) = H_1(X_{\Gamma^0}, \mathbb{Z})$. In the case that Γ is a type I(A) character group of Γ^0 with Γ^0/Γ isomorphic to $\mathbb{Z}/n\mathbb{Z}$, the field of meromorphic modular functions for Γ is a cyclic field extension of that for Γ^0 which can be generated by $\sqrt[n]{f}$ for some modular function f for Γ^0 whose zeros and poles are located at the cusps of Γ^0. A modular function f with zeros and poles only at the cusps is called a modular unit (cf. [KL81]).

A noncongruence subgroup Γ is said to satisfy the **condition (UBD)** if the following conditions hold:

> *If f is an integral weight modular form for Γ such that*
> (1) *f is holomorphic on the upper half plane with poles only at the cusps;*
> (2) *f has algebraic Fourier coefficients at infinity;*
> (3) *f is not a modular form for Γ^c, the congruence closure of Γ in $\mathrm{SL}_2(\mathbb{Z})$,*
>
> *then f has **unbounded denominators**, i.e. there is no algebraic integer $A \neq 0$ such that $A \cdot f$ has algebraic integer coefficients at infinity.*

It is conjectured that every noncongruence group satisfies (UBD). If the conjecture is true, it provides a clear and nice criterion for identifying which modular forms with algebraic coefficients are congruence.

In this short note we prove the following two results using a similar argument which is derived from our previous discussion in [KL08]:

Theorem 1. *Let $\Gamma^0 = \Gamma_0(M)$ with M a square-free positive integer whose genus is at least 1. Then every type I(A) noncongruence character group Γ of $\Gamma_0(M)$ satisfies the condition (UBD).*

Theorem 2. *Let Γ^0 be a genus 1 congruence subgroup whose modular curve has no complex multiplication. Then there exists an integer $M(\Gamma^0)$ depending on Γ^0 such that for any positive integer n relatively prime to $M(\Gamma^0)$, every index-n type II(A) character group of Γ^0 satisfies the condition (UBD).*

This result overrides Theorem 3 of [KL08] when the modular curve X_{Γ^0} has no complex multiplication. For instance, $X_{\Gamma^0(11)}$ has no complex multiplication. Cummins and Pauli have classified all congruence subgroups up to genus 25 [CP03]. Using their database together with a computational package like MAGMA one can check explicitly which genus 1 congruence subgroups satisfy the condition of Theorem 2.

As a corollary, we will prove Conjecture 37 of [KL08].

Theorem 3. *Every noncongruence type II character group of $\Gamma^0(11)$ satisfies the condition (UBD).*

Note that a modular form for a character group is automatically a generalized modular form (GMF) (cf. [KM03] and also the definition in [MK08]). Kohnen and Mason pointed out to the second author that many GMF's have unbounded denominators. They obtained several results in [MK08] regarding the coefficients of GMF's with empty or cuspidal divisor.

In the appendix, we show that if the expansion of a modular form at one cusp has algebraic coefficients, then so does its expansion at any other cusp. It is a fact well-known to the experts and is used in the proofs, but since we could not find a proof in the literature we provide one here for the sake of completeness.

For convenience, we say a Laurent power series satisfies the condition (**FS-AB**) if its coefficients are algebraic and have bounded denominators.

2. Type I(A) character subgroups of $\Gamma_0(M)$ with M square-free

Lemma 4. *If Γ is a type I(A) (resp. II(A)) character group of Γ^0, then $\Gamma = \bigcap_{i=1}^{s} \Gamma_i$ such that each Γ_i is a type I(A) (resp. II(A)) character group of Γ^0 with $\Gamma^0/\Gamma_i \cong \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ for some primes p_i and positive integers e_i.*

Proof. By the definition of character groups, there is a surjective homomorphism $\phi : \Gamma^0 \to G$ where G is a finite abelian group such that $\Gamma = \ker \phi$. By the Fundamental Theorem of Finite Abelian Groups, $G \cong \bigoplus_{i=1}^{s} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. Let $\phi_i : \Gamma^0 \to \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ be the natural projections of ϕ and $\Gamma_i = \ker \phi_i$. Therefore, $\Gamma = \bigcap_{i=1}^{s} \Gamma_i$. If Γ is a type I(A) (resp. II(A)) character group of Γ^0 then by the definitions each Γ_i as a character group of Γ^0 is also of type I(A) (resp. II(A)). □

Let $\mathfrak{M}_\Gamma$ (resp. $\mathfrak{M}_{\Gamma^0}$) denote the field of meromorphic modular functions for Γ (resp. Γ^0). Let $c_1, \cdots, c_{t-1}, c_t = \infty$ be the list of cusps of X_{Γ^0} with γ_i the generator of the stabilizer of c_i. By the Manin-Drinfeld theorem, $(c_i)-(\infty)$ is an order N_i torsion point of the Jacobian $J_0(M)$ of $X_{\Gamma_0(M)}$. Therefore, there is a modular function $h_i \in \mathfrak{M}_{\Gamma_0(M)}$ such that $\mathrm{div}(h_i) = N_i((c_i) - (\infty))$ for every $i = 1, \cdots, t-1$. For a fixed prime number p, the extension $\mathfrak{M}_{\Gamma^0}(\sqrt[p]{h_i})$ over $\mathfrak{M}_{\Gamma^0}$ corresponds to a type I(A) character group of Γ^0 if, and only if, N_i is relatively prime to p.

Lemma 5. (1) *If Γ is a type I(A) character group of Γ^0, then any intermediate group sitting between Γ^0 and Γ is also a type I(A) character group of Γ^0.*
(2) *The intersection of two type I(A) character groups of Γ^0 is also a type I(A) character group of Γ^0.*
(3) *For any integer $e \geq 1$, the extension $\mathfrak{M}_{\Gamma^0}(\sqrt[p^e]{h_i})$ over $\mathfrak{M}_{\Gamma^0}$ corresponds to a type I(A) character group of Γ^0 if, and only if, N_i is relatively prime to p.*
(4) *There are $p^{e(t-2)} + p^{e(t-3)} + \cdots + 1$ non-isomorphic index-p^e type I(A) character groups of Γ^0 whose field extensions over $\mathfrak{M}_{\Gamma^0}$ can be generated by modular units.*

Proof. By the definition of type I(A) character groups, it is straightforward to verify the first two claims.

By part (1), we know that for any integer $e \geq 1$, $\mathfrak{M}_{\Gamma^0}(\sqrt[p^e]{h_i})$ corresponds to a type I(A) character group of Γ^0 if and only if N_i is relatively prime to p. By part (2), $\sqrt[p^e]{h_1^{a_1} \cdots h_{t-1}^{a_{t-1}}}$ with integer a_i's gives rise to a type I(A) character group if and only if p is relatively prime to every N_i. Since each h_i is a modular unit, so is $\sqrt[p^e]{h_1^{a_1} \cdots h_{t-1}^{a_{t-1}}}$. Treating $(a_1, \ldots, a_{t-1})$ as an element of $\mathbb{P}^{t-2}(\mathbb{Z}/p^e\mathbb{Z})$, there is one non-isomorphic index-p^e type I(A) character group of Γ^0, for each element of $\mathbb{P}^{t-2}(\mathbb{Z}/p^e\mathbb{Z})$, namely $\frac{p^{e(t-1)}-1}{p^e-1}$ such groups up to isomorphism.

□

Lemma 6. *If Γ is a type I(A) character group of Γ^0 with $\Gamma^0/\Gamma \cong \mathbb{Z}/p^e\mathbb{Z}$ for some prime power p^e, then $\mathfrak{M}_\Gamma = \mathfrak{M}_{\Gamma^0}(\sqrt[p^e]{f})$ for some modular unit f in $\mathfrak{M}_{\Gamma^0}$.*

Proof. By the Galois correspondence, $\mathfrak{M}_\Gamma$ is a finite Galois extension of $\mathfrak{M}_{\Gamma^0}$ whose Galois group is isomorphic to Γ^0/Γ. Hence $\mathfrak{M}_\Gamma = \mathfrak{M}_{\Gamma^0}(\sqrt[p^e]{f})$ for some $f \in \mathfrak{M}_{\Gamma^0}$.

Now we show that f can be chosen as a modular unit. If $\phi : \Gamma^0 \to \mathbb{Z}/p^e\mathbb{Z}$ is a group homomorphism such that $\Gamma = \ker\phi$ is of type I(A), then ϕ is completely determined by the parabolic elements $\gamma_1, \cdots, \gamma_{t-1}$ and N_i has to be relatively prime to the order of $\phi(\gamma_i)$ for every $i = 1, \cdots, t-1$. By a counting argument, we know there are $\frac{p^{e(t-1)}-1}{p^e-1}$ non-isomorphic index-p^e type I(A) character groups of Γ^0 with cyclic quotient. By part (4) of the previous lemma, this is the same number as arise from modular units, proving the claim. □

Recall that $\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n)$, $q = e^{2\pi iz}$ is the classical Dedekind eta function. Below, we call a function f an eta quotient if $f = \prod_{j=1}^t \eta(a_j z)^{e_j}$ for $a_j \in \mathbb{N}$ listed in a strictly increasing order and $e_j \in \mathbb{Z}\setminus\{0\}$.

Theorem 7 (Tagaki [Tak97])**.** *Up to a scalar multiple, every modular unit for $\Gamma_0(M)$ with the positive integer M square-free is an eta quotient.*

The following lemma is a special case of Lemma 11 in [KL08]. For any $n \geq 1$ and with a principal branch fixed, we formally write

$$(1+x)^{1/n} = \sqrt[n]{1+x} = \sum_{m\geq 0} \frac{\left(\frac{1}{n}\right)_m}{m!} x^m, \tag{2}$$

where $(\frac{1}{n})_m = \frac{1}{n}(\frac{1}{n}-1)\cdots(\frac{1}{n}-m+1)$.

Lemma 8. *Let n be any natural number and $f = 1+\sum_{m\geq 1} a(m)w^m, a(m) \in \mathbb{Z}$ for all m. In terms of (2), we expand $\sqrt[n]{f} = \sum_{m\geq 0} b(m)w^m$, with $b(m) \in \mathbb{Z}[1/n]$ formally. Let p be a prime factor of n. If there exists one $b(m)$ which is not p-integral, then*

$$\limsup_{m\to\infty} (-\mathrm{ord}_p b(m)) \to \infty.$$

In other words, $\{b(m)\}$ has unbounded denominators.

Lemma 9. *Let $f = \prod_{j=1}^t \eta(a_j z)^{e_j}$ be an eta quotient. For any prime power p^e not dividing the greatest common divisor of the e_j's, the Fourier coefficients of $\sqrt[p^e]{f}$ have unbounded denominators.*

Proof. We may assume the greatest common divisor of the exponent e_j's is 1. We now show that the coefficients of $\sqrt[p]{f}$ have unbounded denominators. If not, by Lemma 8 the expansion $\sqrt[p]{\prod_{j=1}^{t}\eta(a_jz)^{e_j}} = \sum b(n)q^{n/p}$ satisfies $b(n)\in\mathbb{Z}$. By Proposition 2.1 of [BKO04] we can write $\sum b(n)q^{n/p}$ uniquely into the form $q^r\prod_{n\geq 1}(1-q^n)^{c(n)}$ for some rational number r and complex numbers $c(n)$'s which can be determined by the $b(n)$'s recursively. It is straightforward to check that if the $b(n)$'s are all integers then so are the $c(n)$'s. On the other hand it is easy to rewrite $\sqrt[p]{\prod_{j=1}^{t}\eta(a_jz)^{e_j}}$ into the infinite product form $q^{r'}\prod_{n\geq 1}(1-q^n)^{c'(n)}$ directly. If n_0 is the least positive integer such that $p\nmid e_{n_0}$ then $c'(a_{n_0})$ is not an integer. By the uniqueness of the $c(n)$'s, $c(n)=c'(n)$ which leads to a contradiction. □

Corollary 10. *Let $f=\prod_{j=1}^{t}\eta(a_jz)^{e_j}$ be an eta quotient, d be the greatest common divisor of the e_j's. If a prime $p\nmid d$, then the Fourier coefficients of $\sqrt[p]{f}$ at infinity have unbounded denominators, and so do the Fourier coefficients at any cusp of Γ. The modular function $\sqrt[p]{f}$ is modular for a congruence subgroup if and only if p divides d.*

Proof. Let c be a cusp and $\gamma_c\in\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_c\infty=c$. The expansion of any modular form h at c is the expansion of $h|_{\gamma_c}$ at infinity. Since f is an eta quotient, $f|_{\gamma_c}$ is also an eta quotient by the well-known transformation formulae of the eta function.

If $p\mid d$, $\sqrt[p]{f}$ is an eta quotient and hence congruence, then so is $\sqrt[p]{f}|_\gamma$ for any $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Thus the Fourier expansion of f at any cusp satisfies (FS-AB). Conversely, if $\sqrt[p]{f}|_\gamma$ satisfies (FS-AB) for some γ, then $\sqrt[p]{f}|_\gamma$ is an eta quotient and hence congruence. This implies $\sqrt[p]{f}$ is also congruence. Therefore it is an eta quotient and $p\mid d$. □

Lemma 11. *If $g(z)$ is a modular function of a congruence group with poles only at the cusps and algebraic Fourier coefficients, then there is a constant A such that $A\cdot g(z)$ has algebraic integer Fourier coefficients.*

Proof. Let $\Delta(z)=\eta^{24}(z)$ which is a cuspform for $\mathrm{SL}_2(\mathbb{Z})$ with series:

$$\Delta(z)=q-24q^2+252q^3+\dots$$

In particular, the Fourier coefficients are all integers. Multiplying g by powers of Δ will kill the poles at the cusps, hence $\Delta^n g$ is also a cuspform for sufficiently large n, and there is a constant A such that $A\cdot\Delta^n g$ has algebraic integer Fourier coefficients (as a result of Theorem 3.52 in [Shi71]). But $\frac{1}{\Delta}$ has algebraic integer Fourier coefficients as well, since

$$\frac{1}{\Delta}=\frac{1}{q}\cdot\frac{1}{1+(\Delta/q-1)}=\frac{1}{q}\left(1-\left(\frac{\Delta}{q}-1\right)+\left(\frac{\Delta}{q}-1\right)^2-\dots\right)$$

So $A\cdot g=A\Delta^{-n}\Delta^n g$ has algebraic integer Fourier coefficients. □

We are ready to prove Theorem 1.

Proof of Theorem 1. Let Γ be a type I(A) noncongruence character group of $\Gamma_0(M)$. Assume $\Gamma_0(M)/\Gamma\cong\bigoplus_{i=1}^{s}\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ and $\Gamma\cong\bigcap_{i=1}^{s}\Gamma_i$ where Γ_i are type I(A) character groups of $\Gamma_0(M)$ with $\Gamma_0(M)/\Gamma_i\cong\langle\gamma_i\Gamma\rangle\cong\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ for some $\gamma_i\in\Gamma_0(M)$ and certain

prime powers $p_i^{e_i}$. We further assume that each $\mathfrak{M}_{\Gamma_i}$ is generated over $\mathfrak{M}_{\Gamma_0(M)}$ by $g_i = \sqrt[p^{e_i}]{f_i}$ with f_i being a modular unit for $\Gamma_0(M)$. By Theorem 7, we can assume that each f_i is an eta quotient. Consequently, a basis of $\mathfrak{M}_\Gamma$ over $\mathfrak{M}_{\Gamma_0(M)}$ is $S = \{\prod_{i=1}^s g_i^{n_i}\}_{0\le n_i\le p^{e_i}-1}$.

Let h be an integral weight k modular form for Γ holomorphic on the upper half plane and satisfying (FS-AB). Up to multiplying with a suitable newform for $\Gamma_0(M)$ one can assume k is a multiple of 12. Dividing by $\Delta^{k/12}$ we obtain a modular function for Γ satisfying (FS-AB). From now on we assume that h is of weight 0. The goal is to show such a modular function h, holomorphic on the upper half plane and satisfying (FS-AB), must be congruence.

Write $h = \sum_{I=(n_1,\cdots,n_s)} a_I \prod_{i=1}^s g_i^{n_i}$ with $a_I \in \mathfrak{M}_{\Gamma_0(M)}$. For convenience, we denote $\prod_{i=1}^s g_i^{n_i}$ by g^I. Note that $g_i|_{\gamma_j} = g_i$ if $i \neq j$ and $g_i|_{\gamma_i} = \mu_{p^e} g_i$ where μ_n stands for a primitive nth root of unity. So for every $\gamma\Gamma \in \Gamma_0(M)/\Gamma$, $g^I|_\gamma = \phi_I(\gamma)g^I$ for some character $\phi_I : \Gamma_0(M)/\Gamma \to \mathbb{C}^\times$ of $\Gamma_0(M)/\Gamma$. The ϕ_I's are non-isomorphic and they form the complete set of non-isomorphic characters of the abelian quotient group $\Gamma_0(M)/\Gamma$. Hence each $a_I g^I$ is a linear combination of $h|_{\gamma_1^{n_1}\cdots\gamma_s^{n_s}}$ with $n_i \in \{0,\cdots,p^{e_i}-1\}$ and some scalars in a cyclotomic field. Note that each $h|_{\gamma_1^{n_1}\cdots\gamma_s^{n_s}}$ is also holomorphic on the upper half plane with algebraic coefficients (cf. Appendix), thus so is each $a_I g^I$. Also each g_i is nonzero in the upper half plane, so each modular function $a_I \in \mathfrak{M}_{\Gamma_0(M)}$ is also holomorphic on the upper half plane with algebraic coefficients. By Lemma 11, each a_I satisfies (FS-AB).

We partition the basis S into two sets S_c and S_n. An element in S belongs to S_c if it is congruence and otherwise it belongs to S_n. Note that $(h)_c = \sum_{I\in S_c} a_I g^I$ is a congruence modular form which is holomorphic on the upper half plane, hence it satisfies (FS-AB). So $(h)_n = \sum_{I\in S_n} a_I g^I = 0$ also satisfies (FS-AB).

If there are g^I and $g^{I'}$ in S_n such that $g^{I'}/g^I = E$ is an eta product, then $a_I g^I + a'_I g^{I'} = (a_I + a'_I E)g^I$ with $a_I + a'_I E$ being congruence and satisfying (FS-AB). Hence one can further assume that for every two elements in S_n their quotient is not a congruence modular form.

With the assumptions above, let $M((h)_n)$ be the number of nonzero a_I's in the expression of $(h)_n$. We will conclude $M((h)_n) = 0$ by using an argument similar to the proof of Lemma 13 in [KL08] to exclude the remaining possibilities.

Case 1: $M((h)_n) = 1$. In this case $a_I g^I$ satisfies (FS-AB) for some nonzero a_I satisfying (FS-AB). Since $(g^I)^{|\Gamma_0(M)/\Gamma|}$ is an eta quotient, it satisfies (FS-AB). By Lemma 39 of [KL08], $(g^I)^{1+|\Gamma_0(M)/\Gamma|}$ satisfies (FS-AB). Note that the reciprocal of the eta quotient $(g^I)^{|\Gamma_0(M)/\Gamma|}$ satisfies (FS-AB). It follows g^I also satisfies (FS-AB). By Lemma 9, g^I is congruence. This contradicts our assumption on $(h)_n$.

Case 2: $M((h)_n) > 1$. Let $\mathcal{D}$ be the differential operator defined in the proof of Lemma 13 in [KL08]. If h is a formal power series whose coefficients have bounded denominators, then so is $\mathcal{D}(h)$. Following the argument of the proof of Lemma 13 in [KL08], there exists a nonzero modular function b_I for $\Gamma_0(M)$ holomorphic on the upper half plane satisfying (FS-AB) such that $\widetilde{h} = (b_I - a_I\mathcal{D})((h)_n) \neq 0$ and $(\widetilde{h})_n = \widetilde{h}$. Moreover, $M((h)_n) > M(\widetilde{h})$. By induction, this case reduces to back to case 1.

So $h = (h)_c$ is congruence. □

In this proof, if we replace h by $h|_\gamma$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ then each $h|_\gamma$ is also a combination of nth roots of eta quotients whose coefficients are congruence modular forms holomorphic on the upper half plane. Consequently, one can strengthen the (UBD) condition in this case to: for every genuine noncongruence modular form, holomorphic on the upper-half plane with algebraic coefficients, its Fourier expansion at *every cusp* has *unbounded denominators*.

3. Type II(A) character groups of genus 1 congruence subgroups

In this section, we follow closely [KL08] and the approach in the previous section. Let Γ^0 be a genus 1 congruence subgroup whose modular curve X_{Γ^0} is defined over a number field K and has no complex multiplication. By the theory of elliptic functions, there exist two modular functions x and y for Γ^0 with poles of order 2 and 3 respectively at infinity and holomorphic everywhere else. The modular functions x and y satisfy $y^2 = x^3 + Ax + B$ for some $A, B \in K$. Moreover, the Fourier coefficients of $x = w^{-2} + a_{-1}w^{-1} + \cdots$ and $y = w^{-3} + b_{-2}w^{-2} + \cdots, w = e^{2\pi i/\mu}$ are in K, where μ is the cusp width of Γ^0 at infinity. By Lemma 11, x has bounded denominators and there exists a rational integer $N(\Gamma^0)$ depending on Γ^0 such that for all prime ideals $\wp$ of $\mathcal{O}_K$ not dividing $N(\Gamma^0)$, the coefficients of x are all $\wp$-integral. Let $R = \mathbb{Z}[A, B]$. By [Sil86, Ex. 3.7 pp. 105], there exists a polynomial

$$\psi_p(x) = px^{(p^2-1)/2} + c_{(p^2-1)/2-1}x^{(p^2-1)/2-1} + \cdots + c_1x + c_0 \in R[x] \tag{3}$$

satisfied by the x-coordinates of the order-p points of X_{Γ^0}. Since $X_{\Gamma^0}[p]$ over $\mathbb{F}_p$ is isomorphic to either $\{0\}$ or $\mathbb{Z}/p\mathbb{Z}$ (cf. [Sil86, Theorem 3.1]), $p \nmid c_n$ for some n. It follows that there exists one p-torsion point P_0, whose x-coordinate is not algebraically integral over $\wp_0$ for some prime ideal above p. By a result of Serre [Ser76], the homomorphism

$$\varphi_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(X_{\Gamma^0}[p]) \cong GL_2(\mathbb{F}_p) \tag{4}$$

on the p-torsion points of X_{Γ^0} is surjective for almost all primes p when X_{Γ^0} has no complex multiplication. When φ_p is surjective, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $X_{\Gamma^0}[p]$ transitively. Consequently for any $P \in X_{\Gamma^0}[p]$, $x(P)$ is not algebraically integral over some prime $\wp$ above p.

Lemma 12. *If α is an algebraic number which is not $\wp$-integral for some prime ideal $\wp \nmid N(\Gamma^0)$, then the Laurent power series $(x-\alpha)^{-1}$ in w has unbounded denominators.*

Proof. Assume $x = w^{-2} + a_{-1}w^{-1} + a_0 + \cdots$. It is equivalent to show that $(1 + a_{-1}w + (a_0 - \alpha)w^2 + \cdots)^{-1} = 1 + \beta + \beta^2 + \cdots = 1 + \sum c(n)w^n$ has unbounded denominators where $\beta = -(a_{-1}w + (a_0 - \alpha)w^2 + \cdots)$. It is straightforward to verify that if $\mathrm{ord}_\wp \alpha = -r$, then $\mathrm{ord}_\wp c(2n) = -nr$. So $(x-\alpha)^{-1}$ has unbounded denominators $\wp$-adically. □

Given a p-torsion point P of X_{Γ^0}, let $f_P \in \mathfrak{M}_{\Gamma^0}$ be a modular function whose divisor satisfies that $\mathrm{div} f_P = p(\infty) - p(P)$. We can assume that the coefficients of f_P are algebraic ([KL08, Lemma 23]). We choose f_{-P} in a similar way.

Lemma 13. *Let p be a prime not dividing $N(\Gamma^0)$, f_P and f_{-P} as above. Then at least one of $(f_P)^{1/p}$ or $(f_{-P})^{1/p}$ has unbounded denominators.*

Proof. By checking the divisors we know that $(f_P f_{-P})^{1/p} = (x - x(P))^{-1}$ up to a scalar. By the previous lemma $(f_P f_{-P})^{1/p}$ has unbounded denominators. Thus, at least one of $(f_P)^{1/p}$ or $(f_{-P})^{1/p}$ satisfies the unbounded denominator property. □

Without loss of generality we assume that $g_P = \sqrt[p]{f_P}$ has unbounded denominators $\wp$-adically for some prime $\wp$ above p. So does $(g_P)^j$ for any integer j which is relatively prime to p. Therefore,

Lemma 14. *Under the above assumptions, $(g_P)^j$ does not satisfies (FS-AB) for any integer $j \in \{p+1, p+2, \cdots, 2p-1\}$,*

Theorem 15. *Let Γ^0 be a genus 1 congruence subgroup whose modular curve has no complex multiplication. Then for almost all primes p, every index-p type II(A) character group of Γ^0 satisfies the condition (UBD).*

Proof. Let p be a prime which is relatively prime to $N(\Gamma^0)$ and such that the homomorphism φ_p (4) is surjective. Let Γ be an index-p type II(A) character group of Γ^0. From [KL08, Proposition 25], $\mathfrak{M}_\Gamma = \mathfrak{M}_{\Gamma^0}(g_P)$ for some g_P as above. We will show that such a group Γ satisfies the condition (UBD). If not, one can construct a genuine noncongruence modular function $f \in \mathfrak{M}_\Gamma$ which is holomorphic on the upper half plane and satisfies (FS-AB) by Lemma 11. We can write $f = \sum_{j=0}^{p-1} a_j g_P^j, a_j \in \mathfrak{M}_{\Gamma^0}$. Assume $\Gamma^0/\Gamma = \langle \gamma\Gamma \rangle$. Then $g_P|_\gamma = e^{2\pi i/p} g_P$. Since $f|_\gamma$ is also holomorphic on the upper half plane, so is every $a_j g_P^j$ which is a combination of $f|_{\gamma^j}$'s. So the poles of the congruence modular functions a_j are supported at the cusps. Thus each a_j satisfies (FS-AB) by Lemma 11. By Lemma 13 of [KL08] (and the proof of Theorem 1), for some $j \in \{p+1, \cdots, 2p-1\}$ ${g_P}^j$ satisfies (FS-AB) which contradicts Lemma 14. □

Proof of Theorem 2. Let $M(\Gamma^0)$ be the product of $N(\Gamma^0)$ and all primes p such that ϕ_p is not surjective. Now let Γ be an index-n type II(A) character group of Γ^0 such that $(n, M(\Gamma^0)) = 1$. By Lemma 4, $\Gamma = \bigcap_{i=1}^s \Gamma_i$ where each Γ_i is a type II(A) character group of Γ^0 with $\Gamma/\Gamma^i \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$ for some prime power $p^{e_i} > 1$ relatively prime to $M(\Gamma^0)$. Because $\mathfrak{M}_{\Gamma_i}$ is a cyclic extension over $\mathfrak{M}_{\Gamma^0}$ of order p^{e_i}, it is generated by some modular function g_i. Let G_i be the unique index-p subgroup of Γ^0 which contains Γ_i. By the proof of the previous theorem, $\mathfrak{M}_{G_i} = \mathfrak{M}_{\Gamma^0}(g_P)$ for some modular function g_P as before. Moreover, we can assume that g_P has unbounded denominators and $g_i^{p^{e_i-1}} = g_P$. It follows that g_i has unbounded denominators too.

Like the case in Section 2, the set of modular functions $S = \{\prod_{i=1}^s g_i^{n_i}\}_{0 \le n_i \le p^{e_i}-1}$ is a basis of $\mathfrak{M}_\Gamma$ over $\mathfrak{M}_{\Gamma^0}$. If h is a modular function for Γ^0 which is holomorphic on the upper half plane and satisfies (FS-AB), then following the argument of the proof of Theorem 1 we know h must be congruence. (Under our assumption on n, $S_n = S$ in this case.) This implies the claim of Theorem 2. □

Proof of Theorem 3. Since the modular curve for $\Gamma^0(11)$ has no elliptic points, a type II character group Γ of $\Gamma^0(11)$ is automatically of type II(A).

We now show that $M(\Gamma^0(11)) = 5$. By a result of Cojocaru [Coj05], when $p > 37$, ϕ_p is surjective for the elliptic curve $X_{\Gamma^0(11)}$. Thus it boils down to checking that the polynomial $\psi_p(x)$ (cf. (3)) is irreducible over $\mathbb{Q}$ when $p \leq 37$ and $p \neq 5$, which can be done computationally. Therefore, Theorem 2 and [KL08, Theorem 36] imply that every type II noncongruence subgroup of $\Gamma^0(11)$ satisfies the condition (UBD), which is equivalent to the claim of [KL08, Conjecture 37].

□

4. Appendix

The goal of this appendix is to show the following proposition used in the previous proof.

Proposition 16. *Let f be a modular function for Γ whose Fourier expansion about ∞ has coefficients in a number field K. Then for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the Fourier expansion of $f|_\gamma$ about ∞, or the expansion of f at the cusp $\gamma \cdot \infty$, also has coefficients in number field K' (K' may be larger than K in general).*

Let $j(z)$ be the classical modular j-function. By Theorem 1 of [ASD71] there is an irreducible polynomial $g(x, y) \in \mathbb{C}[x, y]$ such that $g(f, j) = 0$. Since both f and j have algebraic coefficients at infinity, one can use an elementary argument to show that up to a scalar $g(x, y) \in K'[x, y]$ for some number field K'. Since $j|_\gamma = j$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $g(f|_\gamma, j) = 0$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. The claim of the proposition is equivalent to saying every solution of $g(f, j) = 0$, as a formal power series, has algebraic Fourier coefficients. For now on, we use $g(f, q)$ to denote a polynomial in variable f with coefficients in the ring of Laurent series in q.

Lemma 17. *Let M be a nonnegative integer. Then:*

$$\frac{d^M}{dq^M}\left(g(f(q), q)\right) = \sum_p \left(c_p \left(\frac{\partial^{n+M-d} g(f, q)}{\partial f^n \partial q^{M-d}} \right) \cdot \prod_{i=1}^{n} \frac{d^{d_i} f}{dq^{d_i}} \right)$$

where the sum ranges over all partitions

$$p : d_1 + \cdots + d_n = d,\ d_i \geq 1$$

of all $d \in [0, M]$ (where the partition of 0 is empty), and c_p is a combinatorial constant:

$$c_p = \binom{M}{d} \frac{d!}{d_1! \cdots d_n!} \cdot \frac{1}{\prod_{i=1}^{d} \#(i \in p)!}$$

Proof. First note that:

$$\frac{d}{dq}\left(\frac{\partial^{a+b} g(f, q)}{\partial f^a \partial q^b} \right) = \frac{\partial^{a+b+1} g}{\partial f^{a+1} \partial q^b} \frac{df}{dq} + \frac{\partial^{a+b+1} g}{\partial f^a \partial q^{b+1}}$$

We claim that every term of $\dfrac{d^m}{dq^m}(g(f(q), q))$ is of the form:

$$\frac{\partial^{n+m-d} g}{\partial f^n \partial q^{m-d}} \cdot \prod_{i=1}^{n} \frac{d^{d_i} f}{dq^{d_i}}$$

where $d_1 + \cdots + d_n = d \leq m$.

Suppose this is true for m. Then $\dfrac{d}{dq}\left(\dfrac{\partial^{n+m-d} g}{\partial f^n \partial q^{m-d}} \cdot \prod_{i=1}^{n} \dfrac{d^{d_i} f}{dq^{d_i}}\right)$ has three types of terms, corresponding to new partitions:

$$\frac{\partial^{n+m-d+1} g}{\partial f^{n+1} \partial q^{m-d}} \cdot \prod_{i=1}^{n+1} \frac{d^{d_i} f}{dq^{d_i}} \qquad \text{for } p : d_1 + \cdots + d_n + 1$$

$$\frac{\partial^{n+m-d+1} g}{\partial f^{n} \partial q^{m-d+1}} \cdot \prod_{i=1}^{n} \frac{d^{d_i} f}{dq^{d_i}} \qquad \text{for } p : d_1 + \cdots + d_n$$

$$\frac{\partial^{n+m-d} g}{\partial f^{n} \partial q^{m-d}} \cdot \prod_{i=1}^{n} \frac{d^{d_i} f}{dq^{d_i}} \qquad \text{for } p : d_1 + \cdots + (d_j + 1) + \cdots + d_n$$

where for the last type, there is one for each $1 \leq j \leq n$.

Thus differentiation on a term corresponding to a partition p splits p up into $n+2$ partitions: p itself, p appending "+1", and all terms p with 1 added to one of the elements of p.

To get the combinatorial coefficient, we count how many ways to get to a partition p in M steps using the three rules above. If $M > d$ there are steps where p doesn't change, and they can be put in any order, hence the $\binom{M}{d}$ term in c_p. The remaining steps consist of adding $+1$ to the d_i's, hence the multinomial coefficient, and the remaining term is to remove any overlap in counting when $d_i = d_j$ for some i and j. □

Let $g(x, q)$ be a degree N polynomial (in x) with coefficients in $K[[q]]$ for some field K:

$$g(x,q) \;=\; \sum_{i=0}^{N} g_i(q) x^i = \sum_{j=P}^{\infty} h_j(x) q^j \,.$$

We want to find $f(q)$ such that $g(f(q), q) = 0$. If the order of $f(q)$ at ∞ is Q then $q^{-Q} f(q)$ is holomorphic and non-zero at ∞, and it satisfies $\overline{g}(q^{-Q} f(q), q) = 0$ where

$$\overline{g}(x,q) = \sum_{i=0}^{N} (g_i(q) \cdot q^{Qi}) x^i \,.$$

So, in solving for $f(q)$, we can adjust the h_j polynomials and assume f is holomorphic and non-zero at ∞. Moreover, we can assume $P = 0$ (and hence each $g_i(q)$ is holomorphic at ∞) since we can multiply powers of q to both sides of $g(f(q), q) = 0$. Let:

$$f(q) = \sum_{i=0}^{\infty} a_i q^i \,.$$

We will plug these series into the Lemma. Note that:

$$\frac{\partial^{a+b} g(f,q)}{\partial f^a \partial q^b} = \sum_{j=b}^{\infty} h_j^{(a)}(f) j(j-1)\ldots(j-b+1) q^{j-b} \,.$$

So:

$$\left.\frac{\partial^{a+b} g(f,q)}{\partial f^a \partial q^b}\right|_{q=0} = b! h_b^{(a)}(a_0)\,.$$

Similarly:

$$\left.\frac{d^b f}{dq^b}\right|_{q=0} = b! a_b\,.$$

Now let Q_M be the Mth coefficient of $g(f(q),q)$. Since

$$Q_M = \frac{1}{M!}\frac{d^M}{dq^M} g(f(q),q)\Big|_{q=0}\,,$$

putting it all together we have:

$$\begin{aligned} Q_M &= \frac{1}{M!}\sum_p \left(c_p \frac{\partial^{n+M-d} g}{\partial f^n \partial q^{M-d}} \cdot \prod_{i=1}^n \frac{d^{d_i} f}{dq^{d_i}} \right)\Bigg|_{q=0} \\ &= \frac{1}{M!}\sum_p \left(\binom{M}{d} \frac{d!}{d_1!\cdots d_n!} \cdot \frac{1}{\prod_{i=1}^d \#(i\in p)!} \cdot (M-d)! h_{M-d}^{(n)}(a_0) \prod_{i=1}^n d_i! a_{d_i} \right) \\ &= \sum_p \frac{1}{\prod_{i=1}^d \#(i\in p)!} h_{M-d}^{(n)}(a_0) \prod_{i=1}^n a_{d_i}\,. \end{aligned}$$

For example:

$$\begin{aligned} Q_4 &= a_4 h_0'(a_0) + a_3 a_1 h_0''(a_0) + a_3 h_1'(a_0) + \frac{1}{2} a_2^2 h_0''(a_0) + \frac{1}{2} a_2 a_1^2 h_0'''(a_0) + \\ &\quad + a_2 a_1 h_1''(a_0) + a_2 h_2'(a_0) + \frac{1}{24} a_1^4 h_0''''(a_0) + \frac{1}{6} a_1^3 h_1'''(a_0) + \\ &\quad + \frac{1}{2} a_1^2 h_2''(a_0) + a_1 h_3'(a_0) + h_4(a_0)\,. \end{aligned}$$

We solve $g(f(q),q) = 0$ for the a_i's. Since $Q_0 = h_0(a_0)$, we pick a_0 to be any non-zero root of h_0, an (at most) Nth degree polynomial. If a_0 is a simple root we will see that we can successively solve each a_i. Suppose however that $h_0^{(i)}(a_0) = 0$ for all $i \in \{0,1,\ldots,w-1\}$ and $h_0^{(w)}(a_0) \neq 0$. If $w > 1$ then the a_i's cannot be solved. In this case, instead let $f = \sum a_i q^{i/w}$. Then replace $q^{1/w}$ with q and re-index h_j as h_{jw} and $h_j = 0$ whenever $j \not\equiv 0 \bmod w$. So we have:

$$\begin{aligned} f(q) &= \sum a_i q^i\,, \\ g(x) &= \sum h_{jw}(x) q^{jw}\,. \end{aligned}$$

Then $Q_i = 0$ for all i from 1 to $w-1$, because each of their terms contains either $h_0^{(j)}(a_0)$ for $j \in [0, w-1]$ or h_j for $j \in [1, w-1]$. The next non-zero term is:

$$Q_w = h_w(a_0) + a_1^w h_0^{(w)}(a_0)\,.$$

So we solve

$$a_1^w = \frac{-h_w(a_0)}{h_0^{(w)}(a_0)}.$$

There are two cases:

Case 1: If $a_1 \neq 0$ then there are exactly w choices for a_1 and they all differ by an wth root of unity. Moreover, all subsequent a_i's are uniquely determined because for example:

$$Q_{w+1} = a_1 h'_w(a_0) + a_1^{w+1} h_0^{(w+1)}(a_0) + a_1^{w-1} a_2 h_0^{(w)}(a_0)$$

can be solved for a_2. And more generally:

$$Q_{w+c} = a_1^{w-1} a_{c+1} h_0^{(w)}(a_0) + (\text{terms with all } a_i\text{'s having } i \leq c).$$

So we can solve for each a_{c+1}.

(In general, when calculating Q_M, the partitions that give (possibly) non-zero terms are partitions $d_1 + \cdots + d_n = d$ such that (1) $d \leq M$, (2) $M \equiv d \mod N$, and (3) $n \geq N$ if $M = d$.)

Case 2: On the other hand, if $a_1 = 0$, let $\overline{f}(q) = f(q) + q$ and $\overline{g}(x, q) = g(x - q, q)$. The coefficients of $\overline{f}$ and f are the same except the q-term is non-zero, and $\overline{g}(\overline{f}(q), q) = 0$. If we repeat the above process on $\overline{g}$ and $\overline{f}$ we go into Case 1 and get a sequence for $\overline{f}(q)$, and hence $f(q)$. There is some reindexing involved in this, but note that the "cusp width" w remains the same after the reindexing, because replacing x with $x - q$ in $g(x, q) = \sum h_j(x) q^j$ does not change the $h_0(x)$ term. That is to say, if

$$\overline{g}(x, q) = \sum_{j=0}^{\infty} \overline{h}_j(x) q^j$$

then $\overline{h}_0(x) = h_0(x)$.

Note that in this recursive solving process, we stay in the field K'. That is to say, $a_i \in K'$ for all i. This proves Proposition 16.

Acknowledgements

The authors would like to thank Prof. Wen-Ching Winnie Li and Prof. Yifan Yang for their valuable inputs.

References

[ASD71] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., 1971, pp. 1–25.

[BKO04] J. H. Bruinier, W. Kohnen, and K. Ono, *The arithmetic of the values of modular functions and the divisors of modular forms*, Compos. Math. **140** (2004), no. 3, 552–566.

[Coj05] A. C. Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31, With an appendix by Ernst Kani.

[CP03] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2, \mathbb{Z})$ *of genus less than or equal to 24*, Experiment. Math. http://www.math.tu-berlin.de/∼pauli/congruence/ **12** (2003), no. 2, 243–255.

[DLM00] C. Dong, H. Li, and G. Mason, *Modular-invariance of trace functions in orbifold theory and generalized Moonshine*, Comm. Math. Phys. **214** (2000), no. 1, 1–56.

[Hsu96] T. Hsu, *Identifying congruence subgroups of the modular group*, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1351–1359.

[KL81] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981.

[KL08] C. A. Kurth and L. Long, *On modular forms for some noncongruence arithmetic subgroups*, J. of Number Theory **128** (2008), no. 7, 1989–2009.

[KM03] M. Knopp and G. Mason, *Generalized modular forms*, J. Number Theory **99** (2003), no. 1, 1–28.

[LLT95] M. L. Lang, C. H. Lim, and S. P. Tan, *An algorithm for determining if a subgroup of the modular group is congruence*, J. London Math. Soc. (2) **51** (1995), no. 3, 491–502.

[Man72] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[MK08] G. Mmason and W. Kohnen, *On generalized modular forms and their applications*, Nagoya J. (to appear) (2008).

[Ser76] J. P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. (2) **22** (1976), no. 3-4, 227–260.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[Tak97] T. Takagi, *The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free*, J. Algebra **193** (1997), no. 1, 180–213.

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

E-mail address: kurthc@iastate.edu

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

E-mail address: linglong@iastate.edu