Algebra & Number Theory

Volume 11

2017

No. 5

Modular curves of prime-power level with infinitely many rational points

Andrew V. Sutherland and David Zywina

msp

ALGEBRA AND NUMBER THEORY 11:5 (2017)
dx.doi.org/10.2140/ant.2017.11.1199

Modular curves of prime-power level with infinitely many rational points

Andrew V. Sutherland and David Zywina

For each open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ containing $-I$ with full determinant, let $X_G/\mathbb{Q}$ denote the modular curve that loosely parametrizes elliptic curves whose Galois representation, which arises from the Galois action on its torsion points, has image contained in G. Up to conjugacy, we determine a complete list of the 248 such groups G of prime power level for which $X_G(\mathbb{Q})$ is infinite. For each G, we also construct explicit maps from each X_G to the j-line. This list consists of 220 modular curves of genus 0 and 28 modular curves of genus 1. For each prime ℓ, these results provide an explicit classification of the possible images of ℓ-adic Galois representations arising from elliptic curves over $\mathbb{Q}$ that is complete except for a finite set of exceptional j-invariants.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and denote its j-invariant by j_E. For each positive integer N, let $E[N]$ denote the N-torsion subgroup of $E(\bar{\mathbb{Q}})$, where $\bar{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. The natural action of the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ induces a Galois representation

$$\rho_{E,N} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

After choosing compatible bases for the torsion subgroups $E[N]$, these representations determine a Galois representation

$$\rho_E : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

whose composition with the projection $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ given by reduction modulo N is equal to $\rho_{E,N}$ for each N. The images of $\rho_{E,N}$ and ρ_E are uniquely determined up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{GL}_2(\hat{\mathbb{Z}})$, respectively. If E does not have complex multiplication (CM), then $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, by Serre's [1972] open image theorem, hence of finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Sutherland was supported by NSF grants DMS-1115455 and DMS-1522526.
MSC2010: primary 14G35; secondary 11F80, 11G05.
Keywords: modular curves, elliptic curves, Galois representations.

Let G be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that satisfies $\det(G)=\hat{\mathbb{Z}}^\times$ and $-I\in G$. Let N be the least positive integer such that G is the inverse image of its image under the reduction map $\mathrm{GL}_2(\hat{\mathbb{Z}})\to\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$; we call N the *level* of G.

Associated to G is a modular curve $X_G/\mathbb{Q}$; one can define X_G as the generic fiber of the smooth proper $\mathbb{Z}[1/N]$-scheme that is the coarse moduli space for the algebraic stack $\mathcal{M}_{\overline{G}}[1/N]$ in the sense of [Deligne and Rapoport 1973, §IV], where $\overline{G}$ denotes the image of G under reduction modulo N. See Section 2 for some background on X_G and an alternate description; in particular, it is a smooth projective geometrically integral curve defined over $\mathbb{Q}$.

When $G=\mathrm{GL}_2(\hat{\mathbb{Z}})$, the modular curve X_G is the j-line $\mathbb{P}^1_{\mathbb{Q}}=\mathbb{A}^1_{\mathbb{Q}}\cup\{\infty\}$. If G and G' are open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with $\det(G)=\det(G')=\hat{\mathbb{Z}}^\times$ and $-I\in G, G'$ such that $G\subseteq G'$, then there is a natural morphism $X_G\to X_{G'}$ of degree $[G':G]$. In particular, with $G'=\mathrm{GL}_2(\hat{\mathbb{Z}})$, we have a morphism

$$\pi_G: X_G\to\mathbb{P}^1_{\mathbb{Q}}=\mathbb{A}^1_{\mathbb{Q}}\cup\{\infty\}$$

of degree $[\mathrm{GL}_2(\hat{\mathbb{Z}}):G]$ from X_G to the j-line.

The key property for our applications is that for an elliptic curve $E/\mathbb{Q}$ with $j_E\notin\{0, 1728\}$, the group $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to a subgroup of G if and only if j_E is an element of $\pi_G(X_G(\mathbb{Q}))$; see Proposition 2.7. This property requires $-I\in G$, since there is always an elliptic curve E with any given rational j-invariant such that $-I\in\rho_E(\mathrm{Gal}_{\mathbb{Q}})$; it also requires $\det(G)=\hat{\mathbb{Z}}^\times$, since $\det(\rho_E(\mathrm{Gal}_{\mathbb{Q}}))=\hat{\mathbb{Z}}^\times$, and that G contain an element corresponding to complex conjugation.

We are interested in those groups G for which X_G has infinitely many rational points; equivalently, for which there are infinitely many elliptic curves $E/\mathbb{Q}$, with distinct j-invariants, such that $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G. We need only consider modular curves X_G of genus 0 or 1 since otherwise $X_G(\mathbb{Q})$ is finite by Faltings' theorem [1983].

In this article, we give an explicit description of all such subgroups $G\subseteq\mathrm{GL}_2(\hat{\mathbb{Z}})$ for which the modular curve X_G has infinitely many rational points in the special case where the level N of G is a *prime power*; we also give an explicit model for X_G and the morphism π_G. We need only describe the groups G up to conjugacy in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. For notational simplicity, we define the genus of G to be the genus of the corresponding curve X_G.

Theorem 1.1. *Up to conjugacy, there are* 248 *open subgroups G of* $\mathrm{GL}_2(\hat{\mathbb{Z}})$ *of prime power level satisfying $-I\in G$ and* $\det(G)=\hat{\mathbb{Z}}^\times$ *for which X_G has infinitely many rational points. Of these* 248 *groups, there are* 220 *of genus* 0 *and* 28 *of genus* 1.

The 220 subgroups of genus 0 in Theorem 1.1 are given in Tables 1, 2 and 3 of the online supplement. For such a group G of genus 0, we also describe the morphism π_G. More precisely, we give a rational function $J(t) \in \mathbb{Q}(t)$ such that the function field of X_G is of the form $\mathbb{Q}(t)$ and the morphism from X_G to the j-line is given by the equation $j = J(t)$. In particular, if $E/\mathbb{Q}$ is an elliptic curve with $j_E \notin \{0, 1728\}$, then $\rho_E(\mathrm{Gal}_\mathbb{Q})$ is conjugate to a subgroup of G if and only if $j_E = J(t_0)$ for some $t_0 \in \mathbb{Q} \cup \{\infty\}$.

The 28 subgroups of genus 1 in Theorem 1.1 are listed in Table 4 of the online supplement; their levels are all powers of 2 except for a group of level 11 whose image in $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ is the normalizer of a nonsplit Cartan subgroup. For such a group G of genus 1, we give a Weierstrass model for X_G and the morphism π_G to the j-line.

Example 1.2. Up to conjugacy, there is a unique subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of genus 0 and level 27 given by Theorem 1.1. It has label 27A^0-27a in our classification, and we may choose it so that the image of G in $\mathrm{GL}_2(\mathbb{Z}/27\mathbb{Z})$ is generated by the matrices $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}2&1\\9&5\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&2\\3&2\end{smallmatrix}\right)$. Using Table 1 of the online supplement, associated to G is the rational function

$$J(t) = F_3\big(F_2(F_1(t))\big) = \frac{(t^3+3)^3(t^9+9t^6+27t^3+3)^3}{t^3(t^6+9t^3+27)},$$

where $F_1(t) = t^3$, $F_2(t) = t(t^2+9t+27)$ and $F_3(t) = (t+3)^3(t+27)/t$. That $J(t)$ is the composition of three rational functions reflects the fact that the morphism π_G factors as $X_G \to X_{G'} \to X_{G''} \to \mathbb{P}^1_\mathbb{Q}$ for some groups $G \subsetneq G' \subsetneq G'' \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$. The groups G' and G'' have labels 9B^0-9a and 3B^0-3a, respectively, and can also be found in Table 1 of the online supplement.

Remark 1.3. In contrast to the case of prime power level, in general there are infinitely many open subgroups G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ satisfying $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$ for which the modular curve X_G has infinitely many rational points. Let us explicitly construct just one of several infinite families of such groups G.

Let D be the discriminant of a quadratic number field and let $\chi_D : \hat{\mathbb{Z}}^\times \to \{\pm 1\}$ be the continuous quadratic character arising from the corresponding Dirichlet character. Let $\varepsilon : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \{\pm 1\}$ be the character obtained by composing the reduction map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ with the unique nontrivial homomorphism $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to \{\pm 1\}$. Define the group

$$G_D := \big\{A \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \varepsilon(A) = \chi_D(\det(A))\big\};$$

it is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of index 2 containing $-I$ with $\det(G_D) = \hat{\mathbb{Z}}^\times$ whose level is $|D|$ or $2|D|$, depending on whether $D \equiv 0 \bmod 4$ or $D \equiv 1 \bmod 4$. For $D \neq D'$, the groups G_D and $G_{D'}$ are not conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

The modular curve X_{G_D} has genus 0 and a rational point (it has a unique, hence rational, cusp); the function field of X_{G_D} is of the form $\mathbb{Q}(t)$ with the map to the j-line given by $J(t) = Dt^2 + 1728$. Each X_{G_D} is a $\mathbb{Q}(\sqrt{D})$-twist of the modular curve

X_G corresponding to the unique index 2 subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ whose reduction has index 2 in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$; it has label 2A^0-2a in our classification and can be found in Table 3 (see the online supplement), along with its map to the j-line, which is $J(t) = t^2 + 1728$.

In general, if $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a fixed congruence subgroup of level N and index m containing $-I$, there are infinitely many nonconjugate open subgroups $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of index M containing $-I$ with $\det(G) = \hat{\mathbb{Z}}^\times$ whose reductions modulo N coincide with that of Γ upon intersection with $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The levels M of these groups G may be arbitrarily large multiples of N (and divisible by arbitrarily large primes). The corresponding modular curves $X_G/\mathbb{Q}$ are nonisomorphic, but for each X_G there is a cyclotomic field $\mathbb{Q}(\zeta_M)$ over which X_G becomes isomorphic to the modular curve $X_\Gamma/\mathbb{Q}(\zeta_N)$ (the quotient of the extended upper half plane by the action of Γ) after base change; as in our example, the X_G form an infinite family of twists.

1A. *ℓ-adic representations.* Fix a prime ℓ. Define the set

$$\mathcal{J}_\ell := \bigcup_G \big(\pi_G(X_G(\mathbb{Q})) \cap \mathbb{Q}\big)$$

of rational numbers, where G varies over the open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ whose level is a power of ℓ and satisfies $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$, and for which $X_G(\mathbb{Q})$ is finite. Note that the set $\mathcal{J}_\ell$ contains the 13 j-invariants of CM elliptic curves over $\mathbb{Q}$: for $n \geq 1$ each CM j-invariant corresponds to points on at least one of the modular curves $X_{\mathrm{s}}^+(\ell^n)$, $X_{\mathrm{ns}}^+(\ell^n)$, $X_0(\ell^n)$, and for sufficiently large n these curves have genus at least 2, hence finitely many rational points (by Faltings' theorem).

For an elliptic curve $E/\mathbb{Q}$, let

$$\rho_{E,\ell^\infty} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

be the representation describing the Galois action on the ℓ-power torsion points; it is the composition of ρ_E with the natural projection $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. After excluding a finite number of j-invariants, we will describe the possible images of the ℓ-adic representation arising from elliptic curves over $\mathbb{Q}$. Denote by $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ the group generated by $-I$ and $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$.

The following theorem describes the possibilities for $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$, up to conjugacy, when j_E is not in the (finite!) set $\mathcal{J}_\ell$.

Theorem 1.4.

(i) *The set $\mathcal{J}_\ell$ is finite.*

(ii) *If $E/\mathbb{Q}$ is an elliptic curve with $j_E \notin \mathcal{J}_\ell$, then $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to the ℓ-adic projection of a unique group G from Theorem 1.1 with ℓ-power level. Moreover, G does not have genus* 1, *level* 16, *and index* 24 *in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

(iii) *Let G be a group from Theorem 1.1 with ℓ-power level that does not have genus* 1, *level* 16, *and index* 24 *in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$. *Then there are infinitely many elliptic curves $E/\mathbb{Q}$, with distinct j-invariants, such that $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to the ℓ-adic projection of G.*

Remark 1.5. (i) Serre [1981, p. 399] has asked whether $\rho_{E,\ell}$ is surjective for all non-CM elliptic curves $E/\mathbb{Q}$ and all primes $\ell > 37$. For $\ell > 37$, this would imply that the set $\mathcal{J}_\ell$ consists of only the 13 j-invariants of CM elliptic curves over $\mathbb{Q}$.

(ii) It would be nice to explicitly know the finite sets $\mathcal{J}_\ell$; the proof that $\mathcal{J}_\ell$ is finite relies on [Zywina 2015b], which is ineffective since it applies Faltings' theorem several times.

Theorem 1.4 describes the subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, up to conjugacy, that occur as $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariants.

Theorem 1.4 also allows us to determine the subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, up to conjugacy, that occur as $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariants. They are precisely the subgroups H of the ℓ-adic projection G of a group from Theorem 1.4 with ℓ-power level such that $\pm H = G$. Indeed if $G = \pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$, then for any such H there is a quadratic twist of E such that H is conjugate to $\rho_{E',\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$, see [Zywina 2015a, §5.1; Sutherland 2016, §5.6]; when H is properly contained in G this quadratic twist is unique up to isomorphism and can be explicitly determined.

Corollary 1.6. *For* $\ell = 2, 3, 5, 7, 11, 13$ *there are respectively* $1201, 47, 23, 15, 2, 11$ *subgroups H of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ that arise as $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariants. For $\ell > 13$ the only such subgroup is* $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

A list of the groups H appearing in Corollary 1.6 can be found in electronic form at [Sutherland and Zywina 2016].

1B. *Overview.* We now give a brief overview of the contents of this paper. As already noted, the groups G from Theorem 1.1, along with the corresponding modular curves X_G and morphisms π_G, can be found in the online supplement.

In Section 2, we review the background material we need concerning the modular curves X_G. If G has level N, then we can identify the function field of X_G with a subfield of the field $\mathcal{F}_N$ of modular functions on $\Gamma(N)$ whose Fourier coefficients lie in the cyclotomic field $\mathbb{Q}(\zeta_N)$. As a working definition of X_G, we define it in terms of its function field.

In Section 3, we determine up to conjugacy the open subgroups G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with genus at most 1 that satisfy $\det(G) = \hat{\mathbb{Z}}^\times$, $-I \in G$, and contain an element that "looks like complex conjugation"; this last condition is necessary, since otherwise

$X_G(\mathbb{R})$, and therefore $X_G(\mathbb{Q})$, is empty. We are left with 220 groups of genus 0 and 250 groups of genus 1 that include all the groups that appear in Theorem 1.1. These computations make use of the tables of Cummins and Pauli [2003] of congruence subgroups of low genus.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let X_Γ be the smooth compact Riemann surface obtained by taking the quotient of the complex upper-half plane by Γ and adjoining cusps. Assume further that X_Γ has genus 0. In Section 4, we describe how to explicitly construct a *hauptmodul* for Γ; it is a meromorphic function h on X_Γ that has a unique pole at the cusp at ∞. We describe h in terms of *Siegel functions*; its Fourier coefficients are computable and lie in the field $\mathbb{Q}(\zeta_N) \subseteq \mathbb{C}$.

In Section 5, we prove the part of Theorem 1.1 concerning genus 0 groups. Let G be one of the genus 0 groups from Section 3 and let $J(t) \in \mathbb{Q}(t)$ be the corresponding rational function from the online supplement. We need to verify that the function field $\mathbb{Q}(X_G)$ of X_G is of the form $\mathbb{Q}(f)$, for some modular function f for which $J(f)$ coincides with the modular j-function. Using our work in Section 4, we can construct an explicit modular function h such that $\mathbb{Q}(\zeta_N)(X_G) = \mathbb{Q}(\zeta_N)(h)$, along with a rational function $J'(t) \in \mathbb{Q}(\zeta_N)(t)$ such that $J'(h) = j$. The function f must satisfy $f = \psi(h)$ for some $\psi(t) \in \mathbb{Q}(\zeta_N)(t)$ of degree 1, and therefore $J'(h) = j = J(f) = J(\psi(h))$; this in turn implies that $J'(t) = J(\psi(t))$. We then directly test all the modular functions $f := \psi(h)$, where $\psi(t) \in \mathbb{Q}(\zeta_N)(t)$ is one of the finitely many degree 1 rational functions that satisfy $J'(t) = J(\psi(t))$.

In Section 6, we prove the part of Theorem 1.1 concerning genus 1 groups. Let G be one of the genus 1 groups from Section 3. One can show that X_G has good reduction at all primes $p \nmid N$ and its modular interpretation gives a way to compute $\#X_G(\mathbb{F}_p)$ directly from the group G, without requiring an explicit model. By computing $\#X_G(\mathbb{F}_p)$ for enough primes $p \nmid N$, one can determine the Jacobian J_G of X_G up to isogeny. This allows us to compute the rank of $J_G(\mathbb{Q})$ which is an isogeny invariant of J_G. We need only consider groups for which $J_G(\mathbb{Q})$ has positive rank since otherwise $X_G(\mathbb{Q})$ is finite; this leaves the 28 genus 1 groups in Theorem 1.1. These 28 groups G of genus 1 and a description of their morphisms π_G already appear in the literature; our contribution lies in proving that there are no others.

In Section 7, we complete the proof of Theorem 1.4, and in Section 8 we explain how we found the rational functions $J(t) \in \mathbb{Q}(t)$ whose verification is described in Section 5.

The online supplement lists the 248 groups G that appear in Theorem 1.1, along with explicit maps from X_G to the j-line; for the 220 groups of genus 0 these are rational functions $J(t)$, and for the 28 groups of genus 1 these are morphisms $J(x, y)$ from an explicit Weierstrass model for X_G as an elliptic curve of positive rank. One can use these maps to explicitly construct infinite families of elliptic curves $E/\mathbb{Q}$ with distinct j-invariants whose ℓ-adic Galois images match the groups G listed in Theorem 1.4 and the groups H listed in Corollary 1.6 by choosing appropriate quadratic twists.

1C. ***Related results.*** Contemporaneous with our work, Rouse and Zureick-Brown [2015] independently computed explicit models for all modular curves $X_G/\mathbb{Q}$ of 2-power level that have a noncuspidal rational point, including all those for which $X_G(\mathbb{Q})$ is infinite. The X_G of 2-power level in our list agree with theirs, although we generally obtain different (but isomorphic) models (note our groups are transposed relative to theirs; in our choice of the isomorphism $\mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we view matrices in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as acting on the left, rather than the right).

Notation and terminology. For each integer $n \geq 1$, we denote by ζ_n the n-th root of unity $e^{2\pi i/n}$ in $\mathbb{C}$, and let $K_n := \mathbb{Q}(\zeta_n)$ denote the corresponding cyclotomic field. For any nonconstant function $f \in K(t)$, where K is a field, the *degree* of f is its degree as a morphism $\mathbb{P}^1_K \to \mathbb{P}^1_K$.

For any ring R, we denote by $\mathrm{M}_2(R)$ the ring of 2×2 matrices with coefficients in R. We denote by $\hat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$, and view the profinite group

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \varprojlim_N \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$$

as a topological group in the profinite topology. If G is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, we define its *level* to be the least positive integer N for which G is the inverse image of a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ under the natural projection $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If G is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, its level is defined to be the level of its inverse image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, which is necessarily a divisor of N. For convenience we may identify the level N subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with their inverse images in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, and conversely. By the *genus* of an open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ satisfying $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$, we mean the genus of the modular curve X_G defined in Section 2.

For sets S and T we use $S - T$ to denote the set of elements that lie in S but not T.

2. Modular functions and modular curves

In this section, we summarize the background we need concerning modular curves.

2A. ***Congruence subgroups.*** Fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, i.e., a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing

$$\Gamma(N) := \{A \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv I \pmod{N}\}$$

for some integer $N \geq 1$. The smallest such N is the *level* of Γ.

The group Γ acts on the complex upper half plane $\mathbb{H}$ by linear fractional transformations, and the quotient $Y_\Gamma = \Gamma\backslash\mathbb{H}$ is a smooth Riemann surface. By adding *cusps*, we can extend Y_Γ to a smooth compact Riemann surface X_Γ. We denote by $X(N)$ the Riemann surface $X_{\Gamma(N)}$. The *genus* of Γ is the genus of the Riemann surface X_Γ.

2B. ***Cusps.*** Define the extended upper half plane by $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. The action of Γ extends to $\mathbb{H}^*$ and we can identify the quotient $\Gamma\backslash\mathbb{H}^*$ with X_Γ. In particular, the cusps correspond to the Γ-orbits of $\mathbb{Q} \cup \{\infty\}$.

Lemma 2.1. *Let a/b and α/β be elements of $\mathbb{Q} \cup \{\infty\}$ satisfying* $\gcd(a, b) = 1$ *and* $\gcd(\alpha, \beta) = 1$ (*where we take $\infty = \pm 1/0$*). *Then $\Gamma \cdot a/b = \Gamma \cdot \alpha/\beta$ if and only if $\gamma\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \equiv \pm\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right) \pmod N$ for some $\gamma \in \Gamma$.*

Proof. For the case $\Gamma = \Gamma(N)$, see [Shimura 1971, Lemma 1.42]. The general case follows easily. □

Let $\pm\Gamma$ be the congruence subgroup generated by $-I$ and Γ. From Lemma 2.1, we find that the cusps of X_Γ correspond with the orbits of $\pm\Gamma$ on the set of $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N. Using this, it is straightforward to find representatives of the cusps of X_Γ.

2C. ***Modular functions.*** A *modular function* for Γ is a meromorphic function of X_Γ; they correspond to meromorphic functions f of $\mathbb{H}$ that satisfy $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma$ and are meromorphic at the cusps. The function field $\mathbb{C}(X_\Gamma)$ of X_Γ consists of the meromorphic functions of X_Γ.

Let τ be a variable of the upper half plane. Let w be the width of the cusp at ∞, i.e., the smallest positive integer for which $\left(\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right)$ is an element of Γ; it is a divisor of N. For any rational number m, define $q^m := e^{2\pi i m\tau}$. Then any modular function f for Γ has a unique q-expansion

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n q^{n/w},$$

where the c_n are complex numbers that are 0 for all but finitely many $n < 0$. We will often refer to the c_n as the *coefficients* of f.

2D. ***Field of modular functions.*** Fix a positive integer N. Denote by $\mathcal{F}_N$ the field of meromorphic functions of the Riemann surface $X(N)$ whose q-expansions have coefficients in $K_N := \mathbb{Q}(\zeta_N)$. For example, $\mathcal{F}_1 = \mathbb{Q}(j)$, where j is the modular j-invariant.

For $f \in \mathcal{F}_N$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, let $f|_\gamma \in \mathcal{F}_N$ denote the modular function satisfying $f|_\gamma(\tau) = f(\gamma\tau)$.

For each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, let σ_d be the automorphism of K_N satisfying $\sigma_d(\zeta_N) = \zeta_N^d$. We extend σ_d to an automorphism of the field $\mathcal{F}_N$ by defining

$$\sigma_d(f) := \sum_n \sigma_d(c_n) q^{n/N},$$

where f has expansion $\sum_n c_n q^{n/N}$. We now recall some facts about the extension $\mathcal{F}_N$ of $\mathcal{F}_1 = \mathbb{Q}(j)$.

Proposition 2.2. *The extension $\mathcal{F}_N$ of $\mathbb{Q}(j)$ is Galois. There is a unique isomorphism*

$$\theta_N : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$$

such that the following hold for all $f \in \mathcal{F}_N$:

(a) *For $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $\theta_N(g) f = f|_{\gamma^t}$, where γ is any matrix in $\mathrm{SL}_2(\mathbb{Z})$ that is congruent to g modulo N and γ^t is the transpose of γ.*

(b) *For $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $\theta_N(g) f = \sigma_d(f)$.*

Moreover, the algebraic closure of $\mathbb{Q}$ in $\mathcal{F}_N$ is $\mathbb{Q}(\zeta_N)$; it corresponds to the subgroup $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

Proof. This is well known; see [Kubert and Lang 1981, Chapter 2, §2] for a summary (where the action given is a right action obtained as above but without the transpose in (a)). □

Throughout the rest of the paper, we let $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ act on $\mathcal{F}_N$ via the homomorphism θ_N of Proposition 2.2. We set $g_*(f) := \theta_N(g)(f)$ for $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $f \in \mathcal{F}_N$.

Remark 2.3. There are other natural actions of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$; for example, one could replace γ^t in condition (a) by γ^{-1} or just act on the right. Our choice is motivated by Proposition 2.6 below.

2E. *Modular curves.* Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Let $\mathcal{F}_N^G$ be the subfield of $\mathcal{F}_N$ fixed by the action of G from Proposition 2.2. Proposition 2.2 and the assumption $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ imply that $\mathbb{Q}$ is algebraically closed in $\mathcal{F}_N^G$.

The *modular curve* X_G associated with G is the smooth projective curve with function field $\mathcal{F}_N^G$. The curve X_G is defined over $\mathbb{Q}$ and is geometrically irreducible. The inclusion of fields $\mathcal{F}_N^G \supseteq \mathcal{F}_1 = \mathbb{Q}(j)$ gives rise to a nonconstant morphism

$$\pi_G : X_G \to \mathrm{Spec}\, \mathbb{Q}[j] \cup \{\infty\} = \mathbb{P}^1_{\mathbb{Q}}$$

of degree $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$. Moreover, given another group $G \subseteq G' \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the inclusion $\mathcal{F}_N^{G'} \subseteq \mathcal{F}_N^G$ induces a nonconstant morphism $X_G \to X_{G'}$ of degree $[G' : G]$. Composing $X_G \to X_{G'}$ with $\pi_{G'}$ gives the morphism π_G.

Let Γ be the congruence subgroup consisting of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ for which γ^t modulo N lies in $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The level of Γ divides, but need not equal, N.

Lemma 2.4. (i) *The field $K_N(X_G)$, i.e., the function field of the base extension of X_G to K_N, is the field consisting of $f \in \mathcal{F}_N$ satisfying $f|_\gamma = f$ for all $\gamma \in \Gamma$.*

(ii) *The genus of the modular curve X_G is equal to the genus of Γ.*

Proof. Proposition 2.2 implies that K_N is algebraically closed in $\mathcal{F}_N$ and that we have an isomorphism $\mathrm{Gal}(\mathcal{F}_N/K_N(j)) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. Thus $K_N(X_G)$ is the subfield of $\mathcal{F}_N$ fixed by $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Part (i) is now clear.

Since K_N is algebraically closed in $\mathcal{F}_N$ and $\mathbb{Q}$ is algebraically closed in $\mathbb{Q}(X_G)$, we have

$$[\mathbb{C}\cdot K_N(X_G):\mathbb{C}(j)] = [K_N(X_G):K_N(j)] = [\mathbb{Q}(X_G):\mathbb{Q}(j)] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}):G].$$

Since $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, we deduce that $[\mathbb{C}\cdot K_N(X_G):\mathbb{C}(j)] = [\mathrm{SL}_2(\mathbb{Z}):\Gamma]$.

Clearly each $f \in K_N(X_G)$ is a modular function for Γ, thus $\mathbb{C}\cdot K_N(X_G) \subseteq \mathbb{C}(X_\Gamma)$. We in fact have $\mathbb{C}\cdot K_N(X_G) = \mathbb{C}(X_\Gamma)$, since $[\mathbb{C}\cdot K_N(X_G):\mathbb{C}(j)] = [\mathrm{SL}_2(\mathbb{Z}):\Gamma] = [\mathbb{C}(X_\Gamma):\mathbb{C}(j)]$. The curve X_G has the same genus as the Riemann surface X_Γ because $\mathbb{C}(X_G) = \mathbb{C}(X_\Gamma)$. □

Remark 2.5. Another natural congruence subgroup to study is the congruence subgroup Γ' consisting of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that γ modulo N lies in $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, which we use later in the paper. Observe that the congruence subgroups Γ and Γ' are conjugate in $\mathrm{SL}_2(\mathbb{Z})$; indeed, we have $B^{-1}\gamma B = (\gamma^t)^{-1}$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, where $B := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Thus Γ and Γ' have the same genus.

The following proposition is crucial to our application.

Proposition 2.6. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$. Then $\rho_{E,N}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G if and only if j_E belongs to $\pi_G(X_G(\mathbb{Q}))$.*

Proof. See [Zywina 2015a, §3] for a proof. □

2F. ***Modular curves and open subgroups.*** Fix an open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that satisfies $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$. Let $N \geq 1$ be an integer that is divisible by the level of G. Define the modular curve

$$X_G := X_{\bar{G}},$$

where $\bar{G} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the image of G modulo N. Observe that the modular curve X_G and its function field do not depend on the initial choice of N.

Every (open) subgroup G' of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that contains G satisfies $-I \in G'$ and $\det(G') = \hat{\mathbb{Z}}^\times$, and we have a morphism $X_G \to X_{G'}$. With $G' = \mathrm{GL}_2(\hat{\mathbb{Z}})$, we obtain a morphism $\pi_G : X_G \to X_{G'} = \mathbb{P}^1_\mathbb{Q}$ to the j-line that agrees with $\pi_{\bar{G}}$. The following is equivalent to Proposition 2.6.

Proposition 2.7. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$. Then $\rho_E(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to a subgroup of G if and only if j_E belongs to $\pi_G(X_G(\mathbb{Q}))$.* □

2G. *Complex conjugation.* Fix a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. For our curve X_G to have rational points, we need G to contain an element that "looks like" complex conjugation.

Lemma 2.8. *For any elliptic curve $E/\mathbb{Q}$ and integer $N > 1$, the group $\rho_{E,N}(\mathrm{Gal}_\mathbb{Q})$ contains an element that is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$.*

Proof. This follows from of [Zywina 2015b, Proposition 3.5] (and its proof for the cases $j_E \in \{0, 1728\}$). □

Note that $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$ are conjugate to each other in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ if N is odd. If G does not contain an element that is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$, then $X_G(\mathbb{Q})$ must be empty since $X_G(\mathbb{R})$ is finite (by [Zywina 2015b, Proposition 3.5]), hence empty, since X_G is nonsingular.

3. Group theoretic computations

We define an *admissible group* to be an open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ for which the following conditions hold:

- G has prime power level.
- $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$.
- G contains an element that is conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$.

The condition $\det(G) = \hat{\mathbb{Z}}^\times$ is needed for Proposition 2.7 since $\det(\rho_E(\mathrm{Gal}_\mathbb{Q})) = \hat{\mathbb{Z}}^\times$. If we were interested in elliptic curves defined over other number fields, then we could loosen this restriction which could increase the base field of the modular curve X_G.

The condition $-I \in G$ is also needed in Proposition 2.7. For an elliptic curve $E/\mathbb{Q}$, there is a quadratic twist $E'/\mathbb{Q}$, which automatically has the same j-invariant as E, such that $-I \in \rho_E(\mathrm{Gal}_\mathbb{Q})$.

The last condition on G is necessary in order for $X_G(\mathbb{Q})$ to be nonempty, as explained in Section 2G.

Proposition 3.1. *Let G be an admissible group of genus 0. The set $X_G(\mathbb{Q})$ is infinite.*

Proof. We have $X_G(\mathbb{R}) \neq \varnothing$ by [Zywina 2015b, Proposition 3.5]. For primes p not dividing its prime power level the modular curve X_G has good reduction at p and $X_G(\mathbb{Q}_p) \neq \varnothing$, since the reduction of X_G to $\mathbb{F}_p$ necessarily has rational points that can be lifted to $\mathbb{Q}_p$ via Hensel's lemma. Thus X_G has rational points locally at all but at most one place of $\mathbb{Q}$. The product formula for Hilbert symbols and the Hasse–Minkowksi theorem then imply that X_G has a rational point and is thus isomorphic to $\mathbb{P}^1$ and has infinitely many rational points. $\square$

Remark 3.2. As shown by Proposition 3.1, our three criteria for admissibility rule out genus 0 curves with no rational points. There are ten groups G of 2-power level that satisfy our first two criteria but not the third; these give rise to the ten pointless conics X_G found in [Rouse and Zureick-Brown 2015]. There are three such groups of 3-power level, three of 5-power level, and none of higher prime-power level.

Fix an integer $g \geq 0$. In this section, we explain how to enumerate all admissible subgroups G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, up to conjugacy, that have genus at most g. We shall apply these methods with $g = 1$ to verify Theorem 3.3 below, and to find explicit representatives of these conjugacy classes of groups; Magma [Bosma et al. 1997] scripts that perform this enumeration can be found in [Sutherland and Zywina 2016].

Theorem 3.3.

(i) *Up to conjugacy in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$, *there are* 220 *admissible subgroups of genus* 0.

(ii) *Up to conjugacy in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$, *there are* 250 *admissible subgroups of genus* 1.

Remark 3.4. The 220 admissible subgroups G of genus 0, up to conjugacy, are precisely those given in Tables 1–3 of the online supplement. More precisely, for each entry of the table, we have an integer N and a set of generators that generates the image in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of an admissible group of level N and genus 0.

Remark 3.5. The 28 admissible subgroups G of genus 1 that have infinitely many rational points, up to conjugacy, are precisely those given in Table 4 of the online supplement, of which 27 have level 16 and 1 has level 11. The levels arising among the remaining 222 are 7, 8, 9, 11, 16, 17, 19, 27, 32, and 49.

For a fixed admissible group G of level N, let Γ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices whose image modulo N lies in the image of G mod N; the level of Γ necessarily divides N, and Γ contains $-I$. By Lemma 2.4(ii) and Remark 2.5, the modular curve X_G has the same genus as Γ.

The basic idea of our computation is to reverse the process above; we start with a congruence subgroup Γ of genus at most g and prime power level, and then enumerate the possible groups G that could produce Γ.

Let S_g be the set of congruences subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of prime power level that contain $-I$ and have genus at most g. We know that the set S_g is finite from a theorem of Dennin [1974]. When $g \leq 24$, and in particular, for $g = 1$, we can explicitly determine the elements of S_g from the tables of Cummins and Pauli [2003] (their methods can also be extended to larger g).

Let L_g be the set of primes that divide the level of some congruence subgroup

$\Gamma \in S_g$. The set L_g is finite, since S_g is finite, and we have $L_1 = \{2, 3, 5, 7, 11, 13, 17, 19\}$. If G is an admissible group of genus at most g, then its level must be a power of a prime $\ell \in L_g$. For the rest of the section, we fix a prime $\ell \in L_g$. Since L_g is finite, it suffices to explain how to compute the admissible groups G with genus at most g whose level is a power of ℓ, and we need only consider levels strictly greater than 1 since $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is the only admissible group of level 1.

Fix a prime power $N := \ell^n > 1$, and consider any congruence subgroup $\Gamma \in S_g$ whose level divides N. By enumerating subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ one can explicitly determine those subgroups G_N that satisfy the following conditions:

(1) G_N has level N,

(2) $G_N \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is equal to the image of Γ modulo N,

(3) $\det(G_N) = (\mathbb{Z}/N\mathbb{Z})^\times$,

(4) G_N contains an element that is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$.

Let H be the image of Γ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The group $H = G_N \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is normal in G_N and hence G_N is a subgroup of the normalizer K of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. So rather than searching for G_N in K, we can work in the quotient K/H where the image of G_N is an abelian group isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$. Using Magma, we can efficiently enumerate all abelian subgroups A of K/H of order $\#(\mathbb{Z}/N\mathbb{Z})^\times$. For each such subgroup A we then test whether its inverse image G_N in K satisfies conditions (1)–(4) above.

Let G be the subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ consisting of those matrices whose image modulo N lies in a fixed group G_N satisfying the conditions (1)–(4). The group G is admissible of level N and has genus at most g. Moreover, it is clear that every admissible group of level N and genus at most g arises in this manner.

Fix an integer $e \geq 1$. By applying the above method with $1 \leq n \leq e$, we obtain all admissible groups G of genus at most g and level dividing ℓ^e. Our algorithm proceeds by applying this procedure to increasing values of e. In order for it to terminate we need to know that there are only finitely many admissible groups G of ℓ-power level and genus at most g, and we need an explicit way to determine when we have reached an e that is large enough to guarantee that we have found them all. Proposition 3.6 below addresses both issues.

Proposition 3.6.

(i) *There are only finitely many admissible groups G with genus at most g whose level is a power of ℓ.*

(ii) *Take any integer $n \geq 2$ with $n \neq 2$ if $\ell = 2$. Define $N := \ell^n$. Suppose that there is no subgroup G_N of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies conditions (1)–(4) for some $\Gamma \in S_g$ with level dividing N. Then any admissible group G of genus at most g with level a power of ℓ has level at most N.*

The remainder of this section is devoted to proving Proposition 3.6. We will need the following basic lemma.

Lemma 3.7. *Let ℓ be a prime and let G be an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. For each integer $m \geq 1$, let i_m be the index of the image of G in $\mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$. If $i_{n+1} = i_n$ for an integer $n \geq 1$, with $n \neq 1$ if $\ell = 2$, then $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G] = i_n$.*

Proof. Since G is an open subgroup, it suffices to prove $i_{m+1} = i_m$ for all $m \geq n$; we proceed by induction on m. The base case is given, so we assume $i_{m+1} = i_m$ for some $m \geq n$; we need to show that $i_{m+2} = i_{m+1}$. Let G_m denote the image of G in $\mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$. Reduction modulo ℓ^m gives exact sequences related by inclusions

$$\begin{tikzcd}
1 \arrow[r] & K_{m+1} \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/\ell^{m+1}\mathbb{Z}) \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z}) \arrow[r] & 1 \\
1 \arrow[r] & H_{m+1} \arrow[r] \arrow[u, hook] & G_{m+1} \arrow[r] \arrow[u, hook] & G_m \arrow[r] \arrow[u, hook] & 1.
\end{tikzcd}$$

The inductive hypothesis $i_{m+1} = i_m$ implies that the kernels H_{m+1} and K_{m+1} coincide; in particular, H_{m+1} is as large as possible (i.e., it has order ℓ^4). It thus suffices to show that the kernel H_{m+2} of the reduction map from G_{m+2} to G_{m+1} also has order ℓ^4. We have $|H_{m+2}| \leq \ell^4$, so it suffices to give an injective map $H_{m+1} \to H_{m+2}$.

Let M be an element of G whose image in G_{m+1} lies in H_{m+1}; then $M = I + \ell^m A$ for some $A \in \mathrm{M}_2(\mathbb{Z}_\ell)$. Since $m \geq 1$, with $m \geq 2$ if $\ell = 2$, we have

$$(1 + \ell^m A)^\ell = 1 + \binom{\ell}{1}\ell^m A + \binom{\ell}{2}\ell^{2m} A^2 + \cdots \equiv 1 + \ell^{m+1} A \pmod{\ell^{m+2}}.$$

The ℓ-power map thus induces an injection $H_{m+1} \to H_{m+2}$. □

Remark 3.8. Lemma 3.7 holds more generally. One can replace $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with the unit group of any (unital associative) $\mathbb{Z}_\ell$-algebra $\mathcal{A}$ that is torsion-free and finitely generated as a $\mathbb{Z}_\ell$-module (in the lemma, $\mathcal{A} = \mathrm{M}_2(\mathbb{Z}_\ell)$); the proof is exactly the same.

Proof of Proposition 3.6(i). Let $\mathcal{G}$ be the set of admissible groups of genus at most g whose level is a power of ℓ. Note that if G' is a subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ containing some $G \in \mathcal{G}$, then $G' \in \mathcal{G}$. We wish to show that $\mathcal{G}$ is finite.

We claim that any admissible group G has only finitely many maximal subgroups that are also admissible and whose level is a power of ℓ. It suffices to show that an open subgroup H of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ has only finitely many open maximal subgroups. Let $\Phi(H)$ be the Frattini subgroup of H; it is the intersection of the maximal closed proper subgroups of H. By the proposition in [Serre 1997, §10.5], $\Phi(H)$ is an open subgroup of H. This proves the claim.

Now suppose that $\mathcal{G}$ is infinite. The claim implies that $\mathcal{G}$ contains an infinite descending chain $G_1 \supsetneq G_2 \supsetneq G_3 \supsetneq \cdots$ (let $G_1 = \mathrm{GL}_2(\hat{\mathbb{Z}}) \in \mathcal{G}$, let $G_2 \in \mathcal{G}$ be one of the finitely many maximal subgroups of G_1 in $\mathcal{G}$ that has infinitely many subgroups in $\mathcal{G}$, and continue in this fashion). For each $i \geq 1$, let Γ_i be the congruence subgroup associated to G_i (i.e., Γ_i consists of the matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N lies in the image modulo N of G_i, where N is the level of G_i); then $\Gamma_i \in S_g$. Since $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : G_i] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_i]$, we have inclusions $\Gamma_1 \supsetneq \Gamma_2 \supsetneq \Gamma_3 \supsetneq \cdots$. This contradicts the finiteness of S_g and the proposition follows. □

Proof of Proposition 3.6(ii). Fix an integer $n \geq 1$ as in the statement of part (ii). Suppose there is an integer $m > n$ such that there is an admissible group G of level ℓ^m and genus at most g.

With $N := \ell^n$, let G_N be the image of G in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The curve X_{G_N} has genus at most g since it is dominated by X_G. Therefore, conditions (2), (3), and (4) hold for some $\Gamma \in S_g$ with level dividing N. Our assumption on n implies that the level of G_N is a proper divisor of N. This implies that the index $i_n := [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G_N]$ agrees with $i_{n-1} := [\mathrm{GL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) : G_{\ell^{n-1}}]$, where $G_{\ell^{n-1}}$ is the image of G in $\mathrm{GL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})$. Since $i_n = i_{n-1}$, Lemma 3.7 implies that $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G] = i_{n-1}$. However, this means that G has level dividing ℓ^{n-1} which is impossible since, by assumption, G has level $\ell^m > \ell^{n-1}$. Therefore, no such admissible group G exists. □

4. Construction of hauptmoduls

Fix a congruence subgroup Γ of genus 0 and level N. The function field of X_Γ is then of the form $\mathbb{C}(h)$, where the function $h : X_\Gamma \to \mathbb{C} \cup \{\infty\}$ gives an isomorphism between X_Γ and the Riemann sphere; in particular, h has a unique (simple) pole.

We may choose h so that its unique pole is at the cusp ∞; we will call such an h a *hauptmodul* of Γ. Every hauptmodul of Γ is then of the form $ah + b$ for some complex numbers $a \neq 0$ and b. For example, the familiar modular j-invariant

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

is a hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$. If h is a hauptmodul for Γ, then we have an inclusion of function fields $\mathbb{C}(j) \subseteq \mathbb{C}(h)$ and hence $J(h) = j$ for a unique rational function $J(h) \in \mathbb{C}(t)$.

The main task of Section 4 is to describe how to find an *explicit* hauptmodul h of Γ in terms of Siegel functions when N is a prime power. Our h will have coefficients in K_N. In Section 4D, we explain how to compute the rational function $J(t)$ corresponding to h.

4A. ***Siegel functions.*** Take any pair $a = (a_1, a_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$. We define the *Siegel function* $g_a(\tau)$ to be the holomorphic function $\mathbb{H} \to \mathbb{C}^\times$ defined by the series

$$-q^{1/2B_2(a_1)} \cdot e(a_2(a_1-1)/2) \cdot (1-e(a_2)q^{a_1}) \prod_{n=1}^{\infty} (1-e(a_2)q^{n+a_1})(1-e(-a_2)q^{n-a_1}),$$

where $e(z) = e^{2\pi i z}$ and $B_2(x) = x^2 - x + \frac{1}{6}$.

Recall that the *Dedekind eta function* is the holomorphic function on $\mathbb{H}$ given by

$$\eta(\tau) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

For each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, there is a unique 12-th root of unity $\varepsilon(\gamma) \in \mathbb{C}^\times$ such that

$$\eta(\gamma\tau)^2 = \varepsilon(\gamma)(c\tau + d)\eta(\tau)^2. \tag{4-1}$$

We can characterize the map $\varepsilon : \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}^\times$ by the property that it is a homomorphism satisfying $\varepsilon\big(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\big) = \zeta_{12}$ and $\varepsilon\big(\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\big) = \zeta_4$; see [Kubert and Lang 1981, Chapter 3, §5]. Moreover, the kernel of ε is a congruence subgroup of level 12 and agrees with the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

The following lemma gives several key properties of Siegel functions.

Lemma 4.1. *For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $a \in \mathbb{Q}^2 - \mathbb{Z}^2$, and $b \in \mathbb{Z}^2$, the following hold*:

(i) $g_{-a} = -g_a$,

(ii) $g_{a+b} = (-1)^{b_1+b_2+b_1b_2} \cdot e((b_2a_1 - b_1a_2)/2) \cdot g_a$,

(iii) $g_a|_\gamma = \varepsilon(\gamma) \cdot g_{a\gamma}$, *where we view a as a row vector.*

Proof. In [Kubert and Lang 1981, Chapter 2, §1], we see that $g_a(\tau) = \mathfrak{k}_a(\tau)\eta(\tau)^2$, where $\mathfrak{k}_a(\tau)$ is a Klein form (with $W = W_\tau$ in the notation the previous work). Part (ii) follows directly from property K2 in [loc. cit.].

Take any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and let (c, d) be the last row of γ. From properties K0 and K1 of the above reference, we find that

$$\mathfrak{k}_a(\gamma\tau) = (c\tau + d)^{-1}\mathfrak{k}_{a\gamma}(\tau). \tag{4-2}$$

From (4-1) and (4-2), we deduce that $g_a(\gamma\tau) = \varepsilon(\gamma) \cdot g_{a\gamma}(\tau)$, which proves part (iii). Finally, part (i) follows from part (iii) with $\gamma = -I$, since $\varepsilon(-I) = -1$. $\square$

For an integer $N > 1$, let $\mathcal{A}_N$ be the set of pairs $(a_1, a_2) \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$ that satisfy one of the following conditions:

- $0 < a_1 < \frac{1}{2}$ and $0 \le a_2 < 1$,
- $a_1 = 0$ and $0 < a_2 \le \frac{1}{2}$,
- $a_1 = \frac{1}{2}$ and $0 \le a_2 \le \frac{1}{2}$.

The set $\mathcal{A}_N$ is chosen so that every nonzero coset of $(N^{-1}\mathbb{Z}^2)/\mathbb{Z}^2$ is represented by an element of the form a or $-a$ for a unique $a \in \mathcal{A}_N$. So for any $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$, we can use parts (i) and (ii) of Lemma 4.1 to show that

$$g_a = \epsilon \cdot \zeta \cdot g_{a'}$$

for an explicit sign $\epsilon \in \{\pm 1\}$, N-th root of unity ζ, and pair $a' \in \mathcal{A}_N$.

4B. ***Siegel orbits.*** Now fix a congruence subgroup Γ of level $N > 1$. For each $a \in \mathcal{A}_N$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, let $a * \gamma$ be the unique element of $\mathcal{A}_N$ such that $a * \gamma$ or $-a * \gamma$ lies in the coset $a\gamma + \mathbb{Z}^2$. The map

$$\mathcal{A}_N \times \mathrm{SL}_2(\mathbb{Z}) \to \mathcal{A}_N, \quad (a, \gamma) \mapsto a * \gamma$$

then gives a right action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{A}_N$. In particular, this gives a right action of Γ on $\mathcal{A}_N$.

Fix a Γ-orbit $\mathcal{O}$ of $\mathcal{A}_N$ and define

$$g_{\mathcal{O}} := \prod\nolimits_{a \in \mathcal{O}} g_a;$$

it is a holomorphic function $\mathbb{H} \to \mathbb{C}^\times$.

Lemma 4.2. *The function $g_{\mathcal{O}}^{12N}$ is a modular function for Γ. Every pole and zero of $g_{\mathcal{O}}^{12N}$ on X_Γ is a cusp.*

Proof. Take any $\gamma \in \Gamma$ and $a \in \mathcal{A}_N$. By Lemma 4.1(iii), we have $g_a^{12N}|_\gamma = g_{a\gamma}^{12N}$. We have $a\gamma = \epsilon \cdot (a * \gamma + b)$ for some $\epsilon \in \{\pm 1\}$ and $b \in \mathbb{Z}^2$. By parts (i) and (ii) of Lemma 4.1, we find that $g_a^{12N}|_\gamma = g_{a\gamma}^{12N}$ is equal to $g_{a*\gamma}^{12N}$. Therefore,

$$g_{\mathcal{O}}^{12N}|_\gamma = \prod_{a \in \mathcal{O}} g_a^{12N}|_\gamma = \prod_{a \in \mathcal{O}} g_{a*\gamma}^{12N} = g_{\mathcal{O}}^{12N},$$

where the last equality uses the fact that the map $\mathcal{O} \to \mathcal{O}$, $a \mapsto a * \gamma$ is a bijection (since $\mathcal{O}$ is a Γ-orbit). The remaining statement about the poles and zeros of $g_{\mathcal{O}}^{12N}$ follows immediately since each g_a is holomorphic and nonzero on $\mathbb{H}$. $\square$

Let $P_1, \ldots, P_r$ be the cusps of X_Γ. Choose a representative $s_j \in \mathbb{Q} \cup \{\infty\}$ of each cusp P_j and a matrix $A_j \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $A_j \cdot \infty = s_j$. Let w_j be the *width* of the cusp P_j; it is the smallest positive integer b such that $A_j \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) A_j^{-1}$ is an element of Γ.

For a nonzero meromorphic function f of $\mathbb{H}$ given by a q-expansion, we define $\mathrm{ord}_q(f)$ to be the smallest rational number m such that there is a nonzero term of the form q^m in the expansion of f. For each cusp P_j, define the map

$$v_{P_j} : \mathbb{C}(X_\Gamma)^\times \to \mathbb{Z}, \quad f \mapsto w_j \cdot \mathrm{ord}_q(f|_{A_j});$$

it is a surjective homomorphism and agrees with the valuation giving the order of vanishing of a function at P_j. We extend ord_q and v_{P_j} by setting $\mathrm{ord}_q(0) = +\infty$ and $v_{P_j}(0) = +\infty$.

We now give a computable expression for the divisor of $g_{\mathcal{O}}^{12N}$ on X_Γ.

Lemma 4.3. *With notation as above, we have*

$$\mathrm{div}(g_{\mathcal{O}}^{12N}) = \sum_{j=1}^{r} \Bigl(6N w_j \sum_{a \in \mathcal{O}} B_2\bigl(\langle (aA_j)_1 \rangle\bigr) \Bigr) \cdot P_j,$$

where $B_2(x) = x^2 - x + \frac{1}{6}$, $(aA_j)_1$ *is the first coordinate of the row vector* aA_j, *and* $\langle x \rangle$ *denotes the positive fractional part of the real number* x, *chosen so* $0 \le \langle x \rangle < 1$ *and* $x - \langle x \rangle \in \mathbb{Z}$.

Proof. For any $a \in (N^{-1}\mathbb{Z}^2) - \mathbb{Z}^2$, we have $\mathrm{ord}_q(g_a) = \frac{1}{2} \cdot B_2(\langle a_1 \rangle)$; see [Kubert and Lang 1981, p. 31]. We have

$$v_{P_j}(g_{\mathcal{O}}^{12N}) = \sum_{a \in \mathcal{O}} v_{P_j}(g_a^{12N}) = \sum_{a \in \mathcal{O}} w_j \, \mathrm{ord}_q(g_a^{12N}|_{A_j}) = \sum_{a \in \mathcal{O}} w_j \, \mathrm{ord}_q(g_{aA_j}^{12N}),$$

where the last equality uses Lemma 4.1(iii). Therefore,

$$v_{P_j}(g_{\mathcal{O}}^{12N}) = \sum_{a \in \mathcal{O}} 12N w_j \, \mathrm{ord}_q(g_{aA_j}) = 6N w_j \sum_{a \in \mathcal{O}} B_2\bigl(\langle (aA_j)_1 \rangle\bigr).$$

Since all poles and zeros of $g_{\mathcal{O}}^{12N}$ are cusps, we have $\mathrm{div}(g_{\mathcal{O}}^{12N}) = \sum_{i=1}^{r} v_{P_j}(g_{\mathcal{O}}^{12N}) \cdot P_j$, and the lemma follows immediately. $\square$

4C. *Constructing hauptmoduls of prime power level.* Fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ of *prime power* level $N > 1$ that has genus 0. Let $P_1, \dots, P_r$ be the cusps of Γ; we choose our cusps so that P_1 is the cusp at ∞.

In this section, we explain how to construct an explicit hauptmodul of Γ whose q-expansion has coefficients in K_N. Moreover, our hauptmodul will be of the form

$$\sum_{i=1}^{M} \zeta_{2N^2}^{e_i} \prod_{a \in \mathcal{A}_N} g_a^{m_{a,i}} \tag{4-3}$$

with integers $m_{a,i}$ and e_i.

Case 1: multiple cusps. First assume that Γ has at least two cusps. We will use the following lemma to construct a hauptmodul for certain genus 0 congruence subgroups.

Let $\mathcal{O}_1, \dots, \mathcal{O}_n$ be the distinct Γ-orbits of $\mathcal{A}_N$. For each $\mathcal{O}_i$, define the divisor $D_i := \mathrm{div}(g_{\mathcal{O}_i}^{12N})$ on X_Γ. By Lemma 4.3, the divisors $D_1, \dots, D_n$ are supported on $\{P_1, \dots, P_r\}$ and are straightforward to compute.

Lemma 4.4. *Suppose there is an* n*-tuple* $m \in \mathbb{Z}^n$ *such that*

$$\sum_{i=1}^{n} m_i D_i = -12N \cdot P_1 + 12N \cdot P_2.$$

Let $0 \le e < 2N^2$ *be the integer satisfying* $e \equiv \sum_{i=1}^n m_i \sum_{a\in\mathcal{O}_i} Na_2(N - Na_1) \pmod{2N^2}$. *Then*

$$h := \zeta_{2N^2}^{e} \prod_{i=1}^{n} g_{\mathcal{O}_i}^{m_i}$$

is a hauptmodul for Γ *whose* q*-expansion has coefficients in* K_N. *On* X_Γ, *we have* $\operatorname{div}(h) = -P_1 + P_2$.

Proof. Since X_Γ has genus 0, there is a meromorphic function f on X_Γ with $\operatorname{div}(f) = -P_1 + P_2$. Lemma 4.2 implies that f^{12N}/h^{12N} defines a function on X_Γ; it has divisor

$$12N \operatorname{div}(f) - \sum_{i=1}^{n} m_i \operatorname{div}(g_{\mathcal{O}_i}^{12N}) = 12N(-P_1 + P_2) - \sum_{i=1}^{n} m_i D_i = 0,$$

where the last equality uses our assumption on m. Therefore, f^{12N}/h^{12N} is constant. Since f and h are meromorphic functions on the upper half-plane, we deduce that f/h is a (nonzero) constant. In particular, h is modular for Γ and $\operatorname{div}(h) = -P_1 + P_2$. The function h on X_Γ is a hauptmodul for Γ since its only pole is the simple pole at P_1, i.e., the cusp at ∞.

It remains to show that the coefficients of h lie in K_N. Take any $a \in \mathcal{A}_N$. From the series defining g_a, we find that a equals the root of unity $e\big(\tfrac{1}{2}a_2(a_1 - 1)\big) = \zeta_{2N^2}^{Na_2(Na_1-N)}$ times a Laurent series in $q^{1/(6N^2)}$ with coefficients in K_N. Set

$$e' := \sum_{i=1}^{n} m_i \sum_{a\in\mathcal{O}_i} Na_2(Na_1 - N).$$

The coefficients of $\zeta_{2N^2}^{-e'} \prod_{i=1}^n g_{\mathcal{O}_i}^{m_i}$ thus all lie in K_N. The lemma follows since $e \equiv -e' \pmod{2N^2}$. □

Using the Cummins–Pauli classification of genus 0 congruence subgroups [Cummins and Pauli 2003], we have explicitly verified that the n-tuple m from Lemma 4.4 always exists. Using Lemma 4.3, the existence of m comes down to finding integral solutions to r linear equations with integer coefficients in n variables. Using Lemma 4.4, we can thus find an explicit hauptmodul for Γ of the form (4-3) with $M = 1$ (we have $m_{a,i} = m_i$ if $a \in \mathcal{O}_i$).

Remark 4.5. One can also abstractly prove the existence of the n-tuple m. If N is an *odd* prime power, then any modular function of level N whose zeros and poles are all cusps can be expressed as a constant times a product of Siegel functions g_a with $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}$; see [Kubert and Lang 1981, Chapter 5, Theorem 1.1(i)].

If $N \ge 4$ is a power of 2, this can also be deduced from [loc. cit.]. (One needs to be a little careful here since g_a has a different definition in [Kubert and Lang 1981, Chapter 4, §1] when $2a \in \mathbb{Z}$. For the alternate g_a from the previous work with $2a \in \mathbb{Z}$, one can express them as a constant times a product of Siegel functions $g_{a'}$ with $a' \in \mathcal{A}_4 \subseteq \mathcal{A}_N$.)

The case $N = 2$ can be handled directly. For example, one can show that

$$g^8_{(1/2,0)} \cdot g^4_{(1/2,1/2)} \quad \text{and} \quad g^{12}_{(1/2,0)} \cdot g^{12}_{(1/2,1/2)}$$

are hauptmoduls for $\Gamma(2)$ and $\Gamma_0(2)$, respectively (note that $\Gamma_{\mathrm{ns}}(2)$ has a single cusp and does not fall into this case; it falls into case 2 below).

Case 2: a single cusp and $N \neq 11$. Now assume that X_Γ has a single cusp and that $N \neq 11$. There are no nonconstant modular functions for Γ whose zeros and poles are only at the cusps of X_Γ. In particular, a hauptmodul of Γ is never be equal to a product of Siegel functions.

Using the Cummins–Pauli classification, we find that there is a congruence subgroup Γ' that is a proper normal subgroup of Γ, also of level N and containing $-I$, such that $X_{\Gamma'}$ has genus 0 and has exactly $[\Gamma : \Gamma']$ cusps (this is where we use $N \neq 11$).

Since $X_{\Gamma'}$ has multiple cusps, we know from Case 1 how to construct a hauptmodul h' of Γ' with coefficients in K_N that is of the form (4-3). Using that Γ' is normal in Γ, we find that $h'|_\gamma$ is modular for Γ' for all $\gamma \in \Gamma$ and the function depends only on the coset $\Gamma' \cdot \gamma$. Define

$$h := \sum_{\gamma \in \Gamma' \backslash \Gamma} h'|_\gamma;$$

it is a modular function for Γ. Since X_Γ has only one cusp and $X_{\Gamma'}$ has $[\Gamma : \Gamma']$ cusps, we deduce that the modular functions $\{h'|_\gamma\}_{\gamma \in \Gamma' \backslash \Gamma}$ on $X_{\Gamma'}$ each have their unique (simple) pole at different cusps. This implies that h has a simple pole at the unique cusp of X_Γ and is holomorphic elsewhere. Therefore, h is a hauptmodul for Γ.

Since h' is modular for $\Gamma(N)$ and has coefficients in K_N, so does $h'|_\gamma$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$; see Proposition 2.2. Therefore, the coefficients of h lie in K_N.

Finally, it remains to show that h is of the form (4-3). It suffices to show that $h'|_\gamma$ is of the form (4-3) for a fixed $\gamma \in \Gamma$. We know that h' is equal to some product $\zeta_{2N^2}^e \prod_{a \in \mathcal{A}_N} g_a^{m_a}$, so

$$h|_\gamma = \varepsilon(\gamma)^b \zeta_{2N^2}^e \prod_{a \in \mathcal{A}_N} g_{a\gamma}^{m_a}$$

with $b := \sum_{a \in \mathcal{A}_N} m_a$ by Lemma 4.1(iii). Recall that for each $a \in \mathcal{A}_N$, there is a unique $a * \gamma \in \mathcal{A}_N$ such that $a\gamma$ lies in the same coset of $(N^{-1}\mathbb{Z}^2)/\mathbb{Z}^2$ as $a * \gamma$ or $-a * \gamma$. From Lemma 4.1(i) and (ii), the functions $g_{a\gamma}^{m_a}$ and $g_{a*\gamma}^{m_a}$ agree up to a multiplication by some computable root of unity $-\zeta_N^{e'}$. Therefore, $h|_\gamma$ is equal to $\varepsilon(\gamma)^b$ times a function of the form (4-3) with $M = 1$.

It remains only to show that $\varepsilon(\gamma)^b$ is a power of a $2N^2$-th root of unity. Kubert and Lang [1981, Chapter 3, §5] give a necessary and sufficient condition for the product $\prod_{a \in \mathcal{A}_N} g_a^{m_a}$ to be modular for $\Gamma(N)$; these conditions hold since h' is modular for $\Gamma' \supseteq \Gamma(N)$. If N is a power of a prime $\ell \geq 5$, then [Kubert and Lang 1981, Chapter 3, Theorem 5.2] implies that $b \equiv 0 \pmod{12}$ and hence $\varepsilon(\gamma)^b = 1$. If N is a power of 3, then [Kubert and Lang 1981, Chapter 3, Theorem 5.3] implies that $b \equiv 0 \pmod 4$ and hence $\varepsilon(\gamma)^b$ is a power of ζ_3. If N is a power of 2, then [Kubert and Lang 1981, Chapter 3, Theorem 5.3] implies that $b \equiv 0 \pmod 3$ and hence $\varepsilon(\gamma)^b$ is a power of ζ_4. Therefore, $\varepsilon(\gamma)^b$ is indeed a power of a $2N^2$-th root of unity.

Case 3: $N = 11$. The remaining case is when X_Γ has a single cusp and $N = 11$. We include this case only for completeness; we will not need it for our application.

Define the function

$$f(\tau) := \prod_{(a_1, a_2) \in B} g_{(a_1/11,\, a_2/11)}(\tau),$$

where

$$\begin{aligned} B := \big\{&(0,1), (0,2), (0,3), (1,0), (1,2), (1,5), (1,7), (2,1), (2,2),\\ &(2,4), (2,5), (2,6), (2,7), (2,8), (2,9), (2,10), (3,0), (3,2),\\ &(3,4), (3,5), (3,6), (3,8), (3,10), (4,0), (4,1), (4,2), (4,4),\\ &(4,5), (4,6), (5,1), (5,4), (5,5), (5,6), (5,7), (5,8), (5,9)\big\}. \end{aligned}$$

One can verify that

$$\sum_{(a_1,a_2)\in B} a_1^2 \equiv \sum_{(a_1,a_2)\in B} a_2^2 \equiv \sum_{(a_1,a_2)\in B} a_1 a_2 \equiv 0 \pmod{11}$$

and that $|B| = 36 \equiv 0 \pmod{12}$. Theorem 5.2 of [Kubert and Lang 1981, Chapter 3, §5] implies that f is a modular function for $\Gamma(11)$. Using

$$\sum_{(a_1,a_2)\in B} \frac{1}{11} a_2 \cdot \frac{\frac{1}{11} a_1 - 1}{2} = -\frac{60}{11}$$

and the q-expansion of Siegel functions from Section 4A, we find that all the coefficients of f lie in K_{11}. Therefore, $f \in \mathcal{F}_{11}$.

Using that $\Gamma(11)$ is normal in Γ, we find that $f|_\gamma$ is modular for $\Gamma(11)$ for all $\gamma \in \Gamma$ and the function depends only on the coset $\Gamma(11) \cdot \gamma$. Define

$$h := \sum_{\gamma \in \Gamma(11) \backslash \Gamma} f|_\gamma;$$

it is a modular function for Γ. That h is of the form (4-3) follows as in the previous case.

We claim that h is a hauptmodul for Γ. From our description of h in terms of Siegel functions, we find that h has no poles except possibly at the unique cusp (at ∞). From [Cummins and Pauli 2003], there is a unique genus 0 congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level 11 up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$ (the one labeled $11\mathrm{A}^0$). We have computed all the possible Γ and shown that h has a simple pole at ∞, and is therefore a hauptmodul.

Remark 4.6. The set B comes from Section 5.3 of [Chua et al. 2004]. That work gives methods to compute hauptmoduls for genus 0 congruence subgroups (unfortunately, the accompanying hauptmodul tables are no longer available). The authors use "generalized Dedekind eta functions", which are essentially Siegel functions.

4D. ***The rational function $J(t)$.*** For a hauptmodul h of Γ, there is a unique function $J(t) \in \mathbb{C}(t)$ such that $J(h) = j$; it has degree $d := [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]$.

Let us briefly explain how to compute $J(t)$ assuming that one can compute sufficiently many terms of the expansion of f. Let $K \subseteq \mathbb{C}$ be a field containing all the coefficients of h. Consider the equation

$$(a_d h^d + \cdots + a_1 h + a_0) - j \cdot (b_d h^d + \cdots + b_1 h + b_0) = 0 \tag{4-4}$$

with unknowns $a_i, b_i \in K$, where $d := [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]$. Computing the q-expansion coefficients of the left-hand side of (4-4) yields a system of homogeneous linear equations in the unknowns a_i and b_i. The existence and uniqueness of J ensure that the solutions $(a_1, \ldots, a_d, b_1, \ldots, b_d) \in K^{2d}$ form a one-dimensional subspace. By computing sufficiently many coefficients of (4-4) one can find a nonzero solution $(a_1, \ldots, a_d, b_1, \ldots, b_d) \in K^{2d}$, unique up to scaling by $K^\times$, and

$$J(t) = \frac{a_d t^d + \cdots + a_1 t + a_0}{b_d t^d + \cdots + b_1 t + b_0} \in K(t)$$

is then the unique rational function for which $J(h) = j$. Note that if the hauptmodul h is constructed as in the previous section then we have $J(t) \in K_N(t)$, where N is the level of Γ.

5. Modular curves of genus 0

Fix the following:

- An integer $N > 1$ that is a prime power.
- A subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$.
- A rational function $J(t) \in \mathbb{Q}(t)$.

In this section, we explain how to determine if the function field of X_G is of the form $\mathbb{Q}(f)$ for some modular function $f \in \mathcal{F}_N$ satisfying $J(f) = j$. We will use this to verify the entries of Tables 1–3, found in the online supplement.

If such an f exists, then $X_G \simeq \mathbb{P}^1_{\mathbb{Q}}$ and the isomorphism $\pi_G : X_G \to \mathbb{P}^1_{\mathbb{Q}}$ is given by the relation $j = J(f)$ in their function fields. We may assume the necessary condition that $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G] = \deg \pi_G$ agrees with the degree of $J(t)$.

Remark 5.1. In Section 8 we explain how the $J(t)$ listed in Tables 1–3 of the online supplement, were actually found, which involves the use of a Monte Carlo algorithm and assumes the generalized Riemann hypothesis (GRH). The purpose of this section is to explain how we can unconditionally verify a given $J(t)$, regardless of how it was found.

5A. *Construction of possible f.* Let Γ be the congruence subgroup consisting of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ for which γ^t modulo N lies in G (equivalently, in $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$). By Lemma 2.4(ii), we may assume that Γ has genus 0 since otherwise X_G has positive genus and its function field cannot be of the form $\mathbb{Q}(f)$.

The group Γ acts on the right on the field $\mathcal{F}_N$; let $\mathcal{F}_N^\Gamma$ be subfield fixed by this action. By Lemma 2.4(i), we have $K_N(X_G) = \mathcal{F}_N^\Gamma$.

In Section 4C, we described how to compute an explicit hauptmodul h for Γ such that coefficients of its q-expansion all lie in $K_{N'} \subseteq K_N$, where the level N' of Γ divides N. Therefore, we have

$$K_N(X_G) = \mathcal{F}_N^\Gamma = K_N(h).$$

Moreover, we can express h in terms of Siegel functions and hence we can compute as many of its coefficients as we desire. In Section 4D, we described how to compute the unique rational function $J'(t) \in K_N(t)$ for which $j = J'(h)$. The degree of $J'(t)$ agrees with $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$, thus $J(t)$ and $J'(t)$ have the same degree.

Remark 5.2. The rational function $J'(t)$ gives a map to the j-line from X_Γ, which is defined over $K_N = \mathbb{Q}(\zeta_N)$, while the rational function $J(t)$ gives a map to the j-line from X_G, which is defined over $\mathbb{Q}$. We use $J'(t)$ in our procedure to verify $J(t)$, but note that $J'(t)$ does not determine $J(t)$; in general there will be multiple nonconjugate subgroups G corresponding to Γ and a different rational function $J(t)$ for each of the corresponding X_G (in total we have 220 modular curves X_G of genus 0 corresponding to 73 modular curves X_Γ).

Lemma 5.3. *The modular functions $f \in K_N(X_G)$ that satisfy $K_N(X_G) = K_N(f)$ and $J(f) = j$ are precisely those of the form $\psi(h)$, where $\psi(t) \in K_N(t)$ is a degree 1 function satisfying $J'(t) = J(\psi(t))$.*

Proof. First take any $\psi(t) \in K_N(t)$ of degree 1 satisfying $J'(t) = J(\psi(t))$. Define $f := \psi(h)$. We have $K_N(f) = K_N(h) = K_N(X_G)$, since ψ has an inverse, and $J(f) = J(\psi(h)) = J'(h) = j$.

Now suppose that $K_N(X_G) = K_N(f)$ for some $f \in K_N(X_G)$ satisfying $J(f) = j$. Since $K_N(f) = K_N(X_G) = K_N(h)$, we have $f = \psi(h)$ for a unique $\psi(t) \in K_N(t)$

of degree 1. We then have $j = J(f) = J(\psi(h))$ and therefore $J'(t) = J(\psi(t))$, since $J'(t)$ is the unique element of $K_N(t)$ that satisfies $J'(h) = j$. $\square$

5B. ***Finding possible f.*** Define Ψ to be the set of $\psi(t) \in K_N(t)$ of degree 1 for which $J'(t) = J(\psi(t))$; these ψ arise in Lemma 5.3. We now explain how to compute Ψ.

Choose three distinct elements $\beta_1, \beta_2, \beta_3 \in K_N \cup \{\infty\}$. For $1 \le i \le 3$, define the set

$$R_i := \bigl\{\alpha \in K_N \cup \{\infty\} : J'(\beta_i) = J(\alpha) \text{ and } \operatorname{ord}_{\beta_i}(J') = \operatorname{ord}_\alpha(J)\bigr\},$$

where $\operatorname{ord}_{\beta_i}(J')$ is the order of vanishing of $J'(t)$ at $t = \beta_i$. Let R be the set of triples $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in R_1 \times R_2 \times R_3$ such that α_1, α_2, and α_3 are distinct. Let $\psi_\alpha \in K_N(t)$ be the *unique* rational function of degree 1 such that $\psi_\alpha(\beta_i) = \alpha_i$ for all $1 \le i \le 3$.

Take any $\psi \in \Psi$. We have $J'(\beta_i) = J(\psi(\beta_i))$ and $\operatorname{ord}_\beta(J') = \operatorname{ord}_{\psi(\beta)}(J)$ for each $1 \le i \le 3$. Therefore, $\psi(\beta_i) \in R_i$ for each $1 \le i \le 3$ and hence $\psi = \psi_\alpha$ for some $\alpha \in R$. So we have

$$\Psi = \bigl\{\psi_\alpha : \alpha \in R,\ J'(t) = J(\psi(t))\bigr\}.$$

Since R is finite, this gives us a way to compute the (finite) set Ψ.

By Lemma 5.3, the set

$$\{\psi(h) : \psi \in \Psi\}$$

is the set of modular functions $f \in K_N(X_G)$ that satisfy $K_N(X_G) = K_N(f)$ and $J(f) = j$.

5C. ***Checking each f.*** Let f be one of the finite number of functions that satisfy $K_N(X_G) = K_N(f)$ and $J(f) = j$. We just saw how to compute all such f; they are of the form $\psi(h)$ for a degree 1 function $\psi(t) \in K_N(t)$ and a modular function h satisfying $K_N(X_G) = K_N(h)$ that is expressed in terms of Siegel functions. Recall from Section 2D that each $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $\mathcal{F}_N$ via the isomorphism $\theta_N : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$ of Proposition 2.2, and for $f \in \mathcal{F}_N$ we use $A_*(f) := \theta_N(A)(f)$ to denote this action.

Lemma 5.4. (i) *We have $\mathbb{Q}(X_G) = \mathbb{Q}(f)$ if and only if $f \in \mathbb{Q}(X_G)$.*

(ii) *For a matrix $A \in G$, we have $A_*(f) = f$ if and only if $\operatorname{ord}_q(A_*(f) - f) > 2w/N'$, where w is the width of the cusp ∞ of X_Γ and N' is the level of Γ.*

Proof. We first prove part (i); only one implication needs proof. Suppose that $f \in \mathbb{Q}(X_G)$. Then $\mathbb{Q}(f) \subseteq \mathbb{Q}(X_G)$ and it suffices to show that these two fields have the same degree over $\mathbb{Q}(j)$. This is true since we have been assuming that $\deg \pi_G$ is equal to the degree of $J(t)$.

For part (ii), again only one implication needs proof. Suppose $\mathrm{ord}_q(A_*(f)-f) > 2w/N'$. As meromorphic functions on X_Γ, f and $A_*(f)$ have a unique (simple) pole since h has this property and ψ has degree 1. Therefore, the function $A_*(f)-f$ on X_Γ is zero or has at most two poles (and hence at most two zeros). Our assumption $\mathrm{ord}_q(A_*(f)-f) > 2w/N'$ implies that $A_*(f)-f$ has a zero of order 3 at the cusp ∞ and thus $A_*(f)-f=0$. □

By Lemma 5.4(i), we have $\mathbb{Q}(X_G)=\mathbb{Q}(f)$ if and only if $A_*(f)=f$ for all $A\in G$ in a set of generators of G; it suffices to consider $A\in G$ for which $\det(A)$ generate $(\mathbb{Z}/N\mathbb{Z})^\times$ since h and hence f is fixed by $G\cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. It remains to describe how to determine whether $A_*(f)$ is equal to f. By Lemma 5.4(ii), it suffices to compute enough terms of the q-expansion of $A_*(f)-f$ to determine whether $\mathrm{ord}_q(A_*(f)-f) > 2w/N'$ holds.

Finally, let us briefly explain how to compute terms in the q-expansion of $A_*(f)-f$. Let d be an odd integer congruent to $\det(A)$ modulo N. Choose a matrix $\gamma\in \mathrm{SL}_2(\mathbb{Z})$ so that $A^t \equiv \left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)\gamma \pmod N$. We thus have

$$A_*(f)-f=\sigma_d(f)|_\gamma - f=\sigma_d(\psi)(\sigma_d(h)|_\gamma)-\psi(h), \tag{5-1}$$

where $\sigma_d(\psi)$ is the rational function with σ_d applied to the coefficients of its numerator and denominator. Our hauptmodul h is of the form $\sum_{i=1}^M \zeta_{2N^2}^{e_i}\prod_{a\in\mathcal{A}_N} g_a^{m_{a,i}}$ for certain integers e_i and $m_{a,i}$, so

$$\sigma_d(h)|_\gamma=\sum_{i=1}^M \zeta_{2N^2}^{e_i d}\prod_{a\in\mathcal{A}_N}(\sigma_d(g_a)|_\gamma)^{m_{a,i}}.$$

From the series expansion of g_a, one easily checks that $\sigma_d(g_{(a_1,a_2)})=g_{(a_1,da_2)}$. From Lemma 4.1(iii), we have $\sigma_d(g_a)|_\gamma=\varepsilon(\gamma)g_{(a_1,da_2)\gamma}$ and hence

$$\sigma_d(h)|_\gamma=\sum_{i=1}^M \zeta_{2N^2}^{e_i d}\cdot\prod_{a\in\mathcal{A}_N}\varepsilon(\gamma)^{m_{a,i}}\cdot\prod_{a\in\mathcal{A}_N} g_{(a_1,da_2)\gamma}^{m_{a,i}}.$$

Thus by computing enough terms in the q-expansion of the functions $\{g_a\}_{a\in\mathcal{A}_N}$, we are able to compute the q-expansion of h and $\sigma_d(h)|_\gamma$ to as many terms as we desire. This allows us to compute terms in the q-expansion of $A_*(f)-f$ via (5-1).

Remark 5.5. Suppose that X_Γ has at least 3 cusps. We then have $A_*(f)=f$ if and only if $A_*(f)$ and f take the same value at any three of the cusps (as in the proof of Lemma 5.4, this implies that $A_*(f)-f$ has at least three zeros and hence is the zero function). In the case of at least three cusps, our hauptmodul h was given as a constant times a product of Siegel functions; so its value at the cusp ∞ is determined by the first term of the q-expansion of h. The value at any other cusp c can be determined by the first term of the q-expansion of $h|_\gamma$ with $\gamma\in\mathrm{SL}_2(\mathbb{Z})$

satisfying $\gamma\infty = c$. This approach is quicker since fewer terms of the q-expansions are required.

5D. ***Verifying the entries of our tables.*** We now explain how to verify the validity of our genus 0 tables. Magma scripts that perform these verifications can be found in [Sutherland and Zywina 2016].

In the online supplement, each row of Tables 1–3 gives a set of generators of a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ for a prime power N. We may assume that $N > 1$. By composing rational maps, we obtain a corresponding rational function $J(t) \in \mathbb{Q}(t)$.

Using the earlier parts of Section 5, we can construct a modular function $f \in \mathcal{F}_N$ such that $\mathbb{Q}(X_G) = \mathbb{Q}(f)$ and $J(f) = j$. So X_G is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and the morphism $\pi_G : X_G \to \mathbb{P}^1_{\mathbb{Q}}$ is given by the relation $j = J(f)$ in their function fields. (We also note that there is no harm in replacing G by a conjugate group; this is useful because one can reuse the hauptmodul computations for different groups in the tables.)

Fix a group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as above, and a modular function $f \in \mathcal{F}_N$ satisfying $\mathbb{Q}(X_G) = \mathbb{Q}(f)$ and $J(f) = j$.

Now fix another group $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$ from our table so that N divides N' and the image of G' in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is conjugate to a subgroup of G. In the above computations, we have constructed a modular function f' satisfying $\mathbb{Q}(X_{G'}) = \mathbb{Q}(f')$ and $J'(f') = j$ for a rational function $J'(t) \in \mathbb{Q}(t)$ also arising from the tables.

Take any subgroup $\widetilde{G} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ conjugate to G' whose image modulo N lies in G. Choose any $A \in \mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$ for which $\widetilde{G} := AG'A^{-1}$ and define $\tilde{f} := A_*(f')$. We have an inclusion of fields

$$\mathbb{Q}(\tilde{f}) = \mathbb{Q}(X_{\widetilde{G}}) \supseteq \mathbb{Q}(X_G) = \mathbb{Q}(f).$$

The extension $\mathbb{Q}(\tilde{f})/\mathbb{Q}(f)$ has degree $i := [\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z}) : G'] / [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$. Therefore, $\varphi(\tilde{f}) = f$ for a unique $\varphi(t) \in \mathbb{Q}(t)$ of degree i. We can compute $\varphi(t)$ using the method from Section 4D; the coefficients of f and $\tilde{f}$ can be computed as in Section 5C.

The rational function φ is not unique, it depends on the choices of $\widetilde{G}$, f, f', and A. However, any other rational function occurring would be of the form $\psi'(\varphi(\psi(t)))$, where $\psi, \psi' \in \mathbb{Q}(t)$ are degree 1 functions satisfying $J(\psi(t)) = J(t)$ and $J'(\psi'(t)) = J'(t)$. Note that all the possible ψ and ψ' can be computed as in Section 5B (with $J = J'$). We have checked that the rational function relating G and G' in our tables, when given, is indeed of the form $\psi'(\varphi(\psi(t)))$.

6. Modular curves of genus 1

We now consider the open subgroups G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with genus 1 and prime power level $N = \ell^e$ that satisfy $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$. We are interested in describing those G for which $X_G(\mathbb{Q})$ is infinite. There is no harm in replacing G by a conjugate. So by Theorem 3.3(ii), there are 250 cases that need to be checked.

Let J_G be the Jacobian of the curve X_G. Using the methods of [Zywina 2015b], we can compute the rank of $J_G(\mathbb{Q})$. From [Deligne and Rapoport 1973, §IV], we find that the curve X_G has good reduction at all primes $p \nmid N = \ell^e$. Therefore, J_G is an elliptic curve defined over $\mathbb{Q}$ whose conductor is a power of ℓ. The primes ℓ that arise are small enough to ensure that J_G is isomorphic to one of the elliptic curves in Cremona's [2016] tables; this gives a finite number of candidates for J_G up to isogeny.

For each prime $p \nmid 6\ell$, we can compute $\#J_G(\mathbb{F}_p) = \#X_G(\mathbb{F}_p)$ from the modular interpretation of X_G; see [Zywina 2015b, §3.6] for details. In particular, we can compute $\#J_G(\mathbb{F}_p)$ directly from the group G without computing a model for X_G (or its reduction modulo p). By computing several values of $\#J_G(\mathbb{F}_p)$ with $p \neq \ell$, we can quickly distinguish the isogeny class of J_G among the finite set of candidates. We then compute the rank of $J_G(\mathbb{Q})$, which we note is an isogeny invariant.

Running this procedure on each of the 250 genus 1 groups G given by Theorem 3.3, we find that $J_G(\mathbb{Q})$ has rank 0 for 222 groups and $J_G(\mathbb{Q})$ has positive rank for 28 groups; a Magma script that performs this computation can be found in [Sutherland and Zywina 2016]. We need only consider the 28 groups G for which $J_G(\mathbb{Q})$ has positive rank, since $X_G(\mathbb{Q})$ is finite if $J_G(\mathbb{Q})$ has rank 0.

Now let G be one of the 28 groups for which $J_G(\mathbb{Q})$ has positive rank; they are precisely the 28 genus 1 groups in Theorem 1.1 and can be found in Table 4 of the online supplement. For each of these groups G, if $X_G(\mathbb{Q})$ is nonempty then it must be infinite, since the Abel–Jacobi map then gives a bijection from $X_G(\mathbb{Q})$ to $J_G(\mathbb{Q})$. We initially verified that $X_G(\mathbb{Q})$ is nonempty by finding an elliptic curve $E/\mathbb{Q}$ with $\rho_E(\mathrm{Gal}_{\mathbb{Q}}) \subseteq G$ using an extension of the algorithm in [Sutherland 2016].

For each of these 28 groups G, a model for X_G and the morphism π_G can already be found in the literature (and are equivalent to the ones we give in the online supplement). For the 27 groups G of level 16 these curves and morphisms were constructed in [Rouse and Zureick-Brown 2015]; the models and morphisms we give in Table 4 for these groups are slightly different (we constructed them by taking fiber products of our genus 0 curves), but we have verified that they are isomorphic (note that their groups are transposed relative to ours). The remaining group G has level 11 and its image in $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ is the normalizer of a nonsplit Cartan subgroup. An explicit model for $X_G = X_{\mathrm{ns}}^+(11)$ and the morphism to the j-line can be found in [Halberstadt 1998]; these are reproduced in the online supplement.

7. Proof of Theorem 1.4

If $\ell \leq 13$, then the set $\mathcal{J}_\ell$ is finite by [Zywina 2015b, Proposition 4.8]. If $\ell > 13$, this follows from [Zywina 2015b, Proposition 4.9]; note that ρ_{E,ℓ^∞} is surjective if and only if $\rho_{E,\ell}$ is surjective, since $\ell \geq 5$, by [Serre 1968, §IV, Lemma 3]. This proves (i).

For a group G from Theorem 1.1, define the set

$$\mathcal{S}_G := \bigcup_{G'} \pi_{G',G}(X_{G'}(\mathbb{Q})),$$

where G' varies over the proper subgroups of G that are conjugate to one of the groups in Theorem 1.1 of ℓ-power level and $\pi_{G',G} : X_{G'} \to X_G$ is the natural morphism induced by the inclusion $G' \subseteq G$. Note that this is a finite union.

Suppose first that G has genus 0. Then $X_G \simeq \mathbb{P}^1_{\mathbb{Q}}$ and $\mathcal{S}_G$ is a *thin* subset of $X_G(\mathbb{Q})$, in the language of [Serre 1997, §9]. The field $\mathbb{Q}$ is Hilbertian, and in particular $\mathbb{P}_1(\mathbb{Q}) \simeq X_G(\mathbb{Q})$ is not thin; this implies that the complement $X_G(\mathbb{Q}) - \mathcal{S}_G$ cannot be thin and must be infinite.

Suppose that G has genus 1. If G does not have level 16 and index 24, then there are no proper subgroups G' of G that are conjugate to a group from Theorem 1.1, and therefore $\mathcal{S}_G$ is empty and $X_G(\mathbb{Q}) - \mathcal{S}_G$ is infinite.

Now suppose that G has genus 1, level 16, and index 24. There are 7 such G, labeled

$$16\mathrm{C}^1\text{-}16\mathrm{c},\ 16\mathrm{C}^1\text{-}16\mathrm{d},\ 16\mathrm{B}^1\text{-}16\mathrm{a},\ 16\mathrm{B}^1\text{-}16\mathrm{c},\ 16\mathrm{D}^1\text{-}16\mathrm{d},\ 8\mathrm{D}^1\text{-}16\mathrm{b},\ 8\mathrm{D}^1\text{-}16\mathrm{c}$$

and explicitly described in Table 4 of the online supplement. Each of these G contains either two or four index 2 subgroups G' that are conjugate to one of the groups in Theorem 1.1. In every case we have $\mathcal{S}_G = X_G(\mathbb{Q})$, so that $X_G(\mathbb{Q}) - \mathcal{S}_G$ is empty; see [Rouse and Zureick-Brown 2015, Example 6.11, Remark 6.3].

Let $E/\mathbb{Q}$ be an elliptic curve with $j_E \notin \mathcal{J}_\ell$. The group $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to the ℓ-adic projection of a unique group G from Theorem 1.1 with ℓ-power level. Using Proposition 2.6, we can also characterize G as the unique group from Theorem 1.1 with ℓ-power level such that $j_E \in \pi_G(X_G(\mathbb{Q}) - \mathcal{S}_G)$. Parts (ii) and (iii) follow by noting that $\pi_G(X_G(\mathbb{Q}) - \mathcal{S}_G)$ is empty when G has genus 1, level 16, and index 24, and it is infinite otherwise.

8. How the $J(t)$ were found

Let G be one of the genus 0 subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ from Theorem 1.1; they are listed in Tables 1–3 of the online supplement and were determined using the algorithm described in Section 3. For each G, we also have a rational function $J(t) \in \mathbb{Q}(t)$

such that the function field of X_G is of the form $\mathbb{Q}(f)$ and $j = J(f)$, where j is the modular j-invariant; the verification of this property is described in Section 5.

In this section, we explain how we found $J(t)$; note that the method we used to verify the correctness of $J(t)$ does not depend on how it was found! None of our theorems depend on the techniques described in this section. All that matters is that they eventually produced functions $J(t)$ whose correctness we could verify using the procedure described in Section 5D.

We used an extension of the algorithm in [Sutherland 2016] to search for elliptic curves $E/\mathbb{Q}$ for which $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G. This was initially done by simply checking elliptic curves in Cremona's [2016] tables and the LMFDB [LMFDB Collaboration 2013] (but see Remark 8.1 below). After enough searching, we find elliptic curves E_1, E_2, E_3 defined over $\mathbb{Q}$ with distinct j-invariants j_1, j_2, j_3 for which we believe that $\rho_{E_i}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to a subgroup of G; in particular, we expect that $j_1, j_2, j_3 \in \pi_G(X_G(\mathbb{Q}))$. We ran the Monte Carlo algorithm in [Sutherland 2016] using parameters that ensure the error probability is less than 2^{-100}, under the GRH.

Now suppose that j_1, j_2, j_3 are indeed elements of $\pi_G(X_G(\mathbb{Q}))$. The curve X_G has genus 0 and rational points, so it is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. We can choose an isomorphism $X_G \simeq \mathbb{P}^1_{\mathbb{Q}}$ such that there are points $P_1, P_2, P_3 \in X_G(\mathbb{Q})$ satisfying $\pi_G(P_i) = j_i$ which map to 0, 1, ∞, respectively. There is thus a rational function $J(t) \in \mathbb{Q}(t)$ such that $J(0) = j_1$, $J(1) = j_2$, $J(\infty) = j_3$ and such that $\mathbb{Q}(X_G) = \mathbb{Q}(f)$ for a modular function f satisfying $J(f) = j$; the function f is obtained by composing our isomorphism $\mathbb{P}^1_{\mathbb{Q}} \simeq X_G$ with π_G.

We can now find all such potential J. As explained in Section 5, we can construct a modular function $h \in \mathcal{F}_N$ and a rational function $J'(t) \in K_N(t)$ such that $K_N(X_G) = K_N(h)$ and $j = J'(h)$, where N is the level of G. We thus have

$$J(t) = J'(\psi(t))$$

for some degree 1 function $\psi(t) \in K_N(t)$ satisfying $\psi(0) \in R_1$, $\psi(1) \in R_2$, and $\psi(\infty) \in R_3$, where

$$R_i := \{\alpha \in K_N \cup \{\infty\} : J'(\alpha) = j_i\}.$$

Since the sets R_i are finite and disjoint, there are only finitely many $\psi(t) \in \mathbb{Q}(t)$ of degree 1 satisfying $\psi(0) \in R_1$, $\psi(1) \in R_2$, $\psi(\infty) \in R_3$. For each such $\psi(t)$, we check whether $J'(\psi(t))$ lies in $\mathbb{Q}(t)$.

Consider any ψ as above for which $J'(\psi(t)) \in \mathbb{Q}(t)$. Set $J(t) := J'(\psi(t))$ and $f := \psi^{-1}(h) \in K_N(X_G)$. We have $J(f) = J'(h) = j$. The field $\mathbb{Q}(f)$ is thus the function field of a modular curve $X_{G'}$, where G' is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N satisfying $\det(G') = \hat{\mathbb{Z}}^\times$ and $-I \in G'$; it consists of matrices whose reductions modulo N fix f. We can then check whether G is equal to G'. Since

$[\mathrm{GL}_2(\hat{\mathbb{Z}}) : G] = \deg \pi_G = \deg J = [\mathrm{GL}_2(\hat{\mathbb{Z}}) : G']$, it suffices to determine whether G is a subgroup of G'; equivalently, whether G fixes f. A method for determining whether f is fixed by G is described in Section 5C.

We will eventually find a ψ for which we have $G = G'$ (provided that our initial j-invariants j_i are valid). This then proves that $\mathbb{Q}(X_G) = \mathbb{Q}(f)$ for some f satisfying $J(f) = j$, where $J(t) := J'(\psi(t)) \in \mathbb{Q}(t)$.

Note this rational function $J(t)$ is not unique since $J(\varphi(t))$ would also work for any $\varphi(t) \in \mathbb{Q}(t)$ of degree 1. Using similar reasoning, it is easy to determine if two $J_1, J_2 \in \mathbb{Q}(t)$ satisfy $J_2(t) = J_2(\varphi(t))$ for some degree 1 function $\varphi \in \mathbb{Q}(t)$. We have chosen our rational functions so that they are relatively compact when written down.

Remark 8.1. Having run this procedure to obtain functions $J(t)$ for each of the groups G where we were able to find suitable E_1, E_2, E_3 in Cremona's tables, we then address the remaining groups G by picking a group G' that contains a subgroup conjugate to G for which we already know a function $J'(t) \in \mathbb{Q}(t)$; such a G' existed for every G not addressed in our initial search of Cremona's tables. Using the function $J'(t)$ we can quickly obtain a large list of elliptic curves E for which $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of G'. By running the algorithm in [Sutherland 2016] on several thousand (or even millions) of these curves we are eventually able to find E_1, E_2, E_3 with distinct j-invariants for which it is highly probable that $\rho_{E_i}(\mathrm{Gal}_{\mathbb{Q}})$ is actually conjugate to a subgroup of the smaller group G contained in G'. We then proceed as above to compute the function $J(t)$ for G.

Acknowledgements

We thank Jeremy Rouse and David Zureick-Brown for the feedback on an early draft of this article, and the referees for their careful review and helpful comments.

References

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Chua et al. 2004] K. S. Chua, M. L. Lang, and Y. Yang, "On Rademacher's conjecture: congruence subgroups of genus zero of the modular group", *J. Algebra* **277**:1 (2004), 408–428. MR Zbl

[Cremona 2016] J. E. Cremona, "Elliptic curve data", electronic reference, University of Warwick, 2016, available at http://johncremona.github.io/ecdata/.

[Cummins and Pauli 2003] C. J. Cummins and 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. A database containing the tables is available at http://www.uncg.edu/mat/faculty/pauli/congruence/. MR Zbl

[Deligne and Rapoport 1973] P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques", pp. 143–316 in *Modular functions of one variable, II* (Antwerp, 1972), edited by P. Deligne and W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR Zbl

[Dennin 1974] J. B. Dennin, Jr., "The genus of subfields of $K(p^n)$", *Illinois J. Math.* **18** (1974), 246–264. MR Zbl

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. Correction in **75**: 2 (1984), 381. MR Zbl

[Halberstadt 1998] E. Halberstadt, "Sur la courbe modulaire $X_{\text{ndép}}(11)$", *Experiment. Math.* **7**:2 (1998), 163–174. MR Zbl

[Kubert and Lang 1981] D. S. Kubert and S. Lang, *Modular units*, Grundlehren Math. Wissenschaften **244**, Springer, Berlin, 1981. MR Zbl

[LMFDB Collaboration 2013] LMFDB Collaboration, "The L-functions and modular forms database", electronic reference, 2013, available at http://www.lmfdb.org.

[Rouse and Zureick-Brown 2015] J. Rouse and D. Zureick-Brown, "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois", *Res. Number Theory* **1** (2015), art. id. 12. MR

[Serre 1968] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, New York, 1968. MR Zbl

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR Zbl

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), 323–401. MR Zbl

[Serre 1997] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, 3rd ed., Friedr. Vieweg & Sohn, Braunschweig, 1997. MR Zbl

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures **1**, Iwanami Shoten, Tokyo, 1971. MR Zbl

[Sutherland 2016] A. V. Sutherland, "Computing images of Galois representations attached to elliptic curves", *Forum Math. Sigma* **4** (2016), art. id. e4. MR Zbl

[Sutherland and Zywina 2016] A. V. Sutherland and D. Zywina, Magma scripts associated to "Modular curves of prime-power level with infinitely many rational points", 2016, available at http://math.mit.edu/~drew/SZ16.

[Zywina 2015a] D. Zywina, "On the possible images of the mod l representations associated to elliptic curves over $\mathbb{Q}$", preprint, 2015. arXiv

[Zywina 2015b] D. Zywina, "Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$", preprint, 2015. arXiv

Communicated by Joseph H. Silverman
Received 2016-05-20 Revised 2017-02-10 Accepted 2017-03-10

drew@math.mit.edu Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, MA 02139, United States

zywina@math.cornell.edu Department of Mathematics, Cornell University, Ithaca, NY 14853, United States

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2017 is US $325/year for the electronic version, and $520/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 11 No. 5 2017