IMPROVED BOUNDS FOR INTEGRAL POINTS ON MODULAR CURVES USING RUNGE'S METHOD

DAVID ZYWINA

Abstract. Consider a modular curve X_G defined over a number field K, where G is a subgroup of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $N > 2$. The curve X_G comes with a morphism $j\colon X_G \to \mathbb{P}^1_K = \mathbb{A}^1_K \cup \{\infty\}$ to the j-line. For a finite set of places S of K that satisfies a certain condition, Runge's method shows that there are only finitely many points $P \in X_G(K)$ for which $j(P)$ lies in the ring $\mathcal{O}_{K,S}$ of S-units of K. We prove an explicit version which shows that if $j(P) \in \mathcal{O}_{K,S}$ for some $P \in X_G(K)$, then the absolute logarithmic height of $j(P)$ is bounded above by $N^{12}\log N$. Explicits upper bounds have already been obtained by Bilu and Parent though they are not polynomial in N. The modular functions needed to apply Runge's method are constructing using Eisenstein series of weight 1.

1. Introduction

Fix an integer $N > 2$ and consider a subgroup G of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $-I$. Associated to the group G is a modular curve X_G that is defined over the number field $K_G := \mathbb{Q}(\zeta_N)^{\det(G)}$ and is smooth, projective and geometrically irreducible; see §2 for details. In particular, the curve X_G is defined over $\mathbb{Q}$ when $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. The curve X_G comes with a nonconstant morphism

$$j\colon X_G \to \mathbb{P}^1_{K_G} = \mathbb{A}^1_{K_G} \cup \{\infty\}$$

to the j-line. The cusps of X_G are the points lying over ∞. We define Y_G to be the open subvariety of X_G that is the complement of its cusps.

Fix a number field $K \supseteq K_G$. Let S be a finite set of places of K that contains all the infinite places and let $\mathcal{O}_{K,S}$ be the ring of S-integers in K. Let $\mathfrak{c}_{G,K}$ be the number of orbits of the action of the Galois group $\operatorname{Gal}(\overline{K}/K)$ on the set of cusps $X_G(\overline{K}) - Y_G(\overline{K})$. We say that the pair (K,S) satisfies Runge's condition for X_G if $|S| < \mathfrak{c}_{G,K}$.

Assume that (K,S) satisfies Runge's condition for X_G. *Runge's method* shows that there only finitely many points $P \in Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$. For background on Runge's method see [Sch08, Chapter 5], [BG06, §9.6.5] or [LF19, §4]. An effective version for modular curves was given by Bilu and Parent [BP11] where they showed that for all points $P \in Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$, we have

$$h(j(P)) \le 36|S|^{|S|/2+1}(N^2|G|/2)^{|S|}\log(2N), \tag{1.1}$$

where h denotes the logarithmic absolute height.

Our main result gives a bound for $h(j(P))$ which is polynomial in N and independent of $|S|$; the bound in (1.1) is polynomial in N only when we bound $|S|$.

Theorem 1.1. *Fix an integer $N > 2$ and a subgroup G of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. Let μ be the degree of the morphism $j\colon X_G \to \mathbb{P}^1_{K_G}$. Assume that (K,S) satisfies Runge's condition for X_G, where $K \supseteq K_G$ is a number field and S is a finite set of places of K that contains all the infinite places. Then for any point $P \in Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$, we have $h(j(P)) \le 4(\mu+4)^4 \log N$ and hence*

$$h(j(P)) \le N^{12}\log N.$$

Remark 1.2.

(i) Since G contains $-I$, we have $\mu = [\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z}) : G \cap \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})]$. In particular, we have $\mu \le |\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}| \le N^3/2$. Using that $N > 2$, we find that $4(\mu+4)^4 \le 4(N^3/2+4)^4 \le N^{12}$. This explains how the first inequality of Theorem 1.1 implies the second one.

2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F11.

(ii) Since h is the logarithmic absolute height, Theorem 1.1 implies that there are only finitely many points $P \in Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$ as we vary over all pairs (K, S) satisfying Runge's condition for X_G, where K is a subfield of a fixed algebraic closure of K_G.

(iii) Consider a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for which X_G has at least 3 distinct cusps. Take any number field $K \supseteq K_G$ and any finite set of places S of K. From a classical theorem of Siegel, there are only finitely many points $P \in X_G(K)$ for which $j(P) \in \mathcal{O}_{K,S}$. Unfortunately, Siegel's theorem gives no way to bound the height of the j-invariants $j(P)$ that arise. Bilu [Bil95, §5] showed that the heights could actually be effectively bounded by making use of Baker's method. A quantitative version was given by Sha [Sha14] and see also [Cai22]. We will not state the explicit bound of Sha, but simply remark that it implies that $\log(h(j(P)) + 1) \leq C_{K,S} N \log N$ holds for all $P \in Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$, where $C_{K,S}$ is a positive constant depending only on the pair (K, S). Note that when Runge's condition holds, the bounds in Theorem 1.1 will be stronger and will have no dependency on (K, S).

(iv) The condition $N > 2$ is used several times during the proof; for such N, the classical modular curve $X(N)$ over $\mathbb{Q}(\zeta_N)$ is a fine moduli space. For the excluded case $N = 2$, one can simply lift G to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ to obtain bounds.

(v) Let g be the genus of X_G. We have $\mu < 101(g + 1)$, see the comments after [CP03, Proposition 2.3]. For a pair (K, S) that satisfies Runge's condition for X_G, Theorem 1.1 implies that

$$h(j(P)) \leq 4((101(g + 1) + 4)^4 \cdot \log N$$

holds for all $P \in Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$.

(vi) The points of our modular curves give important arithmetic information about elliptic curves which we now recall; this will not be used elsewhere. Fix a number field $K \supseteq K_G$. Let E be an elliptic curve over K with j-invariant $j(E) \notin \{0, 1728\}$. The N-torsion subgroup $E[N]$ of $E(\overline{K})$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. The natural Galois action on $E[N]$ and a choice of basis gives a Galois representation $\rho_{E,N}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}/N\mathbb{Z}}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. One can show that $\rho_{E,N}(\mathrm{Gal}(\overline{K}/K))$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G^t if and only if $j(E) = j(P)$ for some $P \in Y_G(K)$. Here G^t is the group obtained by taking the transpose of the elements of G. As a warning, we note that in the literature, our modular curve X_G is sometimes denoted X_{G^t}.

1.1. **Overview.** Fix an integer $N > 2$ and a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Fix a number field $K \supseteq K_G$ and a finite set S of places of K containing all the infinite places. The set $\mathcal{C}_G := X_G(\overline{K}) - Y_G(\overline{K})$ of cusps has a natural action by $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$. Assume that Runge's condition for X_G holds for the pair (K, S), i.e., the number of Gal_K-orbits on $\mathcal{C}_G$ is strictly greater than $|S|$.

Consider any nonempty and proper subset $\Sigma \subseteq \mathcal{C}_G$ that is Gal_K-stable. To apply Runge's method, we need a nonconstant function $\varphi \in K(X_G)$ that satisfies the following properties:

- The poles of φ occur only at cusps of X_G.
- The function φ is regular at each cusp in Σ.
- The function φ is a root of a monic polynomial with coefficients in $\mathbb{Z}[j]$.

The existence of a nonconstant function $\varphi \in K(X_G)$ that satisfies the first two properties is an easy consequence of the Riemann–Roch theorem. Since such a function φ is integral over $\mathbb{Q}[j]$, we obtain the third property after scaling φ by an appropriate positive integer. However, this existence is not enough for our application since we also need good estimates on the function φ; especially near the cusps.

The functions φ used by Bilu and Parent in [BP11] are *modular units*, i.e., their zeros and poles only occur at cusps. The existence of suitable modular units is not a consequence of the Riemann–Roch theorem but follows from the Manin–Drinfeld theorem. Modular units can be explicitly constructed by taking products and quotients of Siegel functions; these have many nice properties and have an explicit q-expansion at each cusp. One downside to dealing with modular units is that they can have poles of high order and their q-expansion can have relatively large coefficients. For example in the proof of Bilu and Parent, modular units on X_G arise for which the order of the poles might not be uniformly bounded by a polynomial in N.

Let Δ be the modular discriminant function; it is a cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$ that is everywhere nonzero when viewed as a function of the complex upper half-plane. For a function $\varphi \in K(X_G)$ whose poles only occur at cusps, $\varphi \cdot \Delta^m$ will be a modular form of weight $12m$ on $\Gamma(N)$ for all sufficiently large m.

Now fix a positive integer m. Consider the finite dimensional K_G-vector space $M_{12m,G}$ consisting of those modular forms f of weight $12m$ on $\Gamma(N)$ for which f/Δ^m lies in $K_G(X_G)$. For each $f \in M_{12m,G}$, the function $f/\Delta^m \in K_G(X_G)$ has no poles away from the cusps. One advantage of such functions is that they have a uniformly bounded number of poles; in fact, they have fewer than $mN^3/2$ total poles when counted with multiplicity.

Let W_m be the K_G-subspace of $M_{12m,G}$ consisting of modular forms f for which $f/\Delta^m \in K_G(X_G)$ is regular at each cusp $c \in \Sigma$. For a fixed $f \in W_m$, $\varphi := f/\Delta^m \in K_G(X_G)$ will have all its poles at cusps and will be regular at all $c \in \Sigma$. Since we want φ to be nonconstant, we will also want to choose f so that so that it does not lie in the 1-dimensional subspace $K_G\Delta^m$. By taking m sufficiently large, we will see from the Riemann–Roch theorem that $\dim_{K_G} W_m \geq 2$ and hence we can find a suitable f. This is the source of our functions φ in this paper.

However, to understand the growth of φ near the cusps of X_G, we need to have suitable explicit bounds on the coefficients of the q-expansion of f at each cusp. As a first step, we will find a basis of the vector space $M_{12m,G}$ for which the q-expansions at each cusp have coefficients in $\mathbb{Z}[\zeta_N]$ which can be explicitly bounded with respect to any absolute value of $\mathbb{Q}(\zeta_N)$. Our basis will be expressed in terms of Eisenstein series of weight 1 on $\Gamma(N)$. We then use a version of Siegel's lemma to show the existence of a modular form $f \in W_m - K_G\Delta^m$ with explicit bounds on the coefficients of the q-expansion at each cusp.

Let us give a brief overview of the sections of the paper. In §2, we give background on modular curves. In §3, we will show how around each cusp of X_G we can express rational functions analytically with respect to different places v. In §4, we state a theorem about the existence of a function $\varphi \in K(X_G)$ with the required properties. Assuming the existence of such a function φ, we then prove Theorem 1.1 in §5. The existence of the desired φ is proved in §10 after several sections on modular forms.

In §6, we give some background on modular forms. In particular, we define the vector spaces $M_{k,G}$ of modular forms in §6.3 and we give an explicit generating set for $M_{k,G}$ in terms of Eisenstein series in §6.5. Using this generating set, we prove in §7 the existence of a basis of $M_{k,G}$ whose q-expansions at each cusp have integral coefficients that can be bounded explicitly. In §8, we define the subspace W_m of $M_{12m,G}$ for each positive integer m and use the Riemann–Roch to show that $\dim_{K_G} W_m \geq 2$ for m large enough. For m large enough, we prove in §9 the existence of a modular form $f \in W_m - K_G\Delta^m$ so that its q-expansions at the cusps have integral coefficients that can be bounded explicitly.

1.2. **Notation.** Let ζ_N be the primitive N-th root of unity $e^{2\pi i/N}$ in $\mathbb{C}$. For each positive integer N, we define $q_N := e^{2\pi i\tau/N}$ which we view as a function in τ of the complex upper half-plane. When used with q-expansions, we will often view q_N as an indeterminate variable. For a positive divisor w of N, we have $q_N^{N/w} = q_w$. We set $q := q_1$.

For a field K, we define $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$, where $\overline{K}$ is a fixed algebraic closure of K. When $K \subseteq \mathbb{C}$, we will always take $\overline{K}$ to be the algebraic closure in $\mathbb{C}$.

Consider a number field L. We let M_L be the set of places of L. We let $M_{L,\infty} \subseteq M_L$ be the set of infinite places. Take any place v of L. We let L_v be the completion of L with respect to v. We let $|\cdot|_v$ be the corresponding absolute value on L_v normalized so that $|2|_v = 2$ if v is infinite and $|p|_v = p^{-1}$ if v induces the p-adic topology on $\mathbb{Q}$. For an algebraic closure $\overline{L}_v$ of L_v, the absolute value $|\cdot|_v$ uniquely extends to it. Define the integer $d_v = [L_v : \mathbb{Q}_v]$, where $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ in L_v. For any nonzero $a \in L$, we have the *product formula* $\prod_{v \in M_L} |a|_v^{d_v} = 1$.

Let C be a smooth projective and geometrically irreducible curve defined over a field K. For any point $c \in C(K)$, let $\mathrm{ord}_c \colon K(C) \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ be the discrete valuation whose valuation ring consists of the rational functions that are regular at c.

2. Background: modular curves

Fix a positive integer N and a group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The goal of this section is to give a quick definition of the modular curve X_G. While we could define X_G as a coarse moduli space, we will instead define it by explicitly giving its function field.

Let $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $d \mapsto \sigma_d$ be the group isomorphism for which $\sigma_d(\zeta_N) = \zeta_N^d$. We define $K_G = \mathbb{Q}(\zeta_N)^{\det(G)}$ to be the subfield of $\mathbb{Q}(\zeta_N)$ fixed by σ_d for all $d \in \det(G)$.

2.1. Modular functions.

The group $\mathrm{SL}_2(\mathbb{Z})$ acts by linear fractional transformations on the complex upper half-plane $\mathcal{H}$ and the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The quotient $\mathcal{X}_\Gamma := \Gamma\backslash\mathcal{H}^*$ is a smooth compact Riemann surface (away from the cusps and elliptic points, use the analytic structure coming from $\mathcal{H}$ and extend to the full quotient). Denote the field of meromorphic functions on $\mathcal{X}_\Gamma$ by $\mathbb{C}(\mathcal{X}_\Gamma)$.

Fix a positive integer N and let $\Gamma(N)$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ consisting of matrices that are congruent to the identity modulo N. Every $f \in \mathbb{C}(\mathcal{X}_{\Gamma(N)})$ gives rise to a meromorphic function on $\mathcal{H}$ that satisfies

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n(f) q_N^n$$

for all $\tau \in \mathcal{H}$ with sufficiently large imaginary component, where $q_N := e^{2\pi i\tau/N}$ and the $a_n(f)$ are unique complex numbers which are nonzero for only finitely many $n < 0$. This Laurent series in q_N is called the *q-expansion* of f (at the cusp at infinity) and it determines f uniquely. Let $\mathcal{F}_N$ be the subfield of $\mathbb{C}(\mathcal{X}_{\Gamma(N)})$ consisting of all meromorphic functions f for which $a_n(f)$ lies in $\mathbb{Q}(\zeta_N)$ for all $n \in \mathbb{Z}$. For example, $\mathcal{F}_1 = \mathbb{Q}(j)$, where j is the modular j-invariant.

We now describe a right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$. Note that the following two lemmas are both consequences of Theorem 6.6 and Proposition 6.9 of [Shi94].

Lemma 2.1. *There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathcal{F}_N$ such that the following hold for all $f \in \mathcal{F}_N$:*

- *For $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $(f * A)(\tau) = f(\gamma\tau)$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is any matrix congruent to A modulo N.*
- *For $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the q-expansion of $f * A$ is $\sum_{n\in\mathbb{Z}} \sigma_d(a_n(f)) q_N^n$.*

For each subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, let $\mathcal{F}_N^G$ be the subfield of $\mathcal{F}_N$ fixed by G under the action $*$ of Lemma 2.1.

Lemma 2.2.

(i) *The matrix $-I$ acts trivially on $\mathcal{F}_N$ and the right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ on $\mathcal{F}_N$ is faithful.*
(ii) *We have $\mathcal{F}_N^{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathcal{F}_1 = \mathbb{Q}(j)$ and $\mathcal{F}_N^{\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathbb{Q}(\zeta_N)(j)$.*
(iii) *The field $\mathbb{Q}(\zeta_N)$ is algebraically closed in $\mathcal{F}_N$.*

2.2. Modular curves.

Take any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. From Lemma 2.2, we find that the field $\mathcal{F}_N^G$ has transcendence degree 1 and that K_G is the algebraic closure of $\mathbb{Q}$ in $\mathcal{F}_N^G$. We define the *modular curve* X_G to be the smooth, projective and geometrically irreducible curve over K_G that has function field $\mathcal{F}_N^G$. We have $j \in \mathcal{F}_N^G = K_G(X_G)$ which gives a nonconstant morphism

$$j\colon X_G \to \mathbb{P}^1_{K_G}$$

whose degree we denote by μ.

Let $\overline{G}$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ generated by G and $-I$. Observe that $\mathcal{F}_N^G = \mathcal{F}_N^{\overline{G}}$ and hence $X_G = X_{\overline{G}}$. We have $\mu = [\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \overline{G} \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})]$.

Let Γ_G be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of those matrices whose image modulo N lies in $\overline{G} \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$; it contains $-I$. We have an inclusion $\mathbb{C} \cdot K_G(X_G) \subseteq \mathbb{C}(\mathcal{X}_{\Gamma_G})$ of fields that both have degree $\mu = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_G]$ over $\mathbb{C}(j)$. Therefore, $\mathbb{C}(\mathcal{X}_{\Gamma_G}) = \mathbb{C}(X_G)$. Using this equality of function fields, we shall identify $X_G(\mathbb{C})$ with the Riemann surface $\mathcal{X}_{\Gamma_G}$.

2.3. **Cusps.** Fix notation as in §2.2. Let $\mathcal{C}_G$ be the set of cusps of $\mathcal{X}_{\Gamma_G} = X_G(\mathbb{C})$. i.e., the set of orbits of Γ_G on $\mathbb{Q} \cup \{\infty\}$ or equivalently the points above ∞ under the morphism j. We have $\mathcal{C}_G \subseteq X_G(\mathbb{Q}(\zeta_N))$, see Lemma 2.3(ii).

Let c_∞ be the cusp at infinity, i.e., the orbit containing ∞. We have a bijection

$$\Gamma_G \backslash \operatorname{SL}_2(\mathbb{Z})/U \xrightarrow{\sim} \mathcal{C}_G, \quad \Gamma_G A U \mapsto A \cdot c_\infty,$$

where U is the group of upper triangular matrices in $\operatorname{SL}_2(\mathbb{Z})$ generated by $-I$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Since the level of Γ_G divides N, we find that the cusp $A \cdot c_\infty$ of X_G depends only on A modulo N. In particular, it makes sense to talk about the cusp $A \cdot c_\infty$ for any $A \in \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Now take any cusp $c \in \mathcal{C}_G$. We define w_c to be the ramification index of c over ∞ with respect to the morphism $j\colon X_G \to \mathbb{P}^1_{K_G}$. Equivalently, w_c is the width of the cusp c for the congruence subgroup Γ_G. The integer w_c divides N. Since μ is the degree of $j\colon X_G \to \mathbb{P}^1_{K_G}$, we have

$$\sum_{c \in \mathcal{C}_G} w_c = \mu. \tag{2.1}$$

Take any $A \in \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \cdot c_\infty = c$. Then for any $f \in \mathbb{C}(X_G)$, the q-expansion of $f * A \in \mathcal{F}_N$ is a Laurent series in the variable q_{w_c}.

2.4. **The modular curve $X(N)$.** Let $X(N)$ be the modular curve corresponding to the subgroup of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ consisting of matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$; it is a curve defined over $\mathbb{Q}$. The group $\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ has a left action on the curve $X(N)_{\mathbb{Q}(\zeta_N)}$ corresponding to the right action on the function field $\mathbb{Q}(\zeta_N)(X(N)) = \mathcal{F}_N$ given in Lemma 2.1.

Lemma 2.3.

(i) *The cusp c_∞ of $X(N)$ is defined over $\mathbb{Q}$.*

(ii) *For any subgroup G of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $\mathcal{C}_G \subseteq X_G(\mathbb{Q}(\zeta_N))$. The set $\mathcal{C}_G$ is stable under the action of $\operatorname{Gal}(\mathbb{Q}(\zeta_N)/K_G)$.*

Proof. Let $\mathcal{C}$ be the set of cusps of in $X(N)(\mathbb{C})$. From [Zyw24, Lemma 5.2], we find that $\mathcal{C} \subseteq X(N)(\mathbb{Q}(\zeta_N))$ and that c_∞ is defined over $\mathbb{Q}$. Take any subgroup $G \subseteq \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and let $\pi\colon X(N)_{\mathbb{Q}(\zeta_N)} \to (X_G)_{\mathbb{Q}(\zeta_N)}$ be the morphism corresponding to the inclusion $\mathbb{Q}(\zeta_N)(X_G) \subseteq \mathcal{F}_N = \mathbb{Q}(\zeta_N)(X(N))$ of function fields. We have $\pi(\mathcal{C}) = \mathcal{C}_G$. Therefore, $\mathcal{C}_G \subseteq \pi(X(N)(\mathbb{Q}(\zeta_N)) \subseteq X_G(\mathbb{Q}(\zeta_N))$, where the last equality uses that π is defined over $\mathbb{Q}(\zeta_N)$. Since $j\colon X_G \to \mathbb{P}^1_{K_G}$ is defined over K_G, the set $j^{-1}(\infty) = \mathcal{C}_G \subseteq X_G(\mathbb{Q}(\zeta_N))$ is stable under the action of $\operatorname{Gal}(\mathbb{Q}(\zeta_N)/K_G)$. ☐

Remark 2.4. Suppose that $N > 2$. The modular curve $X(N)_{\mathbb{Q}(\zeta_N)}$ has an alternate description as a fine moduli space. We refer to Deligne and Rapoport [DR73] where this theory is fully developed. They define a smooth projective curve M_N over $\mathbb{Q}(\zeta_N)$ that is the moduli space for generalized elliptic curves with a level N structure (we use $N > 2$ to ensure the moduli problem is represented by a scheme and we have also base extended to $\mathbb{Q}(\zeta_N)$ from the ring $\mathbb{Z}[1/N, \zeta_N]$). The curve M_N has $\phi(N)$ irreducible components. Our curve $X(N)_{\mathbb{Q}(\zeta_N)}$ can be identified with an irreducible C component of M_N (in particular, the irreducible component consisting of generalized elliptic curves with a level N structure so that the Weil pairing of the basis is ζ_N). To prove this identification one need only identify the function field of C with $\mathcal{F}_N = \mathbb{Q}(\zeta_N)(X(N))$; thus can be done using the material in [DR73, Chapter VII, §4] which compares modular forms with the classical theory.

For every $f \in \mathbb{Q}(X(N))$, its q-expansion (at c_∞) lies in $\mathbb{Q}(\!(q_N)\!)$ and it lies in $\mathbb{Q}[\![q_N]\!]$ when f is regular at c_∞. So with $\mathcal{O}$ the local ring of rational functions on $X(N)$ that are regular at c_∞, q-expansions induces an isomorphism between the completion of $\mathcal{O}$ with $\mathbb{Q}[\![q_N]\!]$. Equivalently, q-expansions induces an isomorphism between the formal completion of the curve $X(N)$ along c_∞ with the formal spectrum of $\mathbb{Q}[\![q_N]\!]$.

Now consider *any* field $F \supseteq \mathbb{Q}$. If $\mathcal{O}$ is the local ring of rational functions on $X(N)_F$ that are regular at c_∞, then we obtain an isomorphism between the completion of $\mathcal{O}$ with $F[\![q_N]\!]$. So for any $f \in F(X(N)_F) = F(X(N))$, we obtain a q-expansion in $F(\!(q_N)\!)$ that lies in $F[\![q_N]\!]$ when f is regular at c_∞.

Consider any field $F \supseteq \mathbb{Q}(\zeta_N)$. The group $\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(N)_F$ and hence acts on $F(X(N))$. The field $F(X(N))$ is the compositum of F and $\mathcal{F}_N$. The group $\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the field $F(X(N))$ as the identity on F and as our action $*$ on $\mathcal{F}_N$; we also denote this action by $*$.

3. Analytic expansions at the cusps

Fix an integer $N > 2$. Fix a number field $L \supseteq \mathbb{Q}(\zeta_N)$ and a place v of L.

Take any cusp c of $X(N)$ and choose an $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \cdot c_\infty = c$. Consider a rational function f in $\overline{L}_v(X(N))$. As noted in §2.4, $f * A$ has a q-expansion in $\overline{L}_v(\!(q_N)\!)$ that we denote by $\sum_{n\in\mathbb{Z}} a_n(f*A) q_N^n$. We will show that for all points in $X(N)(\overline{L}_v)$ near c, but maybe not equal to c, the function f can be expressed analytically in terms of the Laurent series of the the q-expansion of $f * A$. In order to make this precise, we will define a subset $\Omega_{c,v} \subseteq X(N)(\overline{L}_v)$ that only contains the one cusp c and whose interior is an open neighborhood of c.

For a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we will also define similar subsets $\Omega_{c,v}$ of $X_G(\overline{L}_v)$ in §3.2.

3.1. **The modular curve $X(N)$.** As noted in §2.4, the group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(N)_F$ and $F(X(N))$ for any field $F \supseteq \mathbb{Q}(\zeta_N)$. For each $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, let ι_A be the corresponding automorphism of $X(N)_{\mathbb{Q}(\zeta_N)}$. For any place v of L, ι_A gives a homeomorphism $X(N)(\overline{L}_v) \xrightarrow{\sim} X(N)(\overline{L}_v)$. Define the open ball $B_v := \{a \in \overline{L}_v : |a|_v < 1\}$ of $\overline{L}_v$.

Proposition 3.1. *Fix a place v of L. Take a matrix $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and define the cusp $c := A \cdot c_\infty$ of $X(N)$. Then there is a unique continuous map*

$$\psi_{A,v} \colon B_v \to X(N)(\overline{L}_v)$$

such that the following hold:

(a) *Take any rational function $f \in \overline{L}_v(X(N))$ and let r be the radius of convergence of the power series $\sum_{n=0}^{\infty} a_n(f*A)x^n$ in $\overline{L}_v[\![x]\!]$. Then for all nonzero $t \in B_v$ with $|t|_v < r$, we have*

$$f(\psi_{A,v}(t)) = \sum_{n\in\mathbb{Z}} a_n(f*A)t^n$$

in $\overline{L}_v$.

(b) *We have $\psi_{A,v}(0) = c$. For any nonzero $t \in B_v$, $\psi_{A,v}(t)$ is not a cusp and*

$$j(\psi_{A,v}(t)) = J(t^N)$$

in $\overline{L}_v$, where $J(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \in \mathbb{Z}(\!(q)\!)$ is the q-expansion of j. When v is finite, we have $|j(\psi_{A,v}(t))|_v = |t|_v^{-N} > 1$ for all nonzero $t \in B_v$.

We have $\psi_{A,v} = \iota_A \circ \psi_{I,v}$.

Proof. We first assume that there is a unique continuous map $\psi_{I,v} \colon B_v \to X(N)(\overline{L}_v)$ satisfying (a) and (b). Define the continuous map $\psi_{A,v} := \iota_A \circ \psi_{I,v} \colon B_v \to X(N)(\overline{L}_v)$. We have $\psi_{A,v}(0) = \iota_A(\psi_{I,v}(0)) = \iota_A(c_\infty) = A \cdot c_\infty = c$. Take any $f \in \overline{L}_v(X(N))$. We have $f * A \in \overline{L}_v(X(N))$. Let r be the radius of convergence of $\sum_{n=0}^{\infty} a_n(f*A)x^n \in \overline{L}_v[\![x]\!]$. For any nonzero $t \in B_v$ with $|t|_v < r$, we have

$$f(\psi_{A,v}(t)) = f(\iota_A(\psi_{I,v}(t)) = (f*A)(\psi_{I,v}(t)) = \sum_{n\in\mathbb{Z}} a_n(f*A)t^n \in \overline{L}_v,$$

where the last equality uses our assumption that $\psi_{I,v}$ exists with the expected properties. For any nonzero $t \in B_v$, we also have $j(\psi_{A,v}(t)) = j(\iota_A(\psi_{I,v}(t))) = (j*A)(\psi_{I,v}(t)) = j(\psi_{I,v}(t))$. So (b) holds for $\psi_{A,v}$ by the corresponding property that we have assumed holds for $\psi_{I,v}$. Therefore, $\psi_{A,v}$ satisfies (a) and (b).

We now show that $\psi_{A,v}$ is unique. A similar argument as above shows that for any continuous $\psi_{A,v}$ satisfying (a) and (b), the map $\iota_A^{-1} \circ \psi_{A,v} \colon B_v \to X(N)(\overline{L}_v)$ is continuous and satisfies the same properties (a) and (b) as $\psi_{I,v}$. By our assumption that $\psi_{I,v}$ is unique, we deduce that $\psi_{I,v} = \iota_A^{-1} \circ \psi_{A,v}$. This proves the uniqueness of $\psi_{A,v}$ and that $\psi_{A,v} = \iota_A \circ \psi_{I,v}$.

So without loss of generality, we may assume that $A = I$ and hence $c = c_\infty$.

Before starting the case where v is infinite, let us recall the classic situation over $\mathbb{C}$. Define $B := \{t \in \mathbb{C} : |t| < 1\}$. Let

$$\pi \colon \mathcal{H} \cup \{\infty\} \to \Gamma(N)\backslash\mathcal{H}^* = \mathcal{X}_{\Gamma(N)} = X(N)(\mathbb{C})$$

be the natural quotient map with the last equality being the identification from §2.2. The map π can be expressed as the composition of $\mathcal{H} \cup \{\infty\} \twoheadrightarrow B$, $\tau \mapsto e^{2\pi i\tau/N}$ (where $\infty \mapsto 0$) with a unique function

$\psi\colon B \to X(N)(\mathbb{C})$. The map ψ is continuous and its image is all of $X(N)(\mathbb{C})$ except for those cusps that are not c_∞. We have $\psi(0) = c_\infty$ and $\psi(t)$ is not a cusp for all nonzero $t \in B$. Take any $f \in \mathbb{C}(X(N)) = \mathbb{C}(\mathcal{X}_{\Gamma(N)})$ that is regular at c_∞. Let $\sum_{n\in\mathbb{Z}} a_n(f) q_N^n \in \mathbb{C}(\!(q_N)\!)$ be the q-expansion of f and let r be its radius of convergence of $\sum_{n=0}^{\infty} a_n(f) x^n \in \mathbb{C}[\![x]\!]$. Take any nonzero $t \in B$ with $|t| < r$ and choose a $\tau \in \mathcal{H}$ for which $t = e^{2\pi i \tau/N}$. We have

$$f(\psi(t)) = (f \circ \pi)(\tau) = \sum_{n\in\mathbb{Z}} a_n(f) e^{2\pi i \tau n/N} = \sum_{n\in\mathbb{Z}} a_n(f) t^n.$$

In the special case $f = j$, we have a q-expansion $J(q) = q^{-1} + 744 + \cdots \in \mathbb{Z}[\![q]\!]$ and hence $j(\psi(t)) = J(t^N)$ for all nonzero $t \in B_v$.

We now consider the case where v is infinite. Fix an embedding $\sigma\colon L \hookrightarrow \mathbb{C}$ that satisfies $|a|_v = |\sigma(a)|$ for all $a \in L$. By continuity, σ extends uniquely to an isomorphism $\bar{\sigma}\colon \bar{L}_v = L_v \xrightarrow{\sim} \mathbb{C}$ of fields that respects absolute values (the field L_v is not real since it contains ζ_N with $N > 2$). Since $X(N)$ and the cusp c_∞ are defined over $\mathbb{Q}$, $\bar{\sigma}$ induces a homeomorphism $\bar{\sigma}_*\colon X(N)(\bar{L}_v) \xrightarrow{\sim} X(N)(\mathbb{C})$ that maps c_∞ to itself. Define the continuous function

$$\psi_{I,v}\colon B_v \xrightarrow{\sim} B \xrightarrow{\psi} X(N)(\mathbb{C}) \xrightarrow{\sim} X(N)(\bar{L}_v),$$

where the first map is given by $\bar{\sigma}$ and the third map is the inverse of $\bar{\sigma}_*$. The image of $\psi_{I,v}$ is equal to $X(N)(\bar{L}_v)$ with all the cusps except c_∞ removed since ψ has this property. The desired properties for $\psi_{I,v}$ are now immediate consequences of the analogous properties of ψ.

The process of q-expansions induces an isomorphism between the formal completion of the curve $X(N)_{\mathbb{Q}(\zeta_N)}$ along c_∞ with the formal spectrum of $\mathbb{Q}(\zeta_N)[\![q_N]\!]$. We will require a stronger version of Deligne and Rapoport that we now recall. Define the ring $R := (\mathbb{Z}[\zeta_N][\![q_N]\!]) \otimes_{\mathbb{Z}[\zeta_N]} \mathbb{Q}(\zeta_N)$; we can view it as a subring of $\mathbb{Q}(\zeta_N)[\![q_N]\!]$. From Deligne and Rapoport [DR73, Chapter VII, Corollary 2.4] with Remark 2.4, the Tate curve produces a morphism

$$\operatorname{Spec} R \to X(N)_{\mathbb{Q}(\zeta_N)} \tag{3.1}$$

that induces an isomorphism between the formal completion of $X(N)_{\mathbb{Q}(\zeta_N)}$ along c_∞ and the formal spectrum of $\mathbb{Q}(\zeta_N)[\![q_N]\!]$.

We now consider a finite place v of L. Define the $\bar{L}_v$-algebra $R' := R \otimes_{\mathbb{Q}(\zeta_N)} \bar{L}_v$. Take any $t \in B_v$. Evaluating the power series in $R' \subseteq \bar{L}_v[\![q_n]\!]$ at t gives a homomorphism $\phi_t\colon R' \to \bar{L}_v$ of $\bar{L}_v$-algebras. Composing $\phi_t^*\colon \operatorname{Spec} \bar{L}_v \to \operatorname{Spec} R'$ with the morphism $\operatorname{Spec} R' \to X(N)_{\bar{L}_v}$ obtained from base changing (3.1) produces a point $\psi_{I,v}(t)$ in $X(N)(\bar{L}_v)$. We thus have defined a map

$$\psi_{I,v}\colon B_v \to X(N)(\bar{L}_v)$$

and it is continuous. Note that $\psi_{I,v}(0) = c$.

Take any $t \in B_v$ and let R_t be the subring of $\bar{L}_v[\![q_N]\!]$ consisting of those series whose radius of convergence is strictly greater than $|t|_v$. By base changing (3.1) by $\bar{L}_v$ and using the inclusion $R' \subseteq R_t$, we obtain a morphism $\operatorname{Spec} R_t \to X(N)_{\bar{L}_v}$ that induces an isomorphism between the formal completion of $X(N)_{\bar{L}_v}$ at c_∞ and the formal spectrum of the power series ring $\bar{L}_v[\![q_N]\!]$. Evaluating power series in R_t at t induces a morphism $\operatorname{Spec} \bar{L}_v \to \operatorname{Spec} R_t$ which after composing with $\operatorname{Spec} R_t \to X(N)_{\bar{L}_v}$ gives the $\bar{L}_v$-point $\psi_{I,v}(t)$. So for any rational function $f \in \bar{L}_v(X(N))$ regular at c_∞ for which $\sum_{n=0}^{\infty} a_n(f) q_N^n \in \bar{L}_v[\![x]\!]$ lies in R_t, we have $f(\psi_{I,v}(t)) = \sum_{n=0}^{\infty} a_n(f) t^n$.

The function j^{-1} is regular at c_∞ and its q-expansion is $h(q) := J(q)^{-1} = q - 744q^2 + \cdots \in \mathbb{Z}[\![q]\!] \subseteq R$. Take any nonzero $t \in B_v$. We have $j^{-1}(\psi_{I,v}(t)) = t^N - 744t^{2N} + \cdots = h(t^N)$ in $\bar{L}_v$. Since $|t|_v < 1$, this series implies that $|j^{-1}(\psi_{I,v}(t))|_v = |t|_v^N$. In particular, $j^{-1}(\psi_{I,v}(t))$ is nonzero since t is nonzero. Therefore, $\psi_{I,v}(t)$ is not a cusp and $j(\psi_{I,v}(t)) = h(t^N)^{-1} = J(t^N)$. We have also shown that $|j(\psi_{I,v}(t))|_v = |t|_v^{-N} > 1$.

We have now shown that $\psi_{I,v}\colon B_v \to X(N)(\bar{L}_v)$ satisfies (b). It also satisfies (a) since we have shown that (a) holds for $f \in \bar{L}_v(x(N))$ regular at c_∞ and for j (for any $f \in \bar{L}_v(X(N))$, there is an integer m for which $f \cdot j^m$ is regular at c).

Finally, it remains to prove the uniqueness of $\psi_{I,v}$; we have already proved the existence. For $\tau \in \mathcal{H}$, let $\wp(z;\tau)$ be the Weierstrass elliptic function for the lattice $\mathbb{Z}\tau + \mathbb{Z} \subseteq \mathbb{C}$. For integers $0 \le r, s < N$ that are not both zero, define the function $x_{(r,s)}(\tau) := 36E_4(\tau)E_6(\tau)\Delta(\tau)^{-1}\cdot(2\pi i)^{-2}\wp(\frac{r}{N}\cdot\tau+\frac{s}{N};\tau)$, where E_4 and E_6 are the usual Eisenstein series of weight 4 and 6, respectively, on $\mathrm{SL}_2(\mathbb{Z})$. The function $x_{(r,s)}$ lies in $\mathcal{F}_N$ with cusps only at the poles, see [Zyw24, Lemma 6.1]. The q-expansion of $12\cdot(2\pi i)^{-2}\wp(\frac{r}{N}\cdot\tau+\frac{s}{N};\tau)$ is of the form $\sum_{n=0}^{\infty} a_n q_N^n$ with $a_n\in\mathbb{Z}[\zeta_N]$ and $|a_n|_v \ll n$ for $n\geq 1$, see the proof of [Zyw24, Lemma 6.1] for the explicit q-expansion. From this, we deduce that the q-expansion of each $x_{(r,s)}$ will have coefficients in $\mathbb{Q}(\zeta_N)\subseteq L$ and will have radius of convergence at least 1 when viewed as having coefficients in $\overline{L}_v$. In particular, the value $x_{(r,s)}(\psi_{I,v}(t))$ depends only on t by (a) (and not the choice of $\psi_{I,v}$). By (b), $j(\psi_{I,v}(t))$ also depends only on t. However, the functions $x_{(r,s)}$ along with j generate the field $\mathcal{F}_N$, cf. [Zyw24, Lemma 6.1], and hence also generate $\overline{L}_v(X(N))$ over $\overline{L}_v$. This implies that $\psi_{I,v}(t)$ does not depend on the choice of $\psi_{I,v}$. ☐

Let $\mathcal{C}$ be the set of cusps of $X(N)$; it is a subset of $X(N)(L)$ by Lemma 2.3(ii). Take any cusp $c\in\mathcal{C}$ and any place v of L. Choose an $A\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A\cdot c_\infty = c$. With $\psi_{A,v}$ as in Proposition 3.1, define the following subset of $X(N)(\overline{L}_v)$:

$$\Omega_{c,v} := \begin{cases}\psi_{A,v}(B_v) & \text{if } v \text{ is finite,}\\ \psi_{A,v}(\{t\in\overline{L}_v : |t|_v \leq e^{-\pi\sqrt{3}/N}\}) & \text{if } v \text{ is infinite.}\end{cases}$$

The only cusp in the set $\Omega_{c,v}$ is c.

Lemma 3.2. *Take any place v of L.*

(i) *For each cusp $c\in\mathcal{C}$, $\Omega_{c,v}$ does not depend on the choice of $A\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A\cdot c_\infty = c$.*
(ii) *If v is finite, then $\bigcup_{c\in\mathcal{C}}\Omega_{c,v} = \{P\in X(N)(\overline{L}_v) : P$ a cusp or $|j(P)|_v > 1\}$.*
(iii) *If v is infinite, then $\bigcup_{c\in\mathcal{C}}\Omega_{c,v} = X(N)(\overline{L}_v)$.*

Proof. Consider any integer b. We have $e^{2\pi i(\tau+b)/N} = \zeta_N^b q_N$. So for a matrix $U = \pm\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and a function $f\in\mathcal{F}_N$, the q-expansion of $f*U$ is $\sum_{n\in\mathbb{Z}} a_n(f*U)q_N^n = \sum_{n\in\mathbb{Z}} a_n(f)\zeta_N^{bn}q_N^n$. The same thing thus holds for the q-expansion of $f*U$ for any $f\in\overline{L}_v(X(N))$.

Take any matrices $A, A'\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A\cdot c_\infty = A'\cdot c_\infty$. We have $A = A'\cdot U$ for some matrix U of the form $\pm\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)$. For any $f\in\overline{L}_v(X(N))$, the q-expansion of $f*A$ is $\sum_{n\in\mathbb{Z}} a_n(f*A)q_N^n = \sum_{n\in\mathbb{Z}} a_n((f*A')*U)q_N^n = \sum_{n\in\mathbb{Z}} a_n(f*A')\zeta_N^{bn}q_N^n$. From the uniqueness of $\psi_{A,v}$ in Proposition 3.1, we deduce that $\psi_{A,v}(t) = \psi_{A',v}(\zeta_N^b t)$ for all $t\in B_v$. Part (i) follows immediately since $|\zeta_N^b|_v = 1$.

Since $\psi_{A,v} = \iota_A\circ\psi_{I,v}$ by Proposition 3.1, we find that $\mathcal{S} := \bigcup_{c\in\mathcal{C}}\Omega_{c,v}$ is equal to the set

$$\bigcup_{A\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})}\iota_A(\Omega_{c_\infty,v}).$$

In particular, $\mathcal{S}\subseteq X(N)(\overline{L}_v)$ is stable under the action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts transitively on the fibers of $j\colon X(N)(\overline{L}_v)\to\mathbb{P}^1(\overline{L}_v)$, we have

$$\mathcal{S} = \{P\in X(N)(\overline{L}_v) : j(P)\in j(\mathcal{S})\}. \tag{3.2}$$

Since $\mathcal{S}$ contains all the cusps $\mathcal{C}$, we need only compute the set $j(\mathcal{S}-\mathcal{C})\subseteq\overline{L}_v$ to prove (ii) and (iii).

First suppose that v is finite. We have $j(\mathcal{S}-\mathcal{C})\subseteq\{a\in\overline{L}_v : |a|_v>1\}$ by Proposition 3.1(b). Now take any $a\in\overline{L}_v$ with $|a|_v>1$. By [Sil94, Chapter V Lemma 5.1], there is a nonzero $t\in\overline{L}_v$ with $|t|_v<1$ such that $a = J(t^N)$ with J as in Proposition 3.1(b). By Proposition 3.1(b), we have $a = J(t^N) = j(\psi_{I,v}(t))\in j(\mathcal{S}-\mathcal{C})$. Therefore, $j(\mathcal{S}-\mathcal{C}) = \{a\in\overline{L}_v : |a|_v>1\}$ and hence we obtain (ii) from (3.2).

Finally suppose that v is infinite. Using (3.2), we need only verify that $j(\mathcal{S}-\mathcal{C}) = \overline{L}_v$ to prove part (iii). We have

$$j(\mathcal{S}-\mathcal{C}) = \bigcup_{c\in\mathcal{C}} j(\Omega_{c,v}-\{c\}) = \{J(t^N) : t\in\overline{L}_v-\{0\}, |t|_v\leq e^{-\pi\sqrt{3}/N}\},$$

where the last equality uses the definition of $\Omega_{c,v}$ and Proposition 3.1(b). So after choosing an isomorphism $\overline{L}_v\cong\mathbb{C}$ that respects absolute values, we need only show that every $a\in\mathbb{C}$ is of the form $J(t^N)$ for some nonzero $t\in\mathbb{C}$ with $|t|\leq e^{-\pi\sqrt{3}/N}$. Take any $a\in\mathbb{C}$. There is a $\tau\in\mathcal{H}$ for which $j(\tau)=a$, where we are viewing j as a holomorphic function of the upper half-plane. Using the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$, we may further assume that $|\tau|\geq 1$ and $-1/2\leq\mathrm{Re}(\tau)\leq 1/2$. In particular, $\mathrm{Im}(\tau)\geq\sqrt{3}/2$. Define

$u = e^{2\pi i\tau} \in \mathbb{C}$. We have $0 < |u| \leq e^{-\pi\sqrt{3}}$. Choose a $t \in \mathbb{C}$ for which $u = t^N$. We have $0 < |t| \leq e^{-\pi\sqrt{3}/N}$ and $J(t^N) = J(u) = j(\tau) = a$. □

Remark 3.3. Consider the cusp $c := c_\infty$. The approach in §3 of [BP11] is to view $t_c := q_N$ as a parameter on $X(N)$ that defines a v-analytic function on a neighborhood of c in $X(N)(\overline{L}_v)$ that maps c to 0. They describe an open neighborhood of c for which their function is defined and analytic; locally it is a homeomorphism whose inverse will agree with the restriction of our function $\psi_{I,v}$. Bilu and Parent take a similar approach for any cusp of a general modular curve X_G. In the setting of this section, our set $\Omega_{c,v}$ will agree with that in §3 of [BP11] when v is finite (our sets are larger when v is infinite).

3.2. **The sets $\Omega_{c,v}$ for a general modular curve.** Take any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The modular curve X_G is defined over $K_G \subseteq \mathbb{Q}(\zeta_N) \subseteq L$. Let $\pi\colon X(N)_{\mathbb{Q}(\zeta_N)} \to (X_G)_{\mathbb{Q}(\zeta_N)}$ be the natural morphism corresponding to the inclusion of function fields $\mathbb{Q}(\zeta_N)(X_G) \subseteq \mathcal{F}_N$. Let $\mathcal{C}$ be the set of cusps in $X(N)(\mathbb{Q}(\zeta_N))$.

Fix a place v of L. For each cusp $c \in \mathcal{C}_G$, we define the subset

$$\Omega_{c,v} := \pi\Big(\bigcup_{c' \in \mathcal{C}\ \pi(c')=c} \Omega_{c',v}\Big)$$

of $X_G(\overline{L}_v)$, where the sets $\Omega_{c',v} \subseteq X(N)(\overline{L}_v)$ are from §3.1. The set $\Omega_{c,v}$ contains c and no other cusps.

Lemma 3.4. *For any place v of L, we have*

$$\bigcup_{c\in\mathcal{C}_G} \Omega_{c,v} = \begin{cases} \{P \in X_G(\overline{L}_v) : P \text{ is a cusp or } |j(P)|_v > 1\} & \text{if } v \text{ is finite,} \\ X_G(\overline{L}_v) & \text{if } v \text{ is infinite.} \end{cases}$$

Proof. We have $\bigcup_{c\in\mathcal{C}_G} \Omega_{c,v} = \pi(\bigcup_{c'\in\mathcal{C}} \Omega_{c',v})$. The lemma now follows from Lemma 3.2. □

4. Properties of φ

Fix an integer $N > 2$ and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. Let μ be the degree of the morphism $j\colon X_G \to \mathbb{P}^1_{K_G}$. The group Gal_{K_G} acts on the set of cusps $\mathcal{C}_G$ of X_G by Lemma 2.3(ii).

Let Σ be a proper subset of $\mathcal{C}_G$ that is stable under the Gal_{K_G}-action. Let m be the smallest positive integer for which $m\sum_{c\in\mathcal{C}_G-\Sigma} w_c > g$, where g is the genus of X_G. Fix a number field $L \supseteq \mathbb{Q}(\zeta_N)$. Define the real numbers

$$\beta := 2(2^3 4.5^{36m} N^{108m+15} m^{72m+1})^{m\mu+1} 4.5^{12m} N^{36m+4},$$

$C := 96.6 \cdot 0.1^{24m} N^{90m+4}$ and $C' := 22.16 N^{144m+7} 0.024^{24m}$.

The following theorem gives the existence of a rational function $\varphi \in K_G(X_G)$ suitable for our application of Runge's method; it makes use of the sets $\Omega_{c,v} \subseteq X_G(\overline{L}_v)$ from §3.2. The proof will given in §10 after several sections discussing modular forms.

Theorem 4.1. *Fix notation and assumptions as above. There is a nonconstant function $\varphi \in K_G(X_G)$ that satisfies the following properties:*

(a) *The function φ is integral over $\mathbb{Z}[j]$, i.e., φ is the root of a monic polynomial with coefficients in $\mathbb{Z}[j]$.*
(b) *The function φ has no poles away from the cusps of X_G.*
(c) *Take any cusp $c \in \Sigma$. The function φ is regular at c. Moreover, $\varphi(c)$ lies in $\mathbb{Z}[\zeta_N]$ and satisfies $|\varphi(c)|_v \leq \beta m^{24m}$ for all infinite places v of L.*
(d) *For any cusp $c \in \Sigma$, place v of L and point $P \in \Omega_{c,v} - \{c\}$, we have*

$$|\varphi(P) - \varphi(c)|_v \leq \begin{cases} |j(P)|_v^{-1/w_c} & \text{if } v \text{ is finite,} \\ |j(P)|_v^{-1/w_c} \cdot \beta C & \text{if } v \text{ is infinite and } |j(P)|_v > 3500, \\ \beta C/2 & \text{if } v \text{ is infinite.} \end{cases}$$

(e) *Let K be any number field with $K_G \subseteq K \subseteq L$ and let Σ' be a Gal_K-orbit of Σ. Let w be the integer for which $w_c = w$ for all $c \in \Sigma'$. Then there is a nonzero $\xi \in \mathcal{O}_K$ such that the following hold:*
   - *We have $|\xi|_v \leq (\beta C')^{w|\Sigma'|}$ for all infinite place v of L.*

- *Consider any point $P \in Y_G(K)$ for which $\varphi(P) = \varphi(c)$ and $P \in \Omega_{c,v}$ for some cusp $c \in \Sigma'$ and place v of L. Then*

$$|\xi|_v \le \begin{cases} |j(P)|_v^{-w} & \text{if } v \text{ is finite,} \\ |j(P)|_v^{-w} \cdot (\beta C')^{w|\Sigma'|} & \text{if } v \text{ is infinite and } |j(P)|_v > 3500. \end{cases}$$

For later use, we now gives some simple bounds on m and μ in terms of N.

Lemma 4.2. *Fix notation as above.*

(i) *We have $\mu \le \frac{1}{2}N^3$, $\mu + 1 \le \frac{29}{54}N^3$ and $\mu + 2 \le \frac{31}{54}N^3$.*

(ii) *We have $m \le \frac{1}{24}N^3$.*

Proof. Since G contains $-I$, we have $\mu = [\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap G]$. In particular, μ is a divisor of $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}|$ and thus $\mu \le N^3/2$. Take any nonnegative real numbers b. From our bound on μ and $N \ge 3$, we have $\mu + b \le (1/2 + b/27)N^3$. Part (i) is obtained by taking specific values of b.

We now bound m. We have $m \le g+1$ since $\sum_{c\in\mathcal{C}_G-\Sigma} w_c \ge 1$. For every congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of level at most 5, $\mathcal{X}_\Gamma$ has genus 0, see [CP03]. So if $N \le 5$, then $g = 0$ and hence $m = 1$; the bound $m \le \frac{1}{24}N^3$ is immediate since $N \ge 3$. We can now assume that $N \ge 6$. By [Shi94, Proposition 1.40], we have $g + 1 \le \mu/12 + 3/2$, where we have used that X_G has at least one cusp. If μ is a proper divisor of $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}|$, then $\mu \le N^3/4$ and hence

$$m \le g + 1 \le \tfrac{1}{48}N^3 + \tfrac{3}{2} \le \tfrac{1}{48}N^3 + \tfrac{3}{2\cdot 6^3}N^3 \le \tfrac{1}{24}N^3.$$

Finally assume that $\mu = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}|$ and hence $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. In this case, we have $g = 1 + \mu(N-6)/(12N)$, cf. [Shi94, Equation (1.6.4)]. Therefore,

$$m \le g + 1 \le 2 + \tfrac{1}{2}N^3\tfrac{N-6}{12N} \le \tfrac{1}{24}N^3 - \tfrac{1}{4}N^2 + 2 \le \tfrac{1}{24}N^3. \qquad \square$$

5. Proof of Theorem 1.1

Take any point P in $Y_G(K)$ with $j(P) \in \mathcal{O}_{K,S}$. Let S' be the set of places v of K for which v is infinite or $|j(P)|_v > 1$. We have $j(P) \in \mathcal{O}_{K,S'}$ and $|S'| \le |S| < \mathfrak{c}_{G,K}$. So without loss of generality, we may assume that $S = S'$, i.e., a finite place v of K lies in S if and only if $|j(P)|_v > 1$.

We have $K_G \subseteq \mathbb{Q}(\zeta_N) \subseteq \mathbb{C}$. Without loss of generality, we may assume that $K_G \subseteq K \subseteq \mathbb{C}$. Let $\overline{K}$ be the algebraic closure of K in $\mathbb{C}$ and define $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$. Define the field $L := K(\zeta_N)$. Let $\mathcal{C}_G$ be the set of cusps in $X_G(\mathbb{C})$; we have $\mathcal{C}_G \subseteq X_G(L)$ by Lemma 2.3(ii).

Take any $v \in S$; it is a place of K. We choose a place of L that extends v which, by abuse of notation, we also denote by v. This choice of place of L will ultimately not matter since we are interested in $|j(P)|_v$ which does not depend on the choice of extension since $j(P) \in K$. As in §3, we define a subset $\Omega_{c,v} \subseteq X_G(\bar{L}_v)$ for each cusp $c \in \mathcal{C}_G$. By Lemma 3.4, there is a cusp $c_v \in \mathcal{C}_G$ for which P lies in $\Omega_{c_v,v}$. Intuitively, c_v is a cusp that is "nearby" P in $X_G(\bar{L}_v)$.

Let Σ be the minimal subset of $\mathcal{C}_G$ that contains $\{c_v : v \in S\}$ and is stable under the Gal_K-action. The action of Gal_K on Σ clearly has at most $|S|$ orbits. We have $|S| < \mathfrak{c}_{G,K}$ by assumption and hence Σ is a proper subset of $\mathcal{C}_G$. The set Σ is nonempty since S is nonempty.

Let m be the smallest positive integer for which $m\sum_{c\in\mathcal{C}_G-\Sigma} w_c > g$, where g is the genus of X_G. Let $\varphi \in K_G(X_G) \subseteq K(X_G)$ be a nonconstant function satisfying all the properties of Theorem 4.1 with respect to the set Σ and the field L.

Let $\Sigma_1, \ldots, \Sigma_h$ be the Gal_K-orbits of Σ. For each $1 \le i \le h$, the values w_c agree as we vary over all $c \in \Sigma_i$; we denote this common integer by w_i.

We now fix an integer $1 \le i \le h$. Let S_i be the set of places $v \in S$ such that $c_v \in \Sigma_i$ and such that $|j(P)|_v > 3500$ if v is infinite. Our goal is to find an upper bound for $\sum_{v\in S_i} d_v \log|j(P)|_v$, where the integers d_v are defined in §1.2. Once this is done we will combine these bounds for all i to obtain an upper bound for $h(j(P))$.

The function φ is regular at all $c \in \Sigma_i$ by Theorem 4.1(c). Define the function

$$g_i := \prod_{c\in\Sigma_i} (\varphi - \varphi(c)).$$

We now give some basic properties of g_i.

Lemma 5.1.

(i) *The rational function g_i lies in $K(X_G)$ and any pole of g_i is a cusp of X_G that does not lie in the set Σ.*

(ii) *We have $g_i(c) = 0$ for all $c \in \Sigma_i$.*

(iii) *We have $\varphi(P) \in \mathcal{O}_{K,S}$ and $g_i(P) \in \mathcal{O}_{K,S}$.*

Proof. For any $\sigma \in \mathrm{Gal}_K$ and $c \in \Sigma_i$, we have $\sigma(\varphi(c)) = \varphi(\sigma(c))$ since $\varphi \in K(X_G)$. Since Σ_i is stable under the Gal_K-action, the polynomial $Q_i(x) := \prod_{c\in\Sigma_i}(x - \varphi(c))$ lies in $K[x]$. Moreover, $Q_i(x) \in \mathcal{O}_K[x]$ since $\varphi(c)$ is algebraic for all $c \in \Sigma$ by Theorem 4.1(c). Therefore, $g_i = Q_i(\varphi)$ is an element of $K(X_G)$. Since $g_i = Q_i(\varphi)$, any pole of g_i will also be a pole of φ. Part (i) thus follows from Theorem 4.1(b) and (c). Part (ii) is immediate from the definition of g_i.

We have $g_i = Q_i(\varphi)$ and hence $g_i(P) = Q_i(\varphi(P))$; the functions are regular at P since P is not a cusp. Since $Q_i(x)$ is a polynomial in $\mathcal{O}_K[x]$, to prove (iii) it suffices to show that $\varphi(P)$ lies in $\mathcal{O}_{K,S}$. Since φ and P are defined over K, we have $\varphi(P) \in K$. By property (a) of Theorem 4.1, φ is the root of a monic polynomial with coefficients in $\mathbb{Z}[j]$. Therefore, $\varphi(P)$ is the root of a monic polynomial with coefficients in $\mathbb{Z}[j(P)] \subseteq \mathcal{O}_{K,S}$. We thus have $\varphi(P) \in \mathcal{O}_{K,S}$ since $\mathcal{O}_{K,S}$ is integrally closed. □

Define the numbers

$$\beta := 2(2^3 4.5^{36m} N^{108m+15} m^{72m+1})^{m\mu+1} 4.5^{12m} N^{36m+4}$$

and $C := 96.6 \cdot 0.1^{24m} N^{90m+4}$. We now bound the absolute value of $g_i(P)$ at infinite places.

Lemma 5.2. *For any infinite place v of K, we have*

$$|g_i(P)|_v \le \begin{cases} (\beta C)^{|\Sigma_i|} \cdot |j(P)|_v^{-1/w_i} & \text{if } v \in S_i, \\ (\beta C)^{|\Sigma_i|} & \text{otherwise.} \end{cases}$$

Proof. Recall we have chosen a place of L extending v that we also denoted by v. We have also chosen a cusp $c_v \in \Sigma$ such that $P \in \Omega_{c_v,v}$. Since P is not a cusp, Theorem 4.1(d) implies that $|\varphi(P) - \varphi(c_v)|_v \le \beta C/2$. Take any cusp $c \in \Sigma$. By Theorem 4.1(c), we have $|\varphi(c)|_v \le \beta m^{24m}$. By using the bound on m from Lemma 4.2, one can show that $|\varphi(c)|_v \le \beta C/4$.

Take any $c \in \Sigma_i$. We have $|\varphi(P)-\varphi(c)|_v \le |\varphi(P)-\varphi(c_v)|_v + |\varphi(c_v)|_v + |\varphi(c)|_v$ and hence $|\varphi(P)-\varphi(c)|_v \le \beta C/2 + \beta C/4 + \beta C/4 = \beta C$. Therefore,

$$|g_i(P)|_v = \prod_{c\in\Sigma_i} |\varphi(P) - \varphi(c)|_v \le (\beta C)^{|\Sigma_i|}.$$

Finally suppose that $v \in S_i$, i.e., $c_v \in \Sigma_i$ and $|j(P)|_v > 3500$. Note that $w_{c_v} = w_i$. We get the other inequality of the lemma in the same manner except also using the bound $|\varphi(P) - \varphi(c_v)|_v \le |j(P)|_v^{-1/w_i} \cdot \beta C$ from Theorem 4.1(d). □

We now bound the absolute value of $g_i(P)$ at finite places.

Lemma 5.3. *For any finite place v of K, we have*

$$|g_i(P)|_v \le \begin{cases} |j(P)|_v^{-1/w_i} & \text{if } v \in S_i \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Take any finite place v of K. First suppose that $v \notin S$. We have $g_i(P) \in \mathcal{O}_{K,S}$ by Lemma 5.1(iii) and hence $|g_i(P)|_v \le 1$.

We can now assume that $v \in S$ and hence $|j(P)|_v > 1$. Recall we have chosen a place of L extending v that we also denoted by v. We have also chosen a cusp $c_v \in \Sigma$ such that $P \in \Omega_{c_v,v}$. Since P is not a cusp, Theorem 4.1(d) implies that $|\varphi(P) - \varphi(c_v)|_v \le |j(P)|_v^{-1/w_{c_v}}$. In particular, $|\varphi(P) - \varphi(c_v)|_v \le 1$.

Take any cusp $c \in \Sigma$. Since $\varphi(c)$ and $\varphi(c_v)$ are integral by Theorem 4.1(c), we find that

$$|\varphi(P) - \varphi(c)|_v \le \max\{|\varphi(P) - \varphi(c_v)|_v, |\varphi(c_v) - \varphi(c)|_v\} \le 1.$$

Therefore, $|g_i(P)| = \prod_{c\in\Sigma_i} |\varphi(P) - \varphi(c)|_v \le 1$. Now assume that $v \in S_i$ and hence $c_v \in \Sigma_i$. Using $w_{c_v} = w_i$, we have $|g_i(P)| = \prod_{c\in\Sigma_i} |\varphi(P) - \varphi(c)|_v \le |\varphi(P) - \varphi(c_v)|_v \le |j(P)|_v^{-1/w_i}$. □

Define $C' := 22.16N^{144m+7}0.024^{24m}$.

Lemma 5.4. *We have*

$$[K:\mathbb{Q}]^{-1} \sum_{v\in S_i} d_v \log|j(P)|_v \le w_i|\Sigma_i|\log(\beta C').$$

Proof. We first assume that $g_i(P) \in K$ is nonzero. We have $\prod_{v\in M_K} |g_i(P)|_v^{d_v} = 1$ by the product formula. Using the upper bounds on $|g_i(P)|_v$ from Lemmas 5.2 and 5.3, we have

$$1 \le \prod_{v\in M_{K,\infty}} (\beta C)^{d_v|\Sigma_i|} \cdot \prod_{v\in S_i} |j(P)|_v^{-d_v/w_i}.$$

Taking logarithms and using that $\sum_{v\in M_{K,\infty}} d_v = [K:\mathbb{Q}]$ gives

$$[K:\mathbb{Q}]^{-1} \sum_{v\in S_i} d_v \log|j(P)|_v \le w_i|\Sigma_i|\log(\beta C).$$

To prove the lemma in this case, it thus suffices to show that $C \le C'$. We have

$$C'/C = \tfrac{22.16}{96.6} N^{54m+3} (\tfrac{0.024}{0.1})^{24m} \ge \tfrac{22.16\cdot 3^3}{96.6} (3^{54} \cdot \tfrac{0.024^{24}}{0.1^{24}})^m > 6\cdot 10^{10m} > 1,$$

where we have used that $N \ge 3$.

We may now assume that $g_i(P) = 0$. We have $\varphi(P) = \varphi(c)$ for some $c \in \Sigma_i$. Since $\varphi(c) = \varphi(P)$ is in K, φ is defined over K and Σ_i has a transitive Gal_K-action, we find that $\varphi(P) = \varphi(c')$ for all $c' \in \Sigma_i$. With our fields $K_G \subseteq K \subseteq L$ and $\Sigma' := \Sigma_i$, let ξ be a nonzero element of $\mathcal{O}_K$ as in Theorem 4.1(e).

Take any place $v \in S_i$. We have $P \in \Omega_{c_v,v} - \{c_v\}$ with $c_v \in \Sigma_i$. Moreover, $|j(P)|_v > 3500$ if v is infinite. By Theorem 4.1(e), we have $|\xi|_v \le |j(P)|_v^{-w_i}$ if v is finite and $|\xi|_v \le |j(P)|_v^{-w_i} \cdot (\beta C')^{w_i|\Sigma_i|}$ if v is infinite.

For any infinite place $v \notin S_i$ of K, we have $|\xi|_v \le (\beta C')^{w_i|\Sigma_i|}$ by Theorem 4.1(e). Since ξ is integral, we have $|\xi|_v \le 1$ for all finite places $v \notin S_i$ of K. The product formula and the above inequalities give

$$1 = \prod_{v\in M_K} |\xi|_v^{d_v} \le \prod_{v\in S_i} |j(P)|_v^{-w_i d_v} \cdot \prod_{v\in M_{K,\infty}} (\beta C')^{w_i|\Sigma_i|d_v}.$$

By taking logarithms and using $\sum_{v\in M_{K,\infty}} d_v = [K:\mathbb{Q}]$, we obtain

$$[K:\mathbb{Q}]^{-1} \sum_{v\in S_i} d_v \log|j(P)|_v \le |\Sigma_i|\log(\beta C') \le w_i|\Sigma_i|\log(\beta C').$$ □

Recall that a finite place v of K lies in S if and only if $|j(P)|_v > 1$. A place $v \in S$ lies in S_i for some $1 \le i \le h$ if v is finite or $|j(P)|_v > 3500$. Therefore,

$$\begin{aligned} h(j(P)) &= [K:\mathbb{Q}]^{-1} \textstyle\sum_{v\in M_K} d_v \log\max\{1, |j(P)|_v\} \\ &\le [K:\mathbb{Q}]^{-1} \sum_{i=1}^h \sum_{v\in S_i} d_v \log|j(P)|_v + [K:\mathbb{Q}]^{-1} \sum_{v\in M_{K,\infty}} d_v \log 3500. \end{aligned}$$

By Lemma 5.4 and $\sum_{v\in M_{K,\infty}} d_v = [K:\mathbb{Q}]$, we obtain

$$h(j(P)) \le \sum_{i=1}^h w_i|\Sigma_i|\log(\beta C') + \log 3500.$$

Observe that $\sum_{i=1}^h w_i|\Sigma_i| \le \sum_{c\in\Sigma} w_c \le \mu$, where the last inequality follows from (2.1). Therefore,

$$h(j(P)) \le \mu\log(\beta C') + \log 3500. \tag{5.1}$$

This is our explicit upper bound for $h(j(P))$; note that the numbers β and C' are both expressed solely in terms of μ, m and N.

We finish by making some estimates to produce worse, though more aesthetically pleasing, bounds for $h(j(P))$.

Lemma 5.5. *We have $h(j(P)) \leq 4(\mu+4)^4 \log N$.*

Proof. Using $m \leq \frac{1}{24}N^3$ from Lemma 4.2, we find that

$$\begin{aligned}\beta &\leq 2(2^3 4.5^{36m}(\tfrac{1}{24})^{72m+1})^{m\mu+1} 4.5^{12m} \cdot N^{(324m+18)(m\mu+1)+(36m+4)}\\ &= 2(\tfrac{1}{3})^{m\mu+1}(\tfrac{4.5}{24^2})^{36m(m\mu+1)} 4.5^{12m} N^{(324m+18)(m\mu+1)+(36m+4)}\end{aligned}$$

and hence

$$\beta C' \leq 44.32(\tfrac{1}{3})^{m\mu+1}(\tfrac{4.5}{24^2})^{36m(m\mu+1)}(4.5\cdot 0.024^2)^{12m}\cdot N^d,$$

where $d := (324m+18)(m\mu+1)+(36m+4)+(144m+7)$. We have $\mu \geq 2$ (since otherwise X_G has only one cusp and hence $1 \leq |S| < \mathfrak{c}_{G,K} = 1$). Using that $m \geq 1$ and $m\mu+1 \geq 3$, we deduce that $\beta C' \leq 44.32(\frac{1}{3})^3(\frac{4.5}{24^2})^{108}(4.5\cdot 0.024^2)^{12}N^d$. Taking logarithms, we find that $\log(\beta C') \leq d \log N - 594.98$. Since $\mu \geq 2$, we have

$$\mu \log(\beta C') + \log 3500 \leq \mu d \log N - 2\cdot 594.98 + \log 3500 \leq \mu d \log N - 1181.$$

In particular, $\mu\log(\beta C') + \log 3500 \leq \mu d \log N$ and hence $h(j(P)) \leq \mu d \log N$ by (5.1).

By [Shi94, Proposition 1.40], we have $g+1 \leq \mu/12+1$, where we have used that X_G has at least two cusps due to the Runge condition on X_G. Using $m \leq g+1 \leq \mu/12+1$, we obtain an upper bound for μd that is a polynomial in μ. In particular, $\mu d \leq f(\mu)$, where $f(x) = (9x^4+222x^3+1536x^2+2132x)/4$. One can readily check that $f(x) \leq 4(x+4)^4$ holds for all $x \geq 0$. Therefore, $\mu d \leq 4(\mu+4)^4$ and hence $h(j(P)) \leq \mu d \log N \leq 4(\mu+4)^4 \log N$. □

By Lemma 4.2, we have $\mu \leq N^3/2$ and hence $h(j(P)) \leq 4(N^3/2+4)^4 \log N$ by Lemma 5.5. Using that $N \geq 3$, one can check that $4(N^3/2+4)^4 \leq N^{12}$ and hence $h(j(P)) \leq N^{12}\log N$.

6. Background: modular forms

In this section, we recall some facts about modular forms. For the basics on modular forms see [Shi94].

6.1. **Notation.** Recall that the group $\mathrm{SL}_2(\mathbb{Z})$ acts by linear fractional transformations on the complex upper half-plane $\mathcal{H}$ and the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Consider an integer $k \geq 0$. For a meromorphic function f on $\mathcal{H}$ and a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, define the meromorphic function $f|_k\gamma$ on $\mathcal{H}$ by $(f|_k\gamma)(\tau) := (c\tau+d)^{-k} f(\gamma\tau)$; we call this the slash operator of weight k.

For a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, we denote by $M_k(\Gamma)$ the set of modular forms of weight k on Γ; it is a finite dimensional complex vector space. Recall that each $f \in M_k(\Gamma)$ is a holomorphic function of the upper half-plane $\mathcal{H}$ that satisfies $f|_k\gamma = f$ for all $\gamma \in \Gamma$ along with the familiar growth condition at the cusps. For each modular form $f \in M_k(\Gamma)$, we have

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, q_w^n$$

for unique $a_n(f) \in \mathbb{C}$, where w is the width of the cusp ∞ of Γ and $q_w := e^{2\pi i\tau/w}$. We call this power series in q_w, the q-expansion of f (at the cusp ∞). Note that f is uniquely determined by its q-expansion and hence we can identify f with its q-expansion. For a subring R of $\mathbb{C}$, we denote by $M_k(\Gamma, R)$ the R-submodule of $M_k(\Gamma)$ consisting of modular forms whose q-expansion has coefficients in R.

6.2. **Actions on $M_k(\Gamma(N))$.** Fix positive integers N and k. Since $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, the slash operator of weight k defines a right action of $\mathrm{SL}_2(\mathbb{Z})$ on $M_k(\Gamma(N))$. Take any modular form $f = \sum_{n=0}^\infty a_n(f) q_N^n$ in $M_k(\Gamma(N))$. For every field automorphism σ of $\mathbb{C}$, there is a unique modular form $\sigma(f) \in M_k(\Gamma(N))$ whose q-expansion is $\sum_{n=0}^\infty \sigma(a_n(f))\, q_N^n$. This defines an action of $\mathrm{Aut}(\mathbb{C})$ on $M_k(\Gamma)$.

The following lemma says that the above actions of $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{C})$ induce a right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N))$. For each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, let σ_d be any automorphism of $\mathbb{C}$ for which $\sigma_d(\zeta_N) = \zeta_N^d$.

Lemma 6.1. *There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ such that the following hold:*

- *if $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then $f * A = f|_k\gamma$, where γ is any matrix in $\mathrm{SL}_2(\mathbb{Z})$ that is congruent to A modulo N,*
- *if $A = \left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$, then $f * A = \sigma_d(f)$.*

Proof. See [BN19, §3]. ☐

6.3. **The spaces $M_{k,G}$.** Fix a positive integer N and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For each integer $k \geq 0$, define

$$M_{k,G} := M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G,$$

i.e., the subgroup fixed by the G-action $*$ from Lemma 6.1. Note that $M_{k,G}$ is a vector space over $K_G = \mathbb{Q}(\zeta_N)^{\det G}$. The following lemma explains how we will use modular forms to produce regular functions on X_G.

Lemma 6.2. *Fix an integer $k \geq 0$ and take any modular forms f and g in $M_{k,G}$ with $g \neq 0$. Then f/g is an element of $K_G(X_G) = \mathcal{F}_N^G$.*

Proof. For any $\gamma \in \Gamma(N)$, we have $(f/g)(\gamma\tau) = f(\gamma\tau)/g(\gamma\tau) = (f|_k\gamma)(\tau)/(g|_k\gamma)(\tau) = f(\tau)/g(\tau)$. Therefore, f/g is a modular function of level N. We have $f/g \in \mathcal{F}_N$ since the q-expansions of f and g both have coefficients in $\mathbb{Q}(\zeta_N)$.

For any $A \in G$, we have $(f/g) * A = (f * A)/(g * A) = f/g$, where the first $*$-action is the one from Lemma 2.1. Therefore, f/g is an element of $\mathcal{F}_N^G = K_G(X_G)$. ☐

Take any cusp $c \in \mathcal{C}_G$ of X_G. Choose an $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \cdot c_\infty = c$, where c_∞ is the cusp at infinity. Set $w = w_c$. For any $f \in M_{k,G}$, the q-expansion of $f * A$ lies in $\mathbb{Q}(\zeta_N)[\![q_w]\!]$. When f is nonzero, we define $\nu_c(f)$ to be the minimal integer n for which the coefficient of q_w^n in the q-expansion of $f * A$ is nonzero. When f is zero, we define $\nu_c(f) = +\infty$. Note that $\nu_c(f)$ does not depend on the choice of A. Now consider any $f, g \in M_{k,G}$ with g nonzero. We have $f/g \in K_G(X_G) \subseteq \mathbb{Q}(\zeta_N)(X_G)$ by Lemma 6.2. Moreover,

$$\mathrm{ord}_c(f/g) = \nu_c(f) - \nu_c(g). \tag{6.1}$$

6.4. **Eisenstein series of weight 1.** See [Kat04, §3] for the basics on Eisenstein series. For further information, we refer to §§2–3 of [BN19] where all the results below are summarized and referenced (except for the explicit constant c_0 in Lemma 6.3, see [Bru17, Lemma 3.1] instead). We will restrict our attention to weight 1 modular forms; our functions E_α are denoted $E_\alpha^{(1)}$ in [BN19].

Fix a positive integer N. Consider any pair $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and choose $a, b \in \mathbb{Z}$ with $\alpha \equiv (a, b) \pmod N$. With $\tau \in \mathcal{H}$, consider the series

$$E_\alpha(\tau, s) = \frac{1}{-2\pi i} \sum_{\substack{\omega \in \mathbb{Z}+\mathbb{Z}\tau \\ \omega \neq -(a\tau+b)/N}} \left(\frac{a\tau+b}{N} + \omega\right)^{-1} \cdot \left|\frac{a\tau+b}{N} + \omega\right|^{-2s}. \tag{6.2}$$

The series (6.2) converges when the real part of $s \in \mathbb{C}$ is large enough. Hecke proved that $E_\alpha(\tau, s)$ can be analytically continued to all $s \in \mathbb{C}$. Using this analytic continuation, we define the Eisenstein series

$$E_\alpha(\tau) := E_\alpha(\tau, 0).$$

For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have $E_\alpha|_1\gamma = E_{\alpha\gamma}$, where $\alpha\gamma \in (\mathbb{Z}/N\mathbb{Z})^2$ denotes matrix multiplication. In particular, E_α is fixed by $\Gamma(N)$ under the slash operator of weight 1.

Lemma 6.3. *Take any $a, b \in \mathbb{Z}$ and let $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ be the image of (a, b) modulo N. The function E_α is a modular form of weight 1 on $\Gamma(N)$ with q-expansion*

$$c_0 + \sum_{\substack{m,n \geq 1 \\ m \equiv a \bmod N}} \zeta_N^{bn} q_N^{mn} - \sum_{\substack{m,n \geq 1 \\ m \equiv -a \bmod N}} \zeta_N^{-bn} q_N^{mn}$$

and $c_0 \in \mathbb{Q}(\zeta_N)$. Moreover,

$$c_0 = \begin{cases} 0 & \text{if } a \equiv b \equiv 0 \pmod N, \\ \frac{1}{2}\,\frac{1+\zeta_N^b}{1-\zeta_N^b} & \text{if } a \equiv 0 \pmod N \text{ and } b \not\equiv 0 \pmod N, \\ \frac{1}{2} - \frac{a_0}{N} & \text{if } a \not\equiv 0 \pmod N, \end{cases}$$

where $0 \le a_0 < N$ is the integer congruent to a modulo N.

The right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_1(\Gamma(N), \mathbb{Q}(\zeta_N))$, described in §6.2, acts on the Eisenstein series E_α in a pleasant manner.

Lemma 6.4. *We have $E_\alpha * A = E_{\alpha A}$ for all $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

6.5. **Expressing modular forms in terms of Eisenstein series.** Using the Eisenstein series of weight 1 from §6.4, we can generate higher weight modular forms.

Theorem 6.5 (Khuri-Makdisi)**.** *Suppose $N > 2$. The $\mathbb{C}$-subalgebra of $\bigoplus_{k\ge 0} M_k(\Gamma(N))$ generated by the Eisenstein series E_α with $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ contains all modular forms of weight k on $\Gamma(N)$ for all $k \ge 2$.*

Proof. This particular formulation of results of Khuri-Makdisi [KM12] is Theorem 3.1 of [BN19]. □

The following is a direct consequence of the above theorem. It describes an explicit finite set of generators for $M_{k,G}$ as a vector space over $\mathbb{Q}$.

Lemma 6.6. *Fix integers $N > 2$ and $k \ge 2$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then $M_{k,G}$, as a $\mathbb{Q}$-vector space, is spanned by the set of modular forms of the form*

$$\sum_{A\in G} \zeta_N^{j \det A}\, E_{\alpha_1 A} \cdots E_{\alpha_k A} \tag{6.3}$$

with $\alpha_i \in (\mathbb{Z}/N\mathbb{Z})^2 - \{0\}$ and $0 \le j < [\mathbb{Q}(\zeta_N) : \mathbb{Q}]$.

Proof. Let S be the set of modular forms of the form $\zeta_N^j E_{\alpha_1} \cdots E_{\alpha_k}$ with pairs $\alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2 - \{(0,0)\}$ and an integer $0 \le j < \phi(N) := [\mathbb{Q}(\zeta_N) : \mathbb{Q}]$. Since $E_{(0,0)} = 0$, Theorem 6.5 implies that S spans the complex vector space $M_k(\Gamma(N))$. We have $S \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ by Lemma 6.3. Since $k \ge 2$ and $N > 2$, the natural map $M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma(N))$ is an isomorphism of complex vector spaces, cf. [Kat73, §1.7]. Since $S \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ spans $M_k(\Gamma(N))$, we deduce that S also spans the $\mathbb{Q}(\zeta_N)$-vector space $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$. Since $1, \zeta_N, \ldots, \zeta_N^{\phi(N)-1}$ is a basis of $\mathbb{Q}(\zeta_N)$ as a vector space over $\mathbb{Q}$, we find S further spans $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ as a vector space over $\mathbb{Q}$.

Define the $\mathbb{Q}$-linear map $T\colon M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \to M_{k,G}$, $f \mapsto \sum_{A\in G} f * A$. The map T is surjective since we have $T(f) = |G|\, f$ for all $f \in M_{k,G}$. Therefore, $M_{k,G}$ as a $\mathbb{Q}$-vector space is spanned by the set of $T(f)$ with $f \in S$. It remains to compute $T(f)$ for $f \in S$. Take any $f = \zeta_N^j E_{\alpha_1} \cdots E_{\alpha_k} \in S$. We have

$$T(f) = \sum_{A\in G} (\zeta_N^j E_{\alpha_1} \cdots E_{\alpha_k}) * A = \sum_{A\in G} \zeta_N^{j \det A} (E_{\alpha_1} * A) \cdots (E_{\alpha_k} * A).$$

Finally note that $T(f)$ equals (6.3) by Lemma 6.4. □

Remark 6.7. In [Zyw24], under the extra assumption $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, a version of Lemma 6.6 is required for an algorithm which finds an explicit basis of $M_{k,G}$ for any given even integer $k \ge 2$. Using a suitable weight $k \in \{2, 4, 6\}$, this basis can then used to compute an explicit model of the curve X_G over $K_G = \mathbb{Q}$.

7. A basis of modular forms with relatively small coefficients

Fix an integer $N > 2$ and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $-I \in G$. In §6.3, we defined a finite dimensional K_G-vector space $M_{k,G}$ of modular forms of level N and weight k. Since $-I \in G$, we find that $M_{k,G} = 0$ for k odd.

In this section, we prove the following result which shows that there is basis of $M_{k,G}$, viewed as a vector over $\mathbb{Q}$, consisting of modular forms whose q-expansion at each cusp has integral and relatively small coefficients.

Theorem 7.1. *Fix an even integer $k \ge 2$. Then there is a basis $f_1, \ldots, f_d$ of the $\mathbb{Q}$-vector space $M_{k,G}$ such that for every $1 \le i \le d$ and every $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have*

$$f_i * A = \sum_{n=0}^{\infty} a_n q_N^n,$$

where each coefficient a_n lies in $\mathbb{Z}[\zeta_N]$ and satisfies

$$|a_n|_v \le 2|G| 4.5^k N^k \max\{N^k, n^{2k}\}$$

for all infinite places v of $\mathbb{Q}(\zeta_N)$.

7.1. **Bounding coefficients.** Fix an even integer $k \geq 2$. Lemma 6.6 shows that there is a basis of $M_{k,G}$ obtained from Eisenstein series of weight 1. We will want to bound the size of the Fourier coefficients that arise in such a basis. We first prove a simple lemma that will be needed for these bounds. For each positive integer n, let $d(n)$ be the number of positive divisors of n.

Lemma 7.2. *Take any positive integers j and n, and define the sum*

$$S_{j,n} := \sum_{a_1+\cdots+a_j=n} \prod_{i=1}^{j} d(a_i)$$

where $a_1, \ldots, a_j$ vary over all positive integers. Then $S_{j,n} \leq 2n^{j-1/2}(\log n + 1)^{j-1}$.

Proof. We proceed by induction on $j \geq 1$. We have $d(n) \leq 2n^{1/2}$ since for every positive divisor e of n at least one of e or n/e is bounded above $n^{1/2}$. The case $j = 1$ is now clear since $S_{1,n} = d(n)$.

Now consider any $j \geq 1$ for which the lemma holds. We have $S_{j+1,n} = \sum_{a=1}^{n} d(a) S_{j,n-a}$. Thus by our inductive hypothesis, we have $S_{j+1,n} \leq 2n^{j-1/2}(\log n + 1)^{j-1} \sum_{a=1}^{n} d(a)$. So to prove the lemma, it suffices to show that $\sum_{a=1}^{n} d(a) \leq n(\log n + 1)$.

We have inequalities $\sum_{a=1}^{n} d(a) = \#\{(b,c) \in \mathbb{N} : bc \leq n\} \leq \sum_{b=1}^{n} \lfloor n/b \rfloor \leq n \sum_{b=1}^{n} 1/b$. Therefore, $\sum_{a=1}^{n} d(a) \leq n(1 + \sum_{b=2}^{n} 1/b) \leq n(1 + \int_1^n 1/x\, dx) = n(\log n + 1)$ as desired. ☐

Lemma 7.3. *Fix positive integers k and N. For any $\alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$, the q-expansion of $E_{\alpha_1} \cdots E_{\alpha_k}$ is of form $\sum_{n=0}^{\infty} a_n q_N^n$ with $a_n \in \mathbb{Q}(\zeta_N)$ that satisfy $|a_0| \leq (N/4)^k$ and*

$$|a_n| \leq 2n^{-1/2}(N/4 + 2n(\log n + 1))^k$$

for all $n \geq 1$.

Proof. First take any $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and fix $a, b \in \mathbb{Z}$ so that $\alpha \equiv (a, b) \pmod{N}$ with $0 \leq a < N$ and $|b| \leq N/2$. Let $\sum_{n=0}^{\infty} c_n(\alpha) q_N^n$ be the q-expansion of E_α. We have $c_n(\alpha) \in \mathbb{Q}(\zeta_N)$ by Lemma 6.3. Moreover, the explicit q-expansion given in Lemma 6.3 implies that $|c_n(\alpha)| \leq 2d(n)$ for all $n \geq 1$.

We claim that $|c_0(\alpha)| \leq N/4$. From Lemma 6.3, we have $|c_0(\alpha)| \leq 1/2$ if $a \not\equiv 0 \pmod{N}$ or $b \equiv 0 \pmod{N}$. So to prove the claim, we may assume from Lemma 6.3 that $b \not\equiv 0 \pmod{N}$ and $c_0(\alpha) = 1/2 \cdot (1 + \zeta_N^b)/(1 - \zeta_N^b)$. We have $|c_0(\alpha)|^2 \leq |1 - \zeta_N^b|^{-2} = (2 - 2\cos(\theta))^{-1}$, where $\theta := 2\pi b/N \in [-\pi, \pi]$. Since $2 - 2\cos(x) \geq 4/\pi^2 \cdot x^2$ for all real $x \in [-\pi, \pi]$ and $\theta \neq 0$, we deduce that $|c_0(\alpha)|^2 \leq \pi^2/4 \cdot \theta^{-2} = N^2/(16b^2) \leq N^2/16$. Therefore, $|c_0(\alpha)| \leq N/4$ as claimed.

Multiplying the q-expansions of $E_{\alpha_1}, \ldots, E_{\alpha_k}$ together, we have

$$a_n = \sum_{n_1+\cdots+n_k=n,\, n_i \geq 0} \prod_{i=1}^{k} c_{n_i}(\alpha_i). \tag{7.1}$$

For $n = 0$, we have $|a_0| = \prod_{i=1}^{k} |c_0(\alpha_i)| \leq (N/4)^k$ which proves the lemma in this case.

Now take any integer $n \geq 1$. For each subset $I \subseteq \{1, \ldots, k\}$, we can consider those terms in the sum (7.1) for which we have $n_i = 0$ exactly when $i \in I$. Using our bounds for the coefficients $c_n(\alpha)$, we deduce that

$$|a_n| \leq \sum_{j=1}^{k} \binom{k}{j} \cdot (N/4)^{k-j} \sum_{a_1+\cdots+a_j=n, a_i \geq 1} \prod_{i=1}^{j} 2d(a_i).$$

Equivalently, $|a_n| \leq \sum_{j=1}^{k} \binom{k}{j} \cdot (N/4)^{k-j} \cdot 2^j S_{j,n}$ with $S_{j,n}$ as in Lemma 7.2. By Lemma 7.2, we obtain the upper bounds

$$|a_n| \leq 2\sum_{j=1}^{k} \binom{k}{j} \cdot (N/4)^{k-j} \cdot 2^j n^{j-1/2}(\log n + 1)^j \leq 2n^{-1/2} \sum_{j=1}^{k} \binom{k}{j} (N/4)^{k-j}(2n(\log n + 1))^j.$$

So by the binomial theorem, we have $|a_n| \leq 2n^{-1/2}(N/4 + 2n(\log n + 1))^k$. ☐

Lemma 7.4. *Fix positive integers k and N and take any $\alpha_1,\ldots,\alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$. Define the modular form $h := (2N)^k E_{\alpha_1}\cdots E_{\alpha_k} \in M_k(\Gamma(N),\mathbb{Q}(\zeta_N))$. For any $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the q-expansion of $h * A$ is of form $\sum_{n=0}^{\infty} a_n q_N^n$ so that each coefficient a_n is an element of $\mathbb{Z}[\zeta_N]$ that satisfy $|a_0| \le N^{2k}/2^k$ and*

$$|a_n| \le 2n^{-1/2} N^k (N/2 + 4n(\log n + 1))^k$$

for all $n \ge 1$.

Proof. By Lemma 6.3, we find that h, and hence also $h*A$, are modular forms in $M_k(\Gamma(N),\mathbb{Q}(\zeta_N))$. Using Lemma 6.4, we have $h*A = (2N)^k(E_{\alpha_1}*A)\cdots(E_{\alpha_k}*A) = (2N)^k E_{\beta_1}\cdots E_{\beta_k}$, where $\beta_i := \alpha_i A$. Therefore, the desired bounds on the $|a_n|$ follow from those of Lemma 7.3 after multiplying by $(2N)^k$.

Finally, to prove that each a_n lies in $\mathbb{Z}[\zeta_N]$, it suffices to show that the q-expansion of $2N\cdot E_{\beta_i}$ has coefficients in $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$ for all $1 \le i \le k$. From the explicit q-expansions given in Lemma 6.3, it suffices to show that $N/(1-\zeta_N^b)$ lies in $\mathbb{Z}[\zeta_N]$ for any integer $b \not\equiv 0 \pmod N$. We have $N/(1-\zeta_N^b) \in \mathbb{Z}[\zeta_N]$ since $\zeta_N^b - 1$ is a root of $((x+1)^N - 1)/x = x^{N-1} + \cdots + N \in \mathbb{Z}[x]$. ☐

7.2. **Proof of Theorem 7.1.** By Lemma 6.6, there is a basis $f_1,\ldots,f_d$ of the $\mathbb{Q}$-vector space $M_{k,G}$ such every f_i has a q-expansion of the form

$$(2N)^k \sum_{g\in G} \zeta_N^{j\det g} E_{\alpha_1 g}\cdots E_{\alpha_k g} \tag{7.2}$$

for some $\alpha_1,\ldots,\alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$ and integer j.

Take any $1 \le i \le d$ and $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $\sum_{n=0}^{\infty} a_n q_N^n$ be the q-expansion of $f_i * A$. Take any infinite place v of $\mathbb{Q}(\zeta_N)$. Since $\mathbb{Q}(\zeta_N) \subseteq \mathbb{C}$, there is a $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ such that $|a|_v = |\sigma(a)|$ for all $a \in \mathbb{Q}(\zeta_N)$. There is a unique $d' \in (\mathbb{Z}/N\mathbb{Z})^\times$ for which $\sigma(\zeta_N) = \zeta_N^{d'}$. Define $B := A\left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By Lemma 6.1, we have $f_i * B = \sum_{n=0}^{\infty}\sigma(a_n)q_N^n$. Since the q-expansion of f_i is of the form (7.2), Lemma 7.4 implies that all of the $\sigma(a_n)$ are in $\mathbb{Z}[\zeta_N]$ and

$$|a_n|_v = |\sigma(a_n)| \le \begin{cases} |G|\cdot N^{2k}/2^k & \text{if } n=0,\\ |G|\cdot 2n^{-1/2}N^k(N/2+4n(\log n+1))^k & \text{if } n \ge 1.\end{cases}$$

It remains to prove that $|a_n|_v \le 2|G|4.5^k N^k \max\{N^k, n^{2k}\}$. This is immediate for $n=0$ from the above bound, so assume that $n \ge 1$. We have $\log n + 1 \le n$, so $|a_n|_v \le 2|G|N^k(N/2+4n^2)^k$. When $N \le n^2$, we have $|a_n|_v \le 2|G|N^k(4.5n^2)^k$. When $N \ge n^2$, we have $|a_n|_v \le 2|G|N^k(4.5N)^k$. The theorem is now immediate.

8. Riemann–Roch

Fix an integer $N > 2$ and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $-I \in G$. Let g be the genus of the curve X_G and let μ be the degree of the morphism $j\colon X_G \to \mathbb{P}^1_{K_G}$. The group Gal_{K_G} acts on the set of cusps $\mathcal{C}_G$ of X_G by Lemma 2.3(ii).

Consider a proper subset of $\Sigma \subseteq \mathcal{C}_G$ that is stable under the Gal_{K_G}-action. For our application, we will require a nonconstant function $\varphi \in K_G(X_G)$ whose poles are all at cusps and has no pole at any cusp $c \in \Sigma$. In this section, we use the Riemann–Roch theorem to find spaces of modular forms from which we can construct such φ.

Consider a divisor $D = \sum_{c\in\mathcal{C}_G} n_c\cdot c$ of X_G that is defined over K_G, i.e., $n_c = n_{\sigma(c)}$ for all $c \in \mathcal{C}_G$ and $\sigma \in \mathrm{Gal}_{K_G}$. Define the K_G-vector space $\mathscr{L}(D) := \{\varphi \in K_G(X_G) : \mathrm{div}(\varphi) + D \ge 0\}$; equivalently, $\mathscr{L}(D)$ consists of those functions $\varphi \in K_G(X_G)$ whose poles all occur at cusps and $\mathrm{ord}_c(\varphi) + n_c \ge 0$ for all $c \in \mathcal{C}_G$. By the Riemann–Roch theorem, we have $\dim_{K_G}\mathscr{L}(D) \ge \deg(D) - g + 1$ with equality holding when $\deg(D) > 2g-2$.

For a fixed positive integer m, define the divisors $D_0 := \sum_{c\in\mathcal{C}_G} mw_c\cdot c$ and $D_1 := \sum_{c\in\mathcal{C}_G-\Sigma} mw_c\cdot c$. The divisors D_0 and D_1 are defined over K_G since $\mathcal{C}_G$ and Σ are both stable under the Gal_{K_G}-action (also $w_{\sigma(c)} = w_c$ for all $c \in \mathcal{C}_G$ and $\sigma \in \mathrm{Gal}_{K_G}$). The functions in $\mathscr{L}(D_0)$ have no poles away from the cusps. The functions in the subspace $\mathscr{L}(D_1) \subseteq \mathscr{L}(D_0)$ are regular at all $c \in \Sigma$.

By Lemma 6.2, we have an injective K_G-linear map

$$T\colon M_{12m,G} \hookrightarrow K_G(X_G),\quad f \mapsto f/\Delta^m.$$

Let W_m be the K_G-subspace of $M_{12m,G}$ consisting of those modular forms f for which $\nu_c(f) \geq mw_c$ for all $c \in \Sigma$, where ν_c is defined in §6.3.

Lemma 8.1.

(i) *We have* $T(M_{12m,G}) = \mathscr{L}(D_0)$ *and* $T(W_m) = \mathscr{L}(D_1)$.

(ii) *We have* $\dim_{K_G} M_{12m,G} = m\mu - g + 1$ *and*

$$\dim_{K_G} W_m \geq m \sum_{c \in \mathcal{C}_G - \Sigma} w_c - g + 1.$$

Proof. We first prove that $T(M_{12m,G}) = \mathscr{L}(D_0)$. Take any $f \in M_{12m,G}$ and define $\varphi := T(f) = f/\Delta^m \in K_G(X_G)$. Every pole of φ is a cusp since Δ, when viewed as a function of the upper half-plane, is holomorphic and everywhere nonzero. Take any cusp $c \in \mathcal{C}_G$. By (6.1), we have $\operatorname{ord}_c \varphi = \nu_c(f) - \nu_c(\Delta^m) = \nu_c(f) - mw_c \geq -mw_c$. Therefore, $T(f) = \varphi \in \mathscr{L}(D_0)$. We have $T(M_{12m,G}) \subseteq \mathscr{L}(D_0)$ since f was an arbitrary element of $M_{12m,G}$.

Now take any $\varphi \in \mathscr{L}(D_0)$. Define $f := \varphi\Delta^m$; it is a weakly modular form of weight $12m$. For each $c \in \mathcal{C}_G$, we have $\operatorname{ord}_c(\varphi) + \nu_c(\Delta^m) = \operatorname{ord}_c(\varphi) + mw_c \geq 0$, where the inequality use our choice of φ. Therefore, f is a modular form of weight $12m$ on $\Gamma(N)$. We have $f \in M_{12m}(\Gamma(N), \mathbb{Q}(\zeta_N))$ since the q-expansions of φ and Δ have coefficients in $\mathbb{Q}(\zeta_N)$. For any $A \in G$, we have $f * A = (\varphi\Delta^m) * A = (\varphi * A)(\Delta^m * A) = \varphi\Delta^m$. Therefore, $f \in M_{12m,G}$ and hence $\varphi = T(f)$ lies in $T(M_{12m,G})$. We have $T(M_{12m,G}) \supseteq \mathscr{L}(D_0)$ since φ was an arbitrary element of $\mathscr{L}(D_0)$. This completes the proof that $T(M_{12m,G}) = \mathscr{L}(D_0)$.

For any $f \in M_{12m,G}$, we have $\operatorname{ord}_c(T(f)) = \nu_c(f) - mw_c$ for each $c \in \mathcal{C}_G$. So $T(f) \in \mathscr{L}(D_1)$ if and only if $\nu_c(f) \geq mw_c$ for each $c \in \Sigma$. Since $T(M_{12m,G}) = \mathscr{L}(D_0)$, we deduce that $T(W_m) = \mathscr{L}(D_1)$.

By the Riemann–Roch theorem, we have

$$\dim_{K_G} W_m = \dim_{K_G} \mathscr{L}(D_1) \geq \deg(D_1) - g + 1 = m \sum_{c \in \mathcal{C} - \Sigma} w_c - g + 1.$$

We have $\deg(D_0) = \sum_{c \in \mathcal{C}_G} mw_c = m\mu$ by (2.1) and $2g - 2 < \mu/6$ by [Shi94, Proposition 1.40]. Therefore, $\deg(D_0) > 2g - 2$. By the Riemann–Roch theorem, we have $\dim_{K_G} M_{12m,G} = \dim_{K_G} \mathscr{L}(D_0) = \deg(D_1) - g + 1 = m\mu - g + 1$. ☐

Take any $f \in W_m$ and define $\varphi := T(f) = f/\Delta^m$. By Lemma 8.1, $\varphi \in K_G(X_G)$ is a function that is regular at all $c \in \Sigma$ and all of its poles are at cusps. In order for φ to be nonconstant, we need f not to lie in the subspace $K_G\Delta^m \subseteq W_m$. Thus to construct a nonconstant φ in this manner, we need $\dim_{K_G} W_m \geq 2$; by Lemma 8.1 this holds for all sufficiently large m.

9. Existence of a certain modular form

Fix an integer $N > 2$ and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $-I \in G$. Let g be the genus of the curve X_G and let μ be the degree of the morphism $j\colon X_G \to \mathbb{P}^1_{K_G}$.

Let Σ be a proper subset of $\mathcal{C}_G$ that is stable under the Gal_{K_G}-action. Let m be the smallest positive integer for which $m \sum_{c \in \mathcal{C}_G - \Sigma} w_c > g$. Define the real number

$$\beta := 2(2^3 4.5^{36m} N^{108m+15} m^{72m+1})^{m\mu+1} 4.5^{12m} N^{36m+4}.$$

Theorem 9.1. *There is a nonzero modular form* $f \in M_{12m,G}$ *that satisfies the following properties:*

(a) *We have* $\nu_c(f) \geq mw_c$ *for all* $c \in \Sigma$.

(b) *The modular form* f *does not lie in* $K_G\Delta^m$.

(c) *Take any* $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. *Define the cusp* $c := A \cdot c_\infty$ *of* X_G, *where* c_∞ *is the cusp at infinity, and set* $w = w_c$. *Then we have* $f * A = \sum_{n=0}^{\infty} b_n q_w^n$, *where each coefficient* b_n *lies in* $\mathbb{Z}[\zeta_N]$ *and satisfies*

$$|b_n|_v \leq \beta \max\{1, (n/w)^{24m}\}$$

for each infinite place v *of* $\mathbb{Q}(\zeta_N)$.

9.1. **Proof of Theorem 9.1.** Set $k = 12m$ and define $d := \dim_{\mathbb{Q}} M_{k,G}$. Fix a basis $f_1, \ldots, f_d$ of the $\mathbb{Q}$-vector space $M_{k,G}$ satisfying the conclusion of Theorem 7.1. Using Lemma 8.1, we find that

$$d = [K_G : \mathbb{Q}] \dim_{K_G} M_{k,G} = [K_G : \mathbb{Q}](m\mu - g + 1).$$

Let W be the K_G-subspace of $M_{k,G}$ consisting of those modular forms f for which $\nu_c(f) \geq mw_c$ for all $c \in \Sigma$. By Lemma 8.1 and our choice of m, we have $\dim_{K_G} W \geq 2$. We will now describe W as the kernel of a linear map on $M_{k,G}$.

Define $L := \mathbb{Q}(\zeta_N)$. For each cusp $c \in \Sigma$, we choose a matrix $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \cdot c_\infty = c$. For any $f \in M_{k,G}$, we have $f * A = \sum_{n=0}^{\infty} a_{c,n}(f)\, q_{w_c}^n$ with $a_{c,n}(f) \in L$. Define the $\mathbb{Q}$-linear map

$$\psi_c \colon M_{k,G} \to L^{mw_c}, \quad f \mapsto (a_{c,0}(f), \ldots, a_{c,mw_c-1}(f)).$$

Combining the maps ψ_c with $c \in \Sigma$, we obtain a $\mathbb{Q}$-linear map

$$\psi \colon M_{k,G} \to \prod_{c \in \Sigma} L^{mw_c}.$$

Note that the kernel of ψ is W. Let

$$\alpha_0 \colon \mathbb{Q}^d \to \prod_{c \in \Sigma} L^{mw_c}$$

be the $\mathbb{Q}$-linear map obtained by composing the isomorphism $\mathbb{Q}^d \xrightarrow{\sim} M_{k,G}$ coming from the basis $f_1, \ldots, f_d$ with ψ. We have $\dim_{\mathbb{Q}} \ker(\alpha_0) = \dim_{\mathbb{Q}} W$.

We have an isomorphism $L \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{v \in M_{L,\infty}} L_v$ of real vector spaces induced by the inclusions $L \subseteq L_v$. Tensoring α_0 with $\mathbb{R}$ gives a $\mathbb{R}$-linear map

$$\alpha \colon V_1 \to V_2,$$

where $V_1 = \mathbb{R}^d$ and $V_2 = \prod_{c \in \Sigma} \prod_{v \in M_{L,\infty}} L_v^{mw_c}$. We have $\dim_{\mathbb{R}} \ker(\alpha) = \dim_{\mathbb{Q}} W$.

We define norms on V_1 and V_2 by $\|b\|_1 := \sum_{i=1}^d |b_i|$ and $\|(b_{c,v})\|_2 := \max_{c \in \Sigma, v \in M_{L,\infty}} |b_{c,v}|_v$, respectively. The group $M_1 := \mathbb{Z}^d$ is a lattice in V_1; it is generated by elements of norm 1. Let M_2 be the lattice in V_2 corresponding to the subgroup $\prod_{c \in \Sigma} \mathcal{O}_L^{mw_c}$ of $\prod_{c \in \Sigma} L^{mw_c}$. For each $i \in \{1, 2\}$ and nonzero $b \in M_i$, we have $\|b\|_i \geq 1$. For each $1 \leq i \leq d$, we have $\psi_c(f_i) \in \mathcal{O}_L^{mw_c}$ for all $c \in \Sigma$ by our choice of basis $f_1, \ldots, f_d$. Therefore, $\alpha(M_1) \subseteq M_2$.

The *norm* $\|\alpha\|$ of α is the minimal real number for which $\|\alpha(v)\|_2 \leq \|\alpha\| \, \|v\|_1$ holds for all $v \in V_1$. We now find an upper bound for $\|\alpha\|$.

Lemma 9.2. *We have* $\|\alpha\| \leq 2|G| 4.5^k N^{3k} m^{2k}$.

Proof. Take any $b \in \mathbb{R}^d$. We have $\alpha(b) = \sum_{i=1}^d b_i \alpha(e_i)$, where $e_1, \ldots, e_d$ is the standard basis of $\mathbb{R}^d$. Taking the norm gives $\|\alpha(b)\|_2 \leq \sum_{i=1}^d |b_i| \, \|\alpha(e_i)\|_2 \leq \max_{1 \leq i \leq d} \|\alpha(e_i)\|_2 \cdot \|b\|_1$. Therefore, $\|\alpha\| \leq \max_{1 \leq i \leq d} \|\alpha(e_i)\|_2$ and hence

$$\|\alpha\| \leq \max\{|a_{c,n}(f_i)|_v : i \in \{1, \ldots, d\}, n \in \{0, \ldots, mw_c - 1\}, c \in \Sigma, v \in M_{L,\infty}\}.$$

Take any $1 \leq i \leq d$, $c \in \Sigma$ and $v \in M_{L,\infty}$. Recall that $f * A = \sum_{n=0}^{\infty} a_{c,n}(f) q_{w_c}^n$ for some $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. In particular, $f * A = \sum_{n=0}^{\infty} a_{c,n}(f) q_N^{nN/w_c}$. By Theorem 7.1, we have $|a_{c,0}(f_i)|_v \leq |G| N^{2k}/2^k$. Now take any $1 \leq n < mw_c$ and define the integer $n_0 := nN/w_c$. We have $1 \leq n_0 < mN$. By Theorem 7.1, we have

$$|a_{c,n}(f_i)|_v \leq 2|G| 4.5^k N^k \max\{N^k, n_0^{2k}\} \leq 2|G| 4.5^k N^{3k} m^{2k}.$$

Combining everything together, we have now shown that $\|\alpha\| \leq 2|G| 4.5^k N^{3k} m^{2k}$. □

Before proceeding, we recall the following version of Siegel's lemma due to Faltings.

Lemma 9.3. *Let V_1 and V_2 be finite dimensional real vector spaces with norms $|\cdot|_1$ and $|\cdot|_2$, respectively. Let M_1 and M_2 be $\mathbb{Z}$-lattices of V_1 and V_2, respectively. Let $\alpha \colon V_1 \to V_2$ be a linear map that satisfies $\alpha(M_1) \subseteq M_2$. Let $C \geq 2$ be a real number such that α has norm at most C (i.e., $|\alpha(v)|_2 \leq C \cdot |v|_1$ for all $v \in V_1$), M_1 is generated by elements of norm at most C, and every nonzero element of M_1 and M_2 has norm at least C^{-1}. Define $a = \dim \ker(\alpha)$ and $b = \dim V_1$. Then for each $0 \leq i \leq a - 1$, $\ker(\alpha)$ contains linearly independent elements $m_1, \ldots, m_{i+1}$ of M_1 satisfying*

$$\max_{1 \leq j \leq i+1} |m_j|_1 \leq (C^3 \cdot b)^{b/(a-i)}.$$

Proof. See [Fal91, Proposition 2.18] or [Koo93, Lemma 4]; they give the upper bound $(C^{3b} \cdot b!)^{1/(a-i)}$ from which our follows by using that $b! \le b^b$. $\square$

We now apply Siegel's lemma in our setting. Define $\mathcal{B} := (2^3 4.5^{3k} N^{9k+15} m^{6k+1})^{m\mu+1}$.

Lemma 9.4. *There is a $u \in \mathbb{Z}^d$ with $\|u\|_1 \le \mathcal{B}$ such that $\sum_{i=1}^d u_i f_i$ lies in W but does not lie in the subspace $K_G \Delta^m$.*

Proof. Define $a := \dim_{\mathbb{R}} \ker(\alpha) = \dim_{\mathbb{Q}} W = [K_G : \mathbb{Q}] \dim_{K_G} W \ge 2[K_G : \mathbb{Q}]$ and $b := \dim V_1 = d = [K_G : \mathbb{Q}](m\mu - g + 1)$. Using Lemma 9.2, we find that the conditions of Lemma 9.3 hold in our setting with $C := 2|G| 4.5^k N^{3k} m^{2k}$.

Now take $i := [K_G : \mathbb{Q}]$; we have $i < a$. By Lemma 9.3, there are linearly independent vectors $m_1, \ldots, m_{i+1} \in \mathbb{Z}^d$ in $\ker(\alpha)$ satisfying $\|m_j\|_1 \le (C^3 b)^{b/(a-i)}$ for all $1 \le j \le i+1$. Since $i + 1 > [K_G : \mathbb{Q}] = \dim_{\mathbb{Q}}(K_G \Delta^m)$, there is a vector $u \in \{m_1, \ldots, m_{i+1}\} \subseteq \mathbb{Z}^d$ so that

$$f := \sum_{i=1}^{d} u_i f_i$$

is a modular form in $M_{k,G}$ for which f does not lie in $K_G \Delta^m$. Since u is in the kernel of α, and hence also the kernel of α_0, we find that f lies in W. We have $\|u\|_1 \le (C^3 b)^{b/(a-i)}$ since $u = m_j$ for some j.

It remains to bound $(C^3 b)^{b/(a-i)}$ from above. We have $a - i \ge 2[K_G : \mathbb{Q}] - [K_G : \mathbb{Q}] = [K_G : \mathbb{Q}]$ and $b = [K_G : \mathbb{Q}](m\mu - g + 1)$, so $b/(a - i) \le m\mu - g + 1 \le m\mu + 1$. We have

$$C^3 b = 2^3 4.5^{3k} N^{9k} m^{6k} \cdot |G|^3 [K_G : \mathbb{Q}] \cdot (m\mu - g + 1).$$

We have $[K_G : \mathbb{Q}] \le [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$, so $|G|^3 [K_G : \mathbb{Q}] \le |\,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})|^3 \le N^{12}$. We have $m\mu - g + 1 \le m\mu + 1 \le 2m\mu \le mN^3$ by Lemma 4.2. Therefore, $C^3 b \le 2^3 4.5^{3k} N^{9k+15} m^{6k+1}$ and hence $(C^3 b)^{b/(a-i)} \le \mathcal{B}$. $\square$

Fix a $u \in \mathbb{Z}^d$ as in Lemma 9.4. Define $f := \sum_{i=1}^d u_i f_i$; it is an element of W that does not lie in $K_G \Delta^m$.

Take any matrix $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and take any infinite place v of $\mathbb{Q}(\zeta_N)$ Define the cusp $c := A \cdot c_\infty$ and set $w = w_c$. We now consider the q-expansions $f * A = \sum_{n=0}^\infty a_n q_N^n$ and $f_i * A = \sum_{n=0}^\infty a_{i,n} q_N^n$ with $1 \le i \le d$. Since $f = \sum_{i=1}^d u_i f_i$, we have $a_n = \sum_{i=1}^d u_i a_{i,n}$ for all $n \ge 0$. So for $n \ge 0$, we have $|a_n|_v \le \|u\|_1 \max_{1 \le i \le d} |a_{i,n}|_v \le \mathcal{B} \max_{1 \le i \le d} |a_{i,n}|_v$.

Since $f_1, \ldots, f_d$ is a basis of $M_{k,G}$ satisfying the conclusion of Theorem 7.1, we find that

$$|a_n|_v \le \mathcal{B} \cdot 2 \cdot 4.5^k N^{k+4} \max\{N^k, n^{2k}\}$$

where we have used the bound $|G| \le N^4$. However, recall that we are interested in the coefficients of the q-expansion $\sum_{n=0}^\infty b_n q_w^n$ of $f * A$. We must have $b_n = a_{nN/w}$ for all $n \ge 0$. So for $n \ge 0$, we have

$$\begin{aligned} |b_n|_v = |a_{nN/w}|_v &\le \mathcal{B} \cdot 2 \cdot 4.5^k N^{k+4} \max\{N^k, (nN/w)^{2k}\} \\ &\le \mathcal{B} \cdot 2 \cdot 4.5^k N^{2k+4} \max\{1, N^k (n/w)^{2k}\} \\ &\le \mathcal{B} \cdot 2 \cdot 4.5^k N^{3k+4} \max\{1, (n/w)^{2k}\}. \end{aligned}$$

The theorem follows since $k = 12m$ and hence $\beta = \mathcal{B} \cdot 2 \cdot 4.5^k N^{3k+4}$.

9.2. **Some bounds.** We now prove some technical lemmas that we will later use to bound functions near cusps. Note that the bound on c_n in the following lemma is, up to a constant factor, that of $|b_n|_v$ from Theorem 9.1.

Lemma 9.5. *Take any real number $0 \le u \le e^{-\pi\sqrt{3}}$ and positive integer m. Fix a positive divisor w of N and let $\{c_n\}_{n \ge 1}$ be a sequence of nonnegative real numbers that satisfy $c_n \le \max\{1, (n/w)^{24m}\}$.*

(i) *For any integer $B \ge 5mw$, we have $\sum_{n=B}^\infty c_n u^{n/w} \le 230.8 w u^{B/w} (B/w)^{24m+1}$.*
(ii) *For any integer $mw \le B \le 5mw$, we have $\sum_{n=B}^\infty c_n u^{n/w} \le 231.6 w u^{B/w} (5m)^{24m+1}$.*

Proof. Set $u_0 := e^{-\pi\sqrt{3}}$ and $a := -24/\log(u_0) \cdot m = m \cdot 4.410\ldots$. Define the function $g(x) = x^{24m} u_0^x$. One can check that $g(x)$ is increasing for $0 \le x \le a$ and decreasing for $x \ge a$.

We first assume that $B \geq 5mw$. We have

$$\sum_{n=B}^{\infty} c_n u^{n/w} = u^{B/w} \sum_{n=0}^{\infty} c_{n+B} u^{n/w} = u^{B/w} \sum_{e=0}^{\infty} \Big(\sum_{r=0}^{w-1} c_{ew+r+B}\, u^{r/w} \Big) u^e.$$

For all integers $e \geq 0$ and $0 \leq r < w$, we have

$$c_{ew+r+B} \leq ((ew+r+B)/w)^{24m} \leq (e+1+B/w)^{24m},$$

where the first bound uses that $(ew+r+B)/w \geq B/w \geq 1$. Using that $u^{r/w} \leq 1$ for all $0 \leq r < w$ and that $u \leq u_0$, we obtain

$$\sum_{n=B}^{\infty} c_n u^{n/w} \leq u^{B/w} w \sum_{e=0}^{\infty} (e+1+B/w)^{24m} u_0^e = u^{B/w} w u_0^{-1-B/w} C, \tag{9.1}$$

where $C := \sum_{e=0}^{\infty} g(e+1+B/w)$. Since $g(x)$ is decreasing for $x \geq 5m$ and $B/w \geq 5m$, we have

$$C \leq \int_0^{\infty} g(x+B/w)\, dx = \int_{B/w}^{\infty} g(x)\, dx = \sum_{i=0}^{\infty} s_i,$$

where $s_i := \int_{2^i B/w}^{2^{i+1}B/w} g(x)\, dx$. For $x \geq 5m$, we have $g(2x)/g(x) = 2^{24m} u_0^x \leq (2^{24} u_0^5)^m \leq 0.000026$. For each $i \geq 1$, we have

$$s_i = 2 \int_{2^{i-1}B/w}^{2^i B/w} g(2x)\, dx \leq 0.000026 \int_{2^{i-1}B/w}^{2^i B/w} g(x)\, dx = 0.000026 s_{i-1}.$$

Therefore, $s_i \leq (0.000026)^i s_0$ for all $i \geq 0$ and hence $C \leq \sum_{i=0}^{\infty} s_i \leq (1-0.000026)^{-1} s_0 \leq 1.00003 s_0$. Since $g(x)$ is decreasing for $x \geq 5m$ and $B/w \geq 5m$, we have $s_0 \leq g(B/w)B/w$ and hence $C \leq 1.00003 (B/w)^{24m+1} u_0^{B/w}$. By (9.1), we deduce that

$$\sum_{n=B}^{\infty} c_n u^{n/w} \leq 1.00003 u_0^{-1} w u^{B/w} (B/w)^{24m+1} \leq 230.8 w u^{B/w} (B/w)^{24m+1}$$

which proves (i).

We now assume that $mw \leq B < 5mw$. From part (i), in the special case $B = 5mw$, we have

$$\sum_{n=5mw}^{\infty} c_n u^{n/w} \leq 230.8 w u^{5m} (5m)^{24m+1} \leq 230.8 w u^{B/w} (5m)^{24m+1}. \tag{9.2}$$

We have

$$\sum_{n=B}^{5mw-1} c_n u^{n/w} \leq u^{B/w} \sum_{n=B}^{5mw-1} (n/w)^{24m} u^{(n-B)/w} \leq u^{B/w} (5m)^{24m} (5mw - mw).$$

So $\sum_{n=B}^{5mw} c_n u^{n/w} \leq 0.8 w u^{B/w} (5m)^{24m+1}$ and by combining with (9.2) we deduce (ii). □

Lemma 9.6. *Take any positive integer m and let $\sum_{n=m}^{\infty} a_n q^n$ be the q-expansion of Δ^m. Take any real number $0 \leq u \leq e^{-\pi\sqrt{3}}$.*

(i) *We have $|a_n| \leq 2n^{6m}$ for all $n \geq 2$.*
(ii) *For any integer $B > 2m$, we have $\sum_{n=B}^{\infty} |a_n| u^n \leq 463 u^B (B-1)^{6m+1}$.*
(iii) *For any integer $m < B \leq 2m$, we have $\sum_{n=B}^{\infty} |a_n| u^n \leq 465 u^B (2m)^{6m+1}$.*

Proof. In [Rou08], Rouse describes a constant C_m for which $|a_n| \leq C_m d(n) n^{(12m-1)/2}$ holds for all $n \geq m$; this follows from expressing Δ^m as a linear combination of Hecke eigenforms and using bounds of Deligne. When $m > 1$, an explicit upper bound for C_m is given in the proof of Theorem 1 in [Rou08] from which we find that $C_m \leq 1$. When $m = 1$, we have $C_m = 1$ as noted in the appendix of [Rou08]. Therefore, $|a_n| \leq d(n) n^{(12m-1)/2}$. We obtain $|a_n| \leq 2n^{6m}$ by using the easy bound $d(n) \leq 2\sqrt{n}$. This proves (i).

Define $u_0 := e^{-\pi\sqrt{3}}$. Define the function $g(x) = x^{6m} u_0^x$; it is decreasing for all $x \geq a := -6/\log(u_0) \cdot m = m \cdot 1.102\ldots$.

We first assume that $B \geq 2m$. Using (i) and $u \leq u_0$, we have

$$\sum_{n=B+1}^{\infty} |a_n| u^n \leq 2u^{B+1} \sum_{n=B+1}^{\infty} n^{6m} u_0^{n-B-1} = 2u^{B+1} u_0^{-B-1} C, \tag{9.3}$$

where $C := \sum_{n=B+1}^{\infty} g(n)$. Since $g(x)$ is decreasing for $x \geq B \geq 2m$, we have $C \leq \int_B^\infty g(x)\, dx = \sum_{i=0}^\infty s_i$, where $s_i := \int_{2^i B}^{2^{i+1}B} g(x)\, dx$. For $x \geq 2m$, we have $g(2x)/g(x) = 2^{6m} u_0^x \leq (2^6 u_0^2)^m \leq 0.0013$. For each $i \geq 1$, we have

$$s_i = 2 \int_{2^{i-1}B}^{2^i B} g(2x)\, dx \leq 0.0013 \int_{2^{i-1}B}^{2^i B} g(x)\, dx = 0.0013 s_{i-1}.$$

Therefore, $s_i \leq (0.0013)^i s_0$ for all $i \geq 0$ and hence $C \leq \sum_{i=0}^\infty s_i \leq (1-0.0013)^{-1} s_0 \leq 1.0014 s_0$. Since $g(x)$ is decreasing for $x \geq B \geq 2m$, we have $s_0 \leq g(B)B$ and hence $C \leq 1.0014 B^{6m+1} u_0^B$. By (9.3), we deduce that

$$\sum_{n=B+1}^{\infty} |a_n| u^n \leq 2 \cdot 1.0014 u_0^{-1} u^{B+1} B^{6m+1} \leq 463 u^{B+1} B^{6m+1}.$$

This implies (ii) after replacing B by $B-1$.

Now take any $m < B \leq 2m$. We have

$$\sum_{n=B}^{2m} |a_n| u^n \leq u^B \sum_{n=B}^{2m} |a_n| \leq u^B \cdot 2(2m)^{6m} \cdot (2m - B + 1) \leq u^B (2m)^{6m+1}.$$

From (ii), we have $\sum_{n=2m+1}^\infty |a_n| u^n \leq 463 u^{2m+1} (2m)^{6m+1}$. By adding these sums, we obtain $\sum_{n=B}^\infty |a_n| u^n \leq 464 u^B (2m)^{6m+1}$. □

10. Proof of Theorem 4.1

With $k := 12m$, fix a modular form $f \in M_{k,G} = M_{12m,G}$ as in Theorem 9.1. Define $\varphi := f/\Delta^m$. We have $\varphi \in K_G(X_G)$ by Lemma 6.2. We now state some basic properties of φ.

Lemma 10.1.

(i) *The function $\varphi \in K_G(X_G)$ is nonconstant and has no poles away from the cusps of X_G.*
(ii) *The q-expansion of $\varphi * A$ has coefficients in $\mathbb{Z}[\zeta_N]$ for each $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*
(iii) *For any cusp c of X_G, we have $\mathrm{ord}_c(\varphi) \geq -mw_c$.*
(iv) *For any cusp $c \in \Sigma$, φ is regular at c. Moreover, $\varphi(c)$ lies in $\mathbb{Z}[\zeta_N]$ and satisfies $|\varphi(c)|_v \leq \beta m^{24m}$ for any infinite places v of L.*
(v) *The rational function φ of X_G has at most $m\mu$ poles counted with multiplicity.*

Proof. With notation as in §8, we have $f \in W_m$ by our choice of f and hence $\varphi \in \mathscr{L}(D_1)$ by Lemma 8.1, where $D_1 := \sum_{c \in \mathcal{C}_G - \Sigma} mw_c \cdot c$. Since $\varphi \in \mathscr{L}(D_1)$, the function φ has no poles away from the cusps, $\mathrm{ord}_c\, \varphi \geq 0$ for all $c \in \Sigma$, and $\mathrm{ord}_c\, \varphi \geq -mw_c$ for all $c \in \mathcal{C}_G$. The function φ is nonconstant since $f \notin K_G \Delta^m$ by our choice of f. We have proved (i) and (iii). By (i) and (iii), the number of poles of φ is bounded above by $\sum_{c \in \mathcal{C}_G} mw_c = m\mu$, where the equality uses (2.1). This proves (v).

We now prove (ii). Since Δ^m lies in $q^m \cdot (1 + q\mathbb{Z}[\![q]\!])$ and $\varphi * A = (f * A)/(\Delta^m * A) = (f * A)/\Delta^m$, it suffices to show that the q-expansion of $f * A$ has coefficients in $\mathbb{Z}[\zeta_N]$ for any $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Take any $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Define the cusp $c := A \cdot c_\infty$ of X_G, where c_∞ is the cusp at infinity, and set $w = w_c$. By property (c) of Theorem 9.1, we have $f * A = \sum_{n=0}^\infty b_n q_w^n$ with $b_n \in \mathbb{Z}[\zeta_N]$. For any $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $f * (AB) = (f * A) * B = \sum_{n=0}^\infty \sigma_d(b_n) q_w^n \in \mathbb{Z}[\zeta_N][\![q_w]\!]$ by Lemma 6.1. This completes the proof of (ii) since any matrix in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is of the form AB for some $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$.

We finally prove (iv). Take any $c \in \Sigma$; we have already shown that φ is regular at c. Fix $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \cdot c_\infty = c$ and set $w = w_c$. We have $\nu_c(f) \geq mw$, so $f * A = \sum_{n=mw}^\infty b_n q_w^n$ with $b_n \in \mathbb{Z}[\zeta_N]$. We have $\Delta^m \in q^m \cdot (1 + q\mathbb{Z}[\![q]\!]) = q_w^{mw} \cdot (1 + q\mathbb{Z}[\![q]\!])$, so the constant term of the q-expansion of $\varphi = f * A/\Delta^m$ is b_{mw}. Therefore, $\varphi(c) = b_{mw}$ and in particular $\varphi(c) \in \mathbb{Z}[\zeta_N]$. For any infinite place v of L, we have $|\varphi(c)| = |b_{mw}| \leq \beta m^{2k} = \beta m^{24m}$ by Theorem 9.1(c). □

From the previous lemma, we have proved (b) and (c). The following lemma proves (a).

Lemma 10.2. *The function φ is the root of a monic polynomial with coefficients in $\mathbb{Z}[j]$.*

Proof. Define the polynomial $Q(x) = \prod_{A\in R}(x - \varphi * A)$, where R is a set of representatives of the right G-cosets of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Since φ is fixed by the right action of G on $\mathcal{F}_N$, we deduce that $Q(x)$ is independent of the choice of R and its coefficients lie in $\mathcal{F}_N^{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathbb{Q}(j)$.

By Lemma 10.1(i), the function φ has all of its poles at cusps. So for each $A \in R$, $\varphi * A$ has all of its poles at cusps. The coefficients of $Q(x)$ lie in $\mathbb{Q}(j)$ and have all of their poles at cusps as well. Therefore, the coefficients of $Q(x)$ lie in $\mathbb{Q}[j]$. The coefficients of $Q(x)$ all have q-expansions with integral coefficients by Lemma 10.1(ii). The lemma follows by noting that an element of $\mathbb{Q}[j]$ lies in $\mathbb{Z}[j]$ if and only if its q-expansion has integral coefficients (to see this use that $j = q^{-1} + 744 + 196884q + \cdots \in \mathbb{Z}(\!(q)\!)$). □

Now take any cusp $c \in \mathcal{C}_G$ and set $w = w_c$. Choose an $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \cdot c_\infty = c$. By property (c) of Theorem 9.1, we have $f * A = \sum_{n=0}^\infty b_n q_w^n$ with $b_n \in \mathbb{Z}[\zeta_N]$. We also have a q-expansion $\Delta^m = q^m \prod_{i=1}^\infty (1-q^n)^{24m} = \sum_{n=m}^\infty a_n q^n$ with $a_n \in \mathbb{Z}$.

Note that $\Delta^{-1} = q^{-1}h(q)$ with $h(x) := \prod_{n=1}^\infty (1-x^n)^{-24} \in \mathbb{Z}[\![x]\!]$. For later, we remark that a numerical computation shows that

$$|h(t^N)|_v \le \prod_{n=1}^\infty (1 - e^{-\pi\sqrt{3}n})^{-24} < 1.1104 \tag{10.1}$$

holds for any infinite place v of L and any $t \in \overline{L}_v$ with $|t|_v \le e^{-\pi\sqrt{3}/N}$. We now show that with respect to a place v of L, φ can be given by an explicit v-analytic expression on a neighborhood of c.

Lemma 10.3. *Take any place v of L and point $P \in \Omega_{c,v} - \{c\}$. Then there is a nonzero $t \in \overline{L}_v$ such that all the following hold:*

- *We have $|t|_v < 1$. If v is infinite, then $|t|_v \le e^{-\pi\sqrt{3}/N}$.*
- *We have*

$$\varphi(P) = t^{-mN} h(t^N)^m \sum_{n=0}^\infty b_n t^{nN/w} \tag{10.2}$$

  in $\overline{L}_v$.
- *If v is finite, we have $|j(P)|_v = |t|_v^{-N}$.*
- *If v is infinite and $|j(P)|_v > 3500$, we have $|t|_v^N \le 2|j(P)|_v^{-1}$.*

Proof. Denote by $\pi\colon X(N)_{\mathbb{Q}(\zeta_N)} \to (X_G)_{\mathbb{Q}(\zeta_N)}$ the natural morphism corresponding to the inclusion $\mathbb{Q}(\zeta_N)(X_G) \subseteq \mathcal{F}_N$ of function fields. By our definition of $\Omega_{c,v}$, there is a cusp c' of $X(N)$ and a point $P' \in \Omega_{c',v}$ such that $\pi(c') = c$ and $\pi(P') = P$. We have $P \ne c'$ since otherwise $P = c$. Since $\varphi \in K_G(X_G) \subseteq \mathbb{Q}(\zeta_N)(X(N))$, we can view φ as a rational function on $X(N)$ (equivalently, we denote $\varphi \circ \pi$ by φ as well). We have $\varphi(P) = \varphi(P')$ and $j(P) = j(P')$. So without loss of generality, we may assume that c is a cusp of $X(N)$, $P \in \Omega_{c,v} - \{c\} \subseteq X(N)(\overline{L}_v)$ and we may view φ as a function in $\mathbb{Q}(\zeta_N)(X(N)) = \mathcal{F}_N$.

We have

$$\varphi * A = \Delta^{-m}(f * A) = q^{-m} h(q)^m \sum_{n=0}^\infty b_n q_w^n = q_N^{-mN} h(q^N)^m \sum_{n=0}^\infty b_n q_N^{nN/w} \tag{10.3}$$

which when expanded is the q-expansion of φ. We claim that the radius of convergence of (10.2), viewed as a power series in $\overline{L}_v[\![q_N]\!]$, is at least 1. Since the coefficients of h and all the b_n are integral, the claim is immediate when v is finite. When v is infinite, the claim follows from the bounds on $|b_n|_v$ given by property (c) of Theorem 9.1.

For our fixed A, let $\psi_{A,v}\colon B_v \to X(N)(\overline{L}_v)$ be the continuous map from Proposition 3.1. By the definition of $\Omega_{c,v}$, we have $P = \psi_{A,v}(t)$ for some nonzero $t \in B_v$ that also satisfies $|t|_v \le e^{-\pi\sqrt{3}/N}$ when v is infinite. The v-analytic expression (10.2) thus holds by (10.3) and Proposition 3.1. By Proposition 3.1, we also have $j(P) = t^{-N} + 744 + 196884t^N + 21493760t^{2N} + \cdots$ in $\overline{L}_v$, where the coefficients are from the familiar q-expansion of j. When v is finite this implies that $|j(P)|_v = |t|_v^{-N}$. When v is infinite and $|j(P)|_v > 3500$, we have $|t|_v^N \le 2|j(P)|_v^{-1}$, cf. [BP11, Corollary 2.2]. □

We now assume that the cusp $c = A\cdot c_\infty$ lies in Σ. By Lemma 10.1(iv), φ is regular at c and $\varphi(c)\in\mathbb{Z}[\zeta_N]$. The function $\varphi-\varphi(c)$ lies in $\mathbb{Q}(\zeta_N)(X_G)$ and has a zero at c.

Fix an integer $1\le r\le \operatorname{ord}_c(\varphi-\varphi(c))$. Since $A\in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $(\varphi-\varphi(c))*A=\varphi*A-\varphi(c)=(f*A)/\Delta^m-\varphi(c)$. Since $r\le \operatorname{ord}_c(\varphi-\varphi(c))$, the q-expansion of $(f*A)/\Delta^m-\varphi(c)$ lies in $q_w^r\cdot\mathbb{Q}(\zeta_N)[\![q_w]\!]$ and hence the q-expansion of $f*A-\varphi(c)\Delta^m$ lies in $q_w^{mw+r}\cdot\mathbb{Q}(\zeta_N)[\![q_w]\!]$. Therefore,

$$f*A-\varphi(c)\Delta^m=\sum_{n=mw+r}^{\infty}b_nq_w^n-\varphi(c)\sum_{n\ge m+r/w}a_nq^n. \tag{10.4}$$

Take any place v of L and take any point $P\in\Omega_{c,v}-\{c\}$ that satisfies $|j(P)|_v>3500$ when v is infinite. Let $t\in\overline{L}_v$ be an nonzero element satisfying the conclusions of Lemma 10.3. We have

$$\begin{aligned}\varphi(P)-\varphi(c)&=t^{-mN}h(t^N)^m\sum_{n=0}^{\infty}b_nt^{nN/w}-\varphi(c)\\&=t^{-mN}h(t^N)^m\Big(\sum_{n=mw+r}^{\infty}b_nt^{nN/w}-\varphi(c)\sum_{n\ge m+r/w}a_nt^{nN}\Big),\end{aligned}\tag{10.5}$$

where we have used $\Delta^{-m}=q^{-m}h(q)^m$ along with (10.4) which ensures early terms of our sums will cancel. Therefore,

$$\varphi(P)-\varphi(c)=t^{rN/w}h(t^N)^m\Big(\sum_{n=mw+r}^{\infty}b_nt^{(n-mw-r)N/w}-\varphi(c)\sum_{n\ge m+r/w}a_nt^{(n-m-r/w)N}\Big).\tag{10.6}$$

Consider the case where v is finite. From (10.6), we have $\varphi(P)-\varphi(c)=t^{rN/w}g(t)$, where g is a power series with coefficients in $\mathbb{Z}[\zeta_N]$. Therefore, $|\varphi(P)-\varphi(c)|_v\le |t|_v^{rN/w}=|j(P)|_v^{-r/w}$. We obtain $|\varphi(P)-\varphi(c)|_v\le |j(P)|_v^{-1/w}$ by taking $r=1$. This proves (d) in the case that v is finite.

Now suppose that v is infinite and take $r=1$. Starting with (10.5) and taking absolute values gives

$$|\varphi(P)-\varphi(c)|_v\le u^{-m}|h(t^N)|_v^m\Big(\sum_{n=mw+1}^{\infty}|b_n|_vu^{n/w}+|\varphi(c)|_v\sum_{n=m+1}^{\infty}|a_n|u^n\Big),\tag{10.7}$$

where $u:=|t|_v^N\le e^{-\pi\sqrt3}$. Using our bound $|b_n|_v\le\beta(n/w)^{24m}$ for $n\ge mw$, Lemma 9.5(ii) with $B=mw+1$ implies that

$$u^{-m}\sum_{n=mw+1}^{\infty}|b_n|_vu^{n/w}\le\beta\cdot u^{1/w}\cdot 231.6w(5m)^{24m+1}.$$

By Lemma 9.6(iii) with $B=m+1$, we have $u^{-m}\sum_{n=m+1}^{\infty}|a_n|u^n\le 465u(2m)^{6m+1}$ and hence

$$u^{-m}|\varphi(c)|_v\sum_{n=m+1}^{\infty}|a_n|u^n\le\beta\cdot u\cdot 465\cdot 2^{6m+1}m^{30m+1}$$

by Lemma 10.1(iv). We have $|h(t^N)|_v<1.1104$ by (10.1). Combining the above bounds with (10.7) gives

$$\begin{aligned}|\varphi(P)-\varphi(c)|_v&\le\beta\cdot 1.1104^m(u^{1/w}\cdot 231.6w(5m)^{24m+1}+u\cdot 465\cdot 2^{6m+1}m^{30m+1})\\&\le u^{1/w}\beta w\cdot 1.1104^m(231.6(5m)^{24m+1}+465\cdot 2^{6m+1}m^{30m+1})\\&\le u^{1/w}\beta w\cdot 1.1104^m(231.6\cdot 5^{24m+1}+465\cdot 2^{6m+1})m^{30m+1}\\&=u^{1/w}\beta w\cdot 1.1104^m1158\cdot 5^{24m}(1+\tfrac{465}{231.6}\cdot\tfrac{2}{5}\cdot(\tfrac{2^6}{5^{24}})^m)m^{30m+1}\\&\le u^{1/w}\beta C_0/2,\end{aligned}$$

where $C_0:=N\cdot 2\cdot 1159\cdot 5.022^{24m}m^{30m+1}$. Since $u^{1/w}\le 1$, we deduce that $|\varphi(P)-\varphi(c)|_v\le\beta C_0/2$. Now assume further that $|j(P)|_v>3500$. We have $u=|t|_v^N\le 2|j(P)|_v^{-1}$ by Lemma 10.3 and our of choice of t. So $u^{1/w}\le(2|j(P)|_v^{-1})^{1/w}\le 2|j(P)|_v^{-1/w}$ and hence $|\varphi(P)-\varphi(c)|_v\le|j(P)|_v^{-1/w}\cdot\beta C_0$.

To complete the proof of (d) in the case that v is infinite, it suffices to show that $C_0 \le C$. Since $m \le \frac{1}{24}N^3$ by Lemma 4.2, we have

$$C_0 \le 2 \cdot 1159 \cdot 5.022^{24m}(\tfrac{1}{24})^{30m+1}N^{90m+4} \le 96.6 \cdot 0.1^{24m}N^{90m+4} = C.$$

It remains to prove (e). Let K be any number field with $K_G \subseteq K \subseteq L$ and let Σ' be a Gal_K-orbit of Σ. We keep notation as above with a fixed cusp $c \in \Sigma' \subseteq \Sigma$ and we take $r = \mathrm{ord}_c(\varphi - \varphi(c))$. We further assume that $\varphi(c) \in K$; if no such c exists then (e) holds trivially with $\xi = 1$. Since the divisor of $\varphi - \varphi(c)$ has degree 0, we have $r \le m\mu$ by Lemma 10.1(v).

We have $f * A - \varphi(c)\Delta^2 = \gamma q_w^{mw+r} + \cdots$ with $\gamma \in \mathbb{Z}[\zeta_N]$ nonzero. From (10.4), we find that

$$\gamma = \begin{cases} b_{mw+r} - \varphi(c)a_{m+r/w} & \text{if } w|r, \\ b_{mw+r} & \text{if } w \nmid r. \end{cases} \tag{10.8}$$

The rational function $h := (\varphi - \varphi(c))^w j^r$ lies in $K(X_G)$ and we have $\mathrm{ord}_c\, h = wr - rw = 0$. Moreover, $h(c) = \gamma^w$. Since h is defined over K, we have $\gamma^w = h(c) \in K(c)$. Define

$$\xi := N_{K(c)/K}(\gamma^w) \in K.$$

We have $\xi \in \mathcal{O}_K$ since γ is integral. We have $\xi \neq 0$ since $\gamma \neq 0$.

We will prove that (e) holds with this particular ξ. Since $\varphi(c)$ lies in K, by assumption, and φ is defined over K, we deduce that $\varphi(c') = \varphi(c) \in K$ for all $c' \in \Sigma'$. We also have $K(c') = K(c)$ and $w_{c'} = w_c$ for all $c \in \Sigma'$ since Σ' has a transitive $\mathrm{Gal}(L/K)$-action and $K(c)/K$ is abelian. Therefore, $h(c) = \gamma^w$ and $\xi = N_{K(c)/K}(\gamma^w)$ are independent of the choice of $c \in \Sigma'$. So for the rest of the proof we can work with our fixed cusp c.

We now find upper bounds for $|\gamma|_v$ for some places v of L. Define $C' := 22.16N^{144m+7}0.024^{24m}$.

Lemma 10.4. *For any infinite place v of L, we have $|\gamma|_v \le \beta C'$.*

Proof. Take any infinite place v of L. By Theorem 9.1(c) and $r \le m\mu$, we have

$$|b_{mw+r}|_v \le \beta(m + r/w)^{24m} \le \beta m^{24m}(1+\mu)^{24m}.$$

If w divides r, Lemma 9.6(i) and $r \le m\mu$ implies that $|a_{m+r/w}| \le 2(m+r/w)^{6m} \le 2m^{6m}(1+\mu)^{6m}$ and hence

$$|\varphi(c)a_{m+r/w}|_v \le \beta \cdot 2m^{30m}(1+\mu)^{6m}$$

by Lemma 10.1(iv). Using these bounds with (10.8), we obtain

$$|\gamma|_v \le \beta m^{24m}(1+\mu)^{24m} + \beta \cdot 2m^{30m}(1+\mu)^{6m}.$$

Using the bounds on m and $\mu + 1$ from Lemma 4.2, we obtain

$$\begin{aligned} |\gamma|_v &\le \beta((\tfrac{1}{24} \cdot \tfrac{29}{54})^{24m}N^{144m} + 2(\tfrac{1}{24})^{30m}(\tfrac{29}{54})^{6m}N^{108m}) \\ &= \beta N^{144m}(\tfrac{1}{24} \cdot \tfrac{29}{54})^{24m}(1 + 2(\tfrac{1}{24})^{6m}(\tfrac{54}{29})^{18m}N^{-36m}) \\ &\le \beta N^{144m}(\tfrac{1}{24} \cdot \tfrac{29}{54})^{24m}(1 + 2(\tfrac{1}{24}(\tfrac{54}{29})^3 3^{-6})^{6m}), \end{aligned}$$

where in the last inequality we have used that $N \ge 3$. Since $\frac{1}{24}(\frac{54}{29})^3 3^{-6} \le 1$, we have $|\gamma|_v \le \beta N^{144m}(\frac{1}{24} \cdot \frac{29}{54})^{24m}(1 + 2(\frac{1}{24}(\frac{54}{29})^3 3^{-6})^6)$. It is now easy to verify that $|\gamma|_v \le \beta C'$. ∎

Lemma 10.5. *Consider any point $P \in Y_G(K)$ that satisfies $\varphi(P) = \varphi(c)$ and $P \in \Omega_{c,v}$ for some place v of L. Further suppose that $|j(P)|_v > 3500$ when v is infinite. Then*

$$|\gamma|_v \le \begin{cases} |j(P)|_v^{-1} & \textit{if } v \textit{ is finite,} \\ |j(P)|_v^{-1} \cdot \beta C' & \textit{if } v \textit{ is infinite and } |j(P)|_v > 3500. \end{cases}$$

Proof. Using equation (10.5) and $\varphi(P) - \varphi(c) = 0$, we obtain

$$0 = \gamma + t^{-(mw+r)N/w} \sum_{n=mw+r+1}^{\infty} b_n t^{nN/w} - \varphi(c) t^{-(mw+r)N/w} \sum_{n > m+r/w} a_n t^{nN}, \tag{10.9}$$

with $t \in \overline{L}_v$ satisfying $|t|_v < 1$. If v is finite, we also have $|j(P)|_v = |t|_v^{-N}$. If v is infinite, we also have $|t|_v \le e^{-\pi\sqrt{3}/N}$ and $|t|_v^N \le 2|j(P)|_v^{-1}$. In particular, $\gamma = t^{N/w}g(t)$ in $\overline{L}_v$ for some power series $g(x)$ with coefficients in $\mathbb{Z}[\zeta_N]$. So when v is finite, we have $|\gamma|_v = |t|_v^{N/w}|g(t)|_v \le |t|_v^{N/w} = |j(P)|_v^{-1/w}$.

We can now assume that v is infinite. Define $u = |t|_v^N$; we have $u \le e^{-\pi\sqrt{3}}$. Solving for γ in (10.9) and taking absolute values, we obtain

$$|\gamma|_v \le u^{-(mw+r)/w}\, s_1 + |\varphi(c)|_v u^{-(mw+r)/w}\, s_2, \tag{10.10}$$

where $s_1 := \sum_{n=mw+r+1}^{\infty} |b_n|_v u^{n/w}$ and $s_2 := \sum_{n>m+r/w} |a_n| u^n$. Using Lemma 9.5 with $B = mw+r+1$ and our bound $|b_n| \le \beta \max\{1,(n/w)^{24m}\}$, we have

$$\begin{aligned} u^{-(mw+r)/w}s_1 &\le \beta \cdot 231.6wu^{1/w}\max\{(mw+r+1)/w, 5m\}^{24m+1} \\ &\le u^{1/w}\beta \cdot 231.6Nm^{24m+1}\max\{\mu+2,5\}^{24m+1}, \end{aligned}$$

where the last inequality uses $1 \le w \le N$ and $r \le m\mu$. Using the bounds on m and $\mu+2$ from Lemma 4.2, we obtain

$$u^{-(mw+r)/w}s_1 \le u^{1/w}\beta \cdot 231.6N^{144m+7}(\tfrac{1}{24}\cdot\tfrac{31}{54})^{24m+1} \le u^{1/w}\beta \cdot 5.54N^{144m+7}0.024^{24m}.$$

Let B be the smallest integer for which $B > m + r/w$. By Lemma 9.6, we have

$$\begin{aligned} s_2 &\le 465u^B \max\{m+r/w, 2m\}^{6m+1} \\ &\le 465u^{m+r/w+1/w}m^{6m+1}\max\{1+\mu,2\}^{6m+1}, \end{aligned}$$

where in the last inequality we have used that $u < 1$, $B \ge m + r/w + 1/w$, and $r/w \le r \le m\mu$. So by Lemma 10.1(iv),

$$|\varphi(c)|_v u^{-(mw+r)/w}s_2 \le u^{1/w}\beta \cdot 465m^{30m+1}\max\{1+\mu,2\}^{6m+1}.$$

Using the bounds on m and $\mu+1$ from Lemma 4.2, we obtain

$$\begin{aligned} |\varphi(c)|_v u^{-(mw+r)/w}s_2 &\le u^{1/w}\beta \cdot 465N^{108m+6}(\tfrac{1}{24})^{30m+1}(\tfrac{29}{54})^{6m+1} \\ &\le u^{1/w}\beta \cdot 10.41N^{108m+6}0.0162^{24m}. \end{aligned}$$

In particular, $|\varphi(c)|_v u^{-(mw+r)/w}s_2 \le u^{1/w}\beta \cdot 5.54N^{144m+7}0.024^{24m}$ since $N \ge 3$.

Thus from (10.10) and the above bounds, we have

$$|\gamma|_v \le 2\cdot u^{1/w}\beta \cdot 5.54N^{144m+7}0.024^{24m} = u^{1/w}\beta C'/2.$$

Since $u^{1/w} = |t|_v^{N/w} \le (2|j(P)|_v^{-1})^{1/w} \le 2|j(P)|_v^{1/w}$, we conclude that $|\gamma|_v \le |j(P)|_v^{1/w}\beta C'$. □

We have $\gamma^w \in K(c)$. For any place v of L, we have

$$|\xi|_v = \prod_{\sigma\in \mathrm{Gal}(K(c)/K)} |\sigma(\gamma^w)|_v.$$

Since the action of $\mathrm{Gal}(K(c)/K)$ on Σ' is transitive and $c \in \Sigma'$, we have $|\mathrm{Gal}(K(c)/K)| = |\Sigma'|$.

Suppose that v is infinite. We have $|\sigma(\gamma^w)|_v \le (\beta C')^w$ for all $\sigma \in \mathrm{Gal}(K(c)/K)$ by Lemma 10.4; note that the lemma holds for an arbitrary infinite place. Therefore,

$$|\xi|_v \le (\beta C')^{w|\mathrm{Gal}(K(c)/K)|} = (\beta C')^{w|\Sigma'|}.$$

Now suppose further that $|j(P)|_v > 3500$ and that there is a point $P \in Y_G(K)$ for which $\varphi(P) = \varphi(c)$ and $P \in \Omega_{c,v}$. By Lemma 10.5, we have $|\gamma^w|_v \le |j(P)|_v^{-w}(\beta C')^w$. Therefore,

$$|\xi|_v \le (\beta C')^{w(|\mathrm{Gal}(K(c)/K)|-1)}|\gamma^w|_v \le |j(P)|_v^{-w}(\beta C')^{w|\mathrm{Gal}(K(c)/K)|} = |j(P)|_v^{-w}(\beta C')^{w|\Sigma'|}.$$

Finally suppose that v is finite and that there is a point $P \in Y_G(K)$ for which $\varphi(P) = \varphi(c)$ and $P \in \Omega_{c,v}$. Since γ is integral, we have $|\sigma(\gamma^w)|_v \le 1$ for all $\sigma \in \mathrm{Gal}(K(c)/K)$. Therefore, $|\xi|_v \le |\gamma^w|_v$. By Lemma 10.5, we conclude that $|\xi|_v \le |j(P)|_v^{-w}$.

References

[Bil95] Yuri Bilu, *Effective analysis of integral points on algebraic curves*, Israel J. Math. **90** (1995), no. 1-3, 235–252. MR1336325 ↑iii

[BP11] Yuri Bilu and Pierre Parent, *Runge's method and modular curves*, Int. Math. Res. Not. IMRN **9** (2011), 1997–2027. MR2806555 ↑1, 1.1, 3.3, 10

[BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774 ↑1

[Bru17] François Brunault, *Régulateurs modulaires explicites via la méthode de Rogers-Zudilin*, Compos. Math. **153** (2017), no. 6, 1119–1152 (French, with English and French summaries). MR3705252 ↑6.4

[BN19] François Brunault and Michael Neururer, *Fourier expansions at cusps*, The Ramanujan Journal (2019). ↑6.2, 6.4, 6.5

[Cai22] Yulin Cai, *An explicit bound of integral points on modular curves*, Commun. Math. **30** (2022), no. 1, 161–174. MR4450724 ↑iii

[CP03] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2,\mathbb{Z})$ *of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. ↑v, 4

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349, Springer, Berlin-New York, 1973, pp. 143–316 (French). MR337993 ↑2.4, 3.1

[Fal91] Gerd Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), no. 3, 549–576. MR1109353 ↑9.1

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290 (English, with English and French summaries). Cohomologies p-adiques et applications arithmétiques. III. MR2104361 ↑6.4

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. ↑6.5

[KM12] Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748. MR2904927 ↑6.5

[Koo93] Robert Jan Kooman, *Faltings's version of Siegel's lemma*, Diophantine approximation and abelian varieties (Soesterberg, 1992), Lecture Notes in Math., vol. 1566, Springer, Berlin, 1993, pp. 93–96. MR1289008 ↑9.1

[LF19] Samuel Le Fourn, *A tubular variant of Runge's method in all dimensions, with applications to integral points on Siegel modular varieties*, Algebra Number Theory **13** (2019), no. 1, 159–209. MR3917917 ↑1

[Rou08] Jeremy Rouse, *Bounds for the coefficients of powers of the* Δ*-function*, Bull. Lond. Math. Soc. **40** (2008), no. 6, 1081–1090. MR2471957 ↑9.2

[Sch08] René Schoof, *Catalan's conjecture*, Universitext, Springer-Verlag London, Ltd., London, 2008. MR2459823 ↑1

[Sha14] Min Sha, *Bounding the j-invariant of integral points on modular curves*, Int. Math. Res. Not. IMRN **16** (2014), 4492–4520. MR3250041 ↑iii

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. ↑2.1, 4, 5, 6, 8

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 ↑3.1

[Zyw24] David Zywina, *Explicit open images for elliptic curves over* $\mathbb{Q}$ (2024). arXiv:2206.14959 [math.NT]. ↑2.4, 3.1, 6.7

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: zywina@math.cornell.edu