MODULAR CURVES AND RAMANUJAN'S CONTINUED FRACTION

BRYDEN CAIS AND BRIAN CONRAD

Abstract. We use arithmetic models of modular curves to establish some properties of Ramanujan's continued fraction. In particular, we give a new geometric proof that its singular values are algebraic units that generate specific abelian extensions of imaginary quadratic fields, and we use a mixture of geometric and analytic methods to construct and study an infinite family of two-variable polynomials over $\mathbf{Z}$ that are related to Ramanujan's function in the same way that the classical modular polynomials are related to the classical j-function. We also prove that a singular value on the imaginary axis, necessarily real, lies in a radical tower in $\mathbf{R}$ only if all odd prime factors of its degree over $\mathbf{Q}$ are Fermat primes; by computing some ray class groups, we give examples where this necessary condition is not satisfied.

1. Introduction

Let $\mathbf{C}$ be an algebraic closure of $\mathbf{R}$. For $\tau \in \mathbf{C} - \mathbf{R}$, let $q_\tau = e^{2\pi i_\tau \tau}$ with $i_\tau^2 = -1$ and i_τ in the connected component of τ in $\mathbf{C} - \mathbf{R}$, so $|q_\tau| < 1$ and $q_\tau = q_{-\tau}$.

The *Ramanujan continued fraction* $F : \mathbf{C} - \mathbf{R} \to \mathbf{C}$ is

$$F(\tau) := \frac{q_\tau^{1/5}}{1+}\;\frac{q_\tau}{1+}\;\frac{q_\tau^2}{1+}\;\frac{q_\tau^3}{1+}\;\cdots.$$

where q_τ^r means $e^{2\pi i_\tau r\tau}$ for $r \in \mathbf{Q}$. Note that $F(\tau) = F(-\tau)$. In his 1916 letter to Hardy, Ramanujan stated the remarkable identities

$$F(i) = \frac{e^{-2\pi/5}}{1+}\;\frac{e^{-2\pi}}{1+}\;\frac{e^{-4\pi}}{1+}\;\frac{e^{-6\pi}}{1+}\;\frac{e^{-8\pi}}{1+}\;\cdots = \sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2} \tag{1.1}$$

and

$$F\left(\frac{5}{2}+i\right) = \frac{-\,e^{-\pi/5}}{1+}\;\frac{-\,e^{-\pi}}{1+}\;\frac{e^{-2\pi}}{1+}\;\frac{-\,e^{-3\pi}}{1+}\;\cdots = -\sqrt{\frac{5-\sqrt{5}}{2}} + \frac{\sqrt{5}-1}{2} \tag{1.2}$$

for any $i \in \mathbf{C}$ satisfying $i^2 + 1 = 0$, and he asserted that if $\tau \in \mathbf{C} - \mathbf{R}$ satisfies $\tau^2 \in \mathbf{Q}$, then "$F(\tau)$ can be exactly found."

Watson [21] proved (1.1) and (1.2) as consequences of the identity

$$\frac{1}{F(\tau)} - 1 - F(\tau) = \frac{\eta(\tau/5)}{\eta(5\tau)}, \tag{1.3}$$

Date: April 21, 2004.

1991 *Mathematics Subject Classification.* Primary 11F03; Secondary 14G35.

Key words and phrases. q-series, modular curve, Ramanujan continued fraction.

The second author was supported by the NSF and the Sloan Foundation. The authors thank K. Conrad for providing us with a proof of Lemma D.1 and thank William Stein for his publically available computer cluster Meccah that was used for the numerical computations. We are also greatly indebted to James Parson for many enlightening and insightful discussions concerning Appendix C..

where $\eta(\tau) \stackrel{\text{def}}{=} q_\tau^{1/24} \prod_{n=1}^{\infty}(1-q_\tau^n)$ is the Dedekind η-function, and he proved that $F(\tau)$ is an algebraic integer when $\tau \in \mathbf{C} - \mathbf{R}$ is quadratic over $\mathbf{Q}$. Using Watson's identity and an integrality result of Stark's on L-functions at $s = 1$, in [1, Thm. 6.2] it is shown that $F(\tau)$ is an algebraic integral unit for such τ. Ramanujan formulated other modular equations satisfied by F, and there has been a lot of research (for example, see [1], [9], [23], and [24], as well as [2] for an overall survey) investigating these (and other) explicit equations and using them to explicitly compute F at specific imaginary quadratic points in $\mathbf{C} - \mathbf{R}$, making creative use of Watson's identity and its variants.

In [8], Watson's identity is used to show that F is a level-5 modular function, and by determining the minimal polynomial of F over $\mathbf{Q}(j)$, it is proved that $\mathbf{Q}(F)$ is the field of modular functions of level-5 having Fourier expansion at ∞ with rational coefficients (this was already known to Klein [7, vol. 2, p. 383], who described F as a ratio of theta-functions). They employ Shimura reciprocity to describe the Galois conjugates of singular values $F(\tau)$ at quadratic imaginary $\tau \in \mathbf{C} - \mathbf{R}$ and thereby provide an algorithm to compute the minimal polynomial (over $\mathbf{Q}$) of any such singular value. Using standard Kummer theory (and the fact that $F(\tau)$ lies in an abelian—hence solvable—extension of $K = \mathbf{Q}(\tau)$), they show how to compute radical formulae for $F(\tau)$, thereby settling (in the affirmative) Ramanujan's claim that that the singular values of F on the imaginary axis can be "exactly found."

In this paper, we work with the function $j_5 = 1/F$; as is well-known, this is a level-5 modular function with a unique simple pole at the cusp $\infty \in X(5)$, so it defines an isomorphism $j_5 : X(5) \simeq \mathbf{CP}^1$. At the end of §4 we will recall a proof of this fact which does not rest on the crutch of Watson's identity. Our aim is to deduce additional properties of j_5 (and hence of F) by means of the good behavior of j_5 with respect to certain standard canonical integral models for $X(5)$ over $\mathbf{Z}[1/5]$ and $\mathbf{Z}[\zeta_5]$ that we describe in §2; since $\mathbf{Z}[1/5] \cap \mathbf{Z}[\zeta_5] = \mathbf{Z}$, we will also be able to obtain results over $\mathbf{Z}$.

In §3–§4 we quickly review Shimura's canonical models for modular curves and some properties of Klein forms, and in §5 we use Klein forms and arithmetic models of modular curves to construct an integral model J_5 for j_5 on the model $X(5)_{\mathbf{Z}[\zeta_5]}$ and to show that the rational function J_5 has both its zero and polar loci supported in the subscheme of cusps over $\mathbf{Z}[\zeta_5]$ (a contrast with the classical j-function on $X(1)$ over $\mathbf{Z}$). From this we obtain a new geometric proof that the values of j_5 (or Ramanujan's F) at CM-points are algebraic integral units (see Corollary 5.6). An easy application of Shimura's reciprocity law on canonical models implies that for an arbitrary $\tau \in \mathbf{C} - \mathbf{R}$ that is quadratic over $\mathbf{Q}$, the extension $\mathbf{Q}(\tau, j_5(\tau))/\mathbf{Q}(\tau)$ is an *abelian* extension of $K = \mathbf{Q}(\tau)$ that is unramified away from 5; we give the associated open subgroup in the idele class group $\mathbf{A}_K^\times/K^\times$ in Corollary 5.7. (Such a description is not included in [8].) For example, we shall see that if the elliptic curve $\mathbf{C}^\times/q_\tau^{\mathbf{Z}}$ has CM-order $\mathscr{O}_\tau \subseteq \mathscr{O}_K$ and τ is 5-integral, then $K(j_5(\tau))$ is contained in the ray class field of conductor $5 \cdot [\mathscr{O}_K : \mathscr{O}_\tau]$ for K, and if moreover τ is a 5-unit and $\mathscr{O}_\tau = \mathscr{O}_K$ then $K(j_5(\tau))$ is the ray class field of conductor 5 for K. In particular, this latter ray class field is always generated by a singular value of Ramanujan's function F.

A further application of the algebro-geometric link with modular curves is pursued in §6: for all n relatively prime to 5, we construct primitive polynomials $F_n \in \mathbf{Z}[X, Y]$ that are absolutely irreducible over $\mathbf{Q}$ and satisfy $F_n(j_5(\tau), j_5(n\tau)) = 0$. These F_n's for very small n have appeared in the literature on a case-by-case basis, and their existence in general was known to Klein long ago, but there does not seem to have been a systematic construction given before for all n relatively prime to 5 in a manner that is well-adapted to a study of algebraic properties (such as absolute irreducibility over $\mathbf{Q}$). We also establish an analogue of Kronecker's congruence for $F_p \bmod p$, but the shape of the congruence depends on $p \bmod 5$. It seems worth emphasizing that geometry can establish such congruences only up to a unit scaling factor; to eliminate the unit ambiguity, it is essential to bring in the analytic perspective via q-expansions. Similarly, the symmetry $\Phi_n(Y, X) = \Phi_n(X, Y)$ for the classical level-n modular polynomial has an analogue for F_n when $\gcd(n, 5) = 1$, as we show in §6, and geometric methods prove the result up to a factor in $\mathbf{Z}^\times = \{\pm 1\}$; we need q-expansions to determine the sign. Explicitly, if $n \equiv \pm 1 \bmod 5$ then F_n is symmetric, but if $n \equiv \pm 2 \bmod 5$ then $X^{\deg_Y F_n} F_n(Y, -1/X) = \varepsilon_n F_n(X, Y)$ for a sign ε_n that depends on n in a slightly complicated manner; for example, if $n = p$ is an odd prime congruent to ± 2 mod 5 then $\varepsilon_n = 1$, and $\varepsilon_n = -1$ for $n = 2, 32, 72, \ldots$ (see Theorem 6.5).

One virtue of computing the F_n's for many n's is that we thereby noticed that F_n has remarkably small coefficients; we give a list of F_n's for $n \leq 27$ in Appendix C. The reason for such smallness of coefficients is that the q-expansion of j_5 has small coefficients, and in §7 we provide an estimate on the coefficients of j_5 that is obtained by adapting the circle-method arguments of Rademacher for the usual j-function. In [4], P. Cohen established asyptotic estimates on the maximal absolute value of a coefficient of the classical level-n modular polynomial Φ_n (as $n \to \infty$), and in §7 we also give a variant on this method that applies to the F_n's when $\gcd(n, 5) = 1$. One consequence of these estimates is that, as $n \to \infty$, the largest coefficient for F_n (in absolute value) is approximately the 60th root of the largest coefficient for Φ_n. This explains the apparent smallness of the coefficients of the F_n's in examples with $(n, 5) = 1$.

We conclude in §8 by addressing the question of whether a singular value $j_5(\tau)$ can be expressed in radicals *inside of* $\mathbf{R}$ when $\tau^2 \in \mathbf{Q}$. For example, one may wish to interpret Ramanujan's assertion that $j_5(\tau)$ can always be "exactly found" when $\tau^2 \in \mathbf{Q}$ as saying that $j_5(\tau) \in \mathbf{R}$ lies in a radical tower of subfields of $\mathbf{R}$ for such τ. All previously published explicit radical formulas for such real singular values do satisfy this condition, but we will show (in Theorem 8.5) that these many examples are exceptions to the rule: if $\tau^2 \in \mathbf{Q}$ and $j_5(\tau)$ lies in a radical tower in $\mathbf{R}$ then all odd prime factors of $[\mathbf{Q}(j_5(\tau)) : \mathbf{Q}]$ are Fermat primes (we can only prove the converse in the easy case when $[\mathbf{Q}(j_5(\tau)) : \mathbf{Q}]$ is a power of 2, and the *casus irreducibilis* suggests that the converse is probably not true in general). This is a *very restrictive* necessary condition for the existence of a radical formula in $\mathbf{R}$, and it applies (with the same proof) to singular values of the usual j-function on the imaginary axis. In all published examples of radical formulas for singular values of j_5 on the imaginary axis, the degree of the singular value over $\mathbf{Q}$ has been of the form 2^e, $2^e \cdot 3$, or $2^e \cdot 5$; this Fermat criterion is not satisfied for $j_5(\sqrt{-101})$ (see Example 8.4), so the stronger interpretation of Ramanujan's claim using real radical towers is false. For $\tau^2 = q \in \mathbf{Q}$ with the height of q growing to ∞, it seems certain that in the asymptotic sense the necessary Fermat criterion fails to be satisfied 100% of the time.

Notation. The notation we use is standard, but we record one mild abuse of notation: we write G rather than the customary $\underline{G}$ to denote the constant group scheme associated to an abstract group G (when working over a base scheme S that will always be understood from context). This is most commonly used in the case $G = \mathbf{Z}/n\mathbf{Z}$ for a positive integer n.

2. Arithmetic models and analytic models of modular curves

In this section we summarize some basic definitions and theorems in the arithmetic theory of modular curves, and we link it up with the analytic models that are obtained as quotients of $\mathbf{C} - \mathbf{R}$. Everything we say in this section is well-known.

Pick a positive integer N. We will begin our work with level-N moduli problems over the ring of integers $\mathbf{Z}[\zeta_N]$ of a splitting field $\mathbf{Q}(\zeta_N)$ of the Nth cyclotomic polynomial, with ζ_N a choice of root of this polynomial. In [10], Katz and Mazur use Drinfeld level structures to develop a systematic theory of elliptic-curve moduli problems over integer rings (so they can study N-torsion moduli even if N is not a unit on the base scheme); unfortunately, this work omits a treatment of the modular interpretation of the cusps. The earlier work of Deligne and Rapoport [5] required the level to be invertible on the base (*i.e.*, to study moduli of N-torsion level structures, they required the base scheme to live over $\operatorname{Spec} \mathbf{Z}[1/N]$) but it introduced the theory of generalized elliptic curves to provide a modular interpretation along the cusps.

Example 2.1. Let n be a positive integer and S a scheme. Consider a set of n copies of $\mathbf{P}^1_S$ indexed by $\mathbf{Z}/n\mathbf{Z}$. Let C_n be the S-scheme obtained by gluing 0 on the ith copy of $\mathbf{P}^1_S$ to ∞ on the $(i+1)$th copy of $\mathbf{P}^1_S$; when $n = 1$ this is the nodal plane cubic $Y^2 + XY = X^3$. We call C_n the *standard Néron n-gon* over S.

The S-smooth locus C_n^{sm} is naturally identified with $\mathbf{G}_m \times (\mathbf{Z}/n\mathbf{Z})$, and with this evident S-group structure there is a unique action of C_n^{sm} on C_n extending the group law on C_n^{sm}. Equipped with this data, C_n is a generalized elliptic curve. Observe that the n-torsion in C_n^{sm} is naturally isomorphic to $\mu_n \times (\mathbf{Z}/n\mathbf{Z})$.

In [5, II, 1.15], it is proved that a generalized elliptic curve over an algebraically closed field must be isomorphic to either a smooth elliptic curve or to a standard Néron polygon.

The works of Deligne–Rapoport and Katz–Mazur can be combined, and hence it makes sense to consider the moduli functor that classifies *full level-N structures* on generalized elliptic curves: these are pairs (E, ι) where E is a generalized elliptic curve over an arbitrary scheme S and $\iota : (\mathbf{Z}/N\mathbf{Z})^2 \to E^{\mathrm{sm}}(S)[N]$ is a Drinfeld $(\mathbf{Z}/N\mathbf{Z})^2$-structure on the smooth separated S-group E^{sm}. Such an ι is called *S-ample* (or *ample*) if its image meets all irreducible components of all geometric fibers of E over S. If E admits a full level-N structure, then its non-smooth geometric fibers must have number of sides divisible by N and $E^{\mathrm{sm}}[N]$ must be a finite locally free S-group with order N^2. In this case, there is a functorial alternating μ_N-valued self-duality e_N on the N-torsion, and for any ι as above it is automatic (essentially by [10, 10.4.1]) that $\zeta = e_N(\iota(1,0), \iota(0,1)) \in \mu_N(S)$ is a root of the Nth cyclotomic polynomial. We say that (E, ι) is of *type* ζ.

The synthesis of the above work of Katz–Mazur and Deligne–Rapoport is (partly) summarized in the next two theorems (see [10, 10.9.1, 10.9.6-7] for proofs, and note that the theory of level structures in [10, Ch. 1] applies to the smooth locus of a generalized elliptic curve):

Theorem 2.2. *Let N be a positive integer. There exists a coarse moduli scheme $X(N)^{\mathrm{can}}$ over* $\operatorname{Spec} \mathbf{Z}[\zeta_N]$ *for the moduli functor that classifies generalized elliptic curves equipped with an ample full level-N structure of type ζ_N. This moduli scheme is normal, proper, and flat over* $\operatorname{Spec} \mathbf{Z}[\zeta_N]$*, and its fibers are geometrically connected with pure dimension* 1*. It is smooth away from the supersingular geometric points in characteristics dividing N, and when $N \geq 3$ it is a fine moduli scheme over* $\mathbf{Z}[1/N]$.

The second theorem we require from [5] and [10] concerns the formal structure along the subscheme of cusps in $X(N)^{\mathrm{can}}$. There is an elegant abstract technique for defining such a subscheme [5, II, 1.15], but for our expository purposes we will use an *ad hoc* trick as in [10]: there is a finite flat map $j : X(N)^{\mathrm{can}} \to \mathbf{P}^1_{\mathbf{Z}[\zeta_N]}$ induced by formation of j-invariants, and the reduced subscheme underlying the preimage of the section $\infty \in \mathbf{P}^1(\mathbf{Z}[\zeta_N])$ is called the *cuspidal subscheme* $X(N)^{\mathrm{can}}_\infty$. This is finite and flat over $\mathbf{Z}[\zeta_N]$. The key fact is:

Theorem 2.3. *The closed subscheme $X(N)^{\mathrm{can}}_\infty$ is a finite disjoint union of copies of* $\operatorname{Spec} \mathbf{Z}[\zeta_N]$*, and the formal completion of $X(N)^{\mathrm{can}}$ along this closed subscheme is canonically isomorphic to a finite disjoint union of copies of* $\operatorname{Spf} \mathbf{Z}[\zeta_N][\![q^{1/N}]\!]$.

Let us now define the cuspidal section $\infty \in X(N)^{\mathrm{can}}(\mathbf{Z}[\zeta_N])$ algebraically. This definition rests on the standard Néron N-gon C_N over $\operatorname{Spec} \mathbf{Z}[\zeta_N]$. Since the smooth locus C_N^{sm} is canonically identified with $\mathbf{G}_m \times \mathbf{Z}/N\mathbf{Z}$ as a group scheme, we have $C_N^{\mathrm{sm}}[N] = \mu_N \times \mathbf{Z}/N\mathbf{Z}$. There is a canonical full level-N structure of type ζ_N defined by the map

$$\iota : \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z} \to \mu_N \times \mathbf{Z}/N\mathbf{Z}$$

that carries $(1,0)$ to $(\zeta_N, 0)$ and carries $(0,1)$ to $(1,1)$. This defines a section

$$\infty : \operatorname{Spec} \mathbf{Z}[\zeta_N] \hookrightarrow X(N)^{\mathrm{can}}$$

that is one of the components of $X(N)^{\mathrm{can}}_\infty$.

To explain the link between the preceding algebraic theory and the analytic theory, fix a positive integer N and a primitive Nth root of unity ζ in $\mathbf{C}$. We avoid picking a preferred choice of ζ (such as $e^{\pm 2\pi\sqrt{-1}/N}$) because the algebraic theory must treat all choices on an equal footing, and we want to argue in a manner that translates most easily into the algebraic theory. Consider the moduli functor $\overline{\mathscr{M}}_\zeta(N)$ that classifies analytic families of full level-N structures of type ζ. For $N \geq 3$, these structures admit no non-trivial automorphisms and there is a universal analytic family over an open modular curve $Y_\zeta(N)$ that is the complement of finitely many points (the *cusps*) in a compact connected Riemann surface $X_\zeta(N)$. For $N \geq 3$ we may identify $X_\zeta(N)$ as a fine moduli space for the moduli functor that classifies analytic families of full level-N structures of type ζ on generalized elliptic curves [5, VI, §5; VII, §4], and this is isomorphic to the analytification of the complex fiber of $X(N)^{\mathrm{can}}$ via the map $\mathbf{Z}[\zeta_N] \to \mathbf{C}$ carrying ζ_N to ζ.

Remark 2.4. The relative algebraic theory of the Tate curve, as developed in [5, VII], ensures that the $q^{1/N}$-parameter in Theorem 2.3 coincides with the canonical local coordinate at the cusp ∞ in the analytic theory when we use the identification of completed algebraic and analytic local rings at cusps on a complex fiber of $X(N)^{\mathrm{can}}$. In what follows we will make essential use of this compatibility between the analytic and algebraic theories of q-expansion.

Fix $N \geq 3$. There is a very well-known uniformization of the modular curve $Y_\zeta(N)$ via the analytic map

$$\pi_\zeta : \mathbf{C} - \mathbf{R} \twoheadrightarrow Y_\zeta(N)$$

that sends $\tau \in \mathbf{C} - \mathbf{R}$ to the point in $Y_\zeta(N)$ classifying the pair $(E_\tau, \iota_{\tau,\zeta})$, where

$$E_\tau = \mathbf{C}^\times/q_\tau^{\mathbf{Z}}, \ \ \iota_{\tau,\zeta}(1,0) = \zeta \bmod q_\tau^{\mathbf{Z}}, \ \ \iota_{\tau,\zeta}(0,1) = q_\tau^{1/N} \bmod q_\tau^{\mathbf{Z}}. \tag{2.1}$$

There is a functorial left action of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ on $X_\zeta(N)$ defined by

$$[\gamma]_\zeta(E, \iota) = (E, \iota \circ \gamma') \tag{2.2}$$

with $\gamma' = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, but the lift of $[\gamma]_\zeta$ (via π_ζ) to an action on $\mathbf{C}-\mathbf{R}$ depends on ζ. On each connected component $\mathfrak{H}$ of $\mathbf{C} - \mathbf{R}$, the lift of $[\gamma]_\zeta$ is induced by the standard linear-fractional action of any $\gamma_{\mathfrak{H}} \in \mathrm{SL}_2(\mathbf{Z})$ that lifts $\begin{pmatrix} a & u_{\mathfrak{H}} b \\ u_{\mathfrak{H}}^{-1} c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, where $\zeta = e^{2\pi i_{\mathfrak{H}} u_{\mathfrak{H}}/N}$ for $i_{\mathfrak{H}} = \sqrt{-1} \in \mathfrak{H}$ and $u_{\mathfrak{H}} \in (\mathbf{Z}/N\mathbf{Z})^\times$. Since $u_{-\mathfrak{H}} = -u_{\mathfrak{H}}$, we see that the action of $\gamma_{-\mathfrak{H}}$ on $-\mathfrak{H}$ is intertwined with the action of $\gamma_{\mathfrak{H}}$ on $\mathfrak{H}$ by means of negation on $\mathbf{C} - \mathbf{R}$. Observe also that the analytic action $[\cdot]_\zeta$ of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ on $X_\zeta(N)$ arises from an algebraic action of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ on $X(N)^{\mathrm{can}}$ over $\mathbf{Z}[\zeta_N]$ that is defined by means of the same moduli-theoretic definition $(E, \iota) \mapsto (E, \iota \circ \gamma')$.

Remark 2.5. For any two primitive Nth roots of unity ζ and ζ' in $\mathbf{C}$, we may identify $\overline{\mathscr{M}}_\zeta(N)$ and $\overline{\mathscr{M}}_{\zeta'}(N)$ by composing ι with the automorphism of $(\mathbf{Z}/N\mathbf{Z})^2$ defined by $(n,m) \mapsto (en, m)$ for the unique $e \in (\mathbf{Z}/N\mathbf{Z})^\times$ such that $\zeta' = \zeta^e$. This sets up an abstract isomorphism $\alpha_{\zeta',\zeta} : X_\zeta(N) \simeq X_{\zeta'}(N)$ that carries π_ζ to $\pi_{\zeta'}$. The isomorphism $\alpha_{\zeta',\zeta}$ is generally not $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$-equivariant: if $\zeta' = \zeta^e$ for $e \in (\mathbf{Z}/N\mathbf{Z})^\times$ then $\alpha_{\zeta',\zeta} \circ [\gamma]_\zeta = [\gamma_e^{-1}\gamma\gamma_e]_{\zeta'} \circ \alpha_{\zeta',\zeta}$ with $\gamma_e = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}$. Note that $\alpha_{\zeta',\zeta}$ is equivariant for the action of $(\mathbf{Z}/N\mathbf{Z})^\times$ via the diagonal embedding $c \mapsto \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$ into $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$.

The map π_ζ presents $Y_\zeta(N)$ as the quotient of $\mathbf{C} - \mathbf{R}$ by the group of automorphisms generated by negation and the standard linear fractional action of the principal congruence subgroup

$$\Gamma(N) = \ker(\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})).$$

The uniformization π_ζ gives rise to a canonical cusp $\infty_\zeta \in X_\zeta(N)$, and the parameter $q_\tau^{1/N}$ goes over to a canonical local coordinate q_{∞_ζ} around $\infty_\zeta \in X_\zeta(N)$. Under the identification of $X_\zeta(N)$ with the analytic fiber of $X(N)^{\mathrm{can}}$, ∞_ζ arises from $\infty \in X(N)^{\mathrm{can}}(\mathbf{Z}[\zeta_N])$ and q_{∞_ζ} corresponds to $q^{1/N}$.

For $N = 5$, something remarkable happens: there is another canonical cusp 0_ζ (this is *not* $\pi_\zeta(0)$): we define 0_ζ on $X_\zeta(5)$ to be the image of ∞_ζ under the action of $\begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X_\zeta(5)$ for a generator c of $(\mathbf{Z}/5\mathbf{Z})^\times$; this c is unique up to a sign, and so the choice of c does not matter. Explicitly, since $\begin{pmatrix} 2 & 5 \\ 5 & 13 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ lifts such a matrix (with $c = 2$), we see that if $\mathfrak{H}$ is a connected component of $\mathbf{C} - \mathbf{R}$ containing $i = \sqrt{-1}$ then for $\zeta = e^{2\pi i/5}$ we may extend $\pi_\zeta|_{\mathfrak{H}}$ by continuity to points of $\mathbf{P}^1(\mathbf{Q})$ and $\pi_\zeta(2/5) = 0_\zeta$. In particular, $\pi_\zeta(0) \neq 0_\zeta$. When working algebraically with $X(5)^{\mathrm{can}}$ over $\mathrm{Spec}\,\mathbf{Z}[\zeta_5]$, we define the cusp $0 \in X(5)^{\mathrm{can}}(\mathbf{Z}[\zeta_5])$ in terms of ∞ exactly as we just defined 0_ζ in terms of ∞_ζ. The isomorphism $\alpha_{\zeta',\zeta} : X_\zeta(N) \simeq X_{\zeta'}(N)$ carries ∞_ζ to $\infty_{\zeta'}$, q_{∞_ζ} to $q_{\infty_{\zeta'}}$, and (for $N = 5$) 0_ζ to $0_{\zeta'}$.

By means of π_ζ, we may identify the meromorphic function field of $X_\zeta(N)$ with the field of *level-N modular functions*; *i.e.*, the meromorphic functions on $\mathbf{C} - \mathbf{R}$ that are invariant under the actions of negation and of $\Gamma(N)$, and that are meromorphic at the points of $\mathbf{P}^1(\mathbf{Q})$ when such points are approached through neighborhoods in the horocycle topology on either connected component of $\mathbf{C} - \mathbf{R}$. The compact connected Riemann surface $X_\zeta(N)$ has genus zero for $N \leq 5$, and so for such N the meromorphic function field of $X_\zeta(N)$ is a rational function field $\mathbf{C}(j_{N,\zeta})$ where $j_{N,\zeta} : X_\zeta(N) \simeq \mathbf{CP}^1$ is an isomorphism onto the Riemann sphere. To uniquely define $j_{N,\zeta}$ for $N \leq 5$, we need to impose some additional normalization conditions at cusps as follows.

For $N \leq 5$, we can define the modular function $j_{N,\zeta}$ up to an additive constant by requiring that $j_{N,\zeta}(\infty_\zeta) = [1:0]$ and that the Laurent expansion of $j_{N,\zeta}$ at ∞_ζ have leading coefficient 1 with respect to the local coordinate q_{∞_ζ}. We eliminate the additive constant for $N = 5$ by demanding $j_{5,\zeta}(0_\zeta) = 0$. That is,

$$\mathrm{div}(j_{5,\zeta}) = (0_\zeta) - (\infty_\zeta). \tag{2.3}$$

For $N = 5$, the isomorphism $\alpha_{\zeta',\zeta} : X_\zeta(5) \simeq X_{\zeta'}(5)$ must therefore carry $j_{5,\zeta}$ to $j_{5,\zeta'}$, so $j_{5,\zeta} \circ \pi_\zeta$ *is independent of* ζ:

Definition 2.6. The common function $j_{5,\zeta} \circ \pi_\zeta$ on $\mathbf{C} - \mathbf{R}$ is denoted j_5.

At the end of §4 we will review the proof of the well-known fact that $1/j_5$ is Ramanujan's continued fraction F.

Our ability to get integral algebraic results for j_5 will rest on the integral model $X(5)^{\mathrm{can}}$ over $\mathbf{Z}[\zeta_5]$, but to get results over $\mathbf{Z}$ we require a model over $\mathbf{Q}$. More specifically, we shall now construct a model over $\mathbf{Z}[1/5]$; the equality $\mathbf{Z}[1/5] \cap \mathbf{Z}[\zeta_5] = \mathbf{Z}$ will ensure that we are able to get results over $\mathbf{Z}$ and not only over $\mathbf{Z}[\zeta_5]$.

Fix $N \geq 3$. We shall define a twisted modular curve $X_\mu(N)$ over $\mathbf{Z}[1/N]$ that naturally descends the $\mathbf{Z}[\zeta_N, 1/N]$-scheme $X(N)^{\mathrm{can}}$; in particular, $X_\mu(N)$ must be proper and smooth over $\mathrm{Spec}\,\mathbf{Z}[1/N]$ with geometrically connected fibers of dimension 1. The scheme $X_\mu(N)$ is defined to represent the *$\Gamma_\mu(N)$-moduli functor* that classifies pairs (E, ι) where E is a generalized elliptic curve over a variable $\mathbf{Z}[1/N]$-scheme S and

$$\iota : \mu_N \times \mathbf{Z}/N\mathbf{Z} \to E^{\mathrm{sm}}[N]$$

is an isomorphism of finite étale S-groups such that ι is ample on E and intertwines the Weil pairing on $E^{\mathrm{sm}}[N]$ with the evident μ_N-valued symplectic form on $\mu_N \times \mathbf{Z}/N\mathbf{Z}$. On the category of $\mathbf{Z}[\zeta_N][1/N]$-schemes, this moduli functor is naturally isomorphic to the one that is represented by the $\mathbf{Z}[\zeta_N]$-scheme $X(N)^{\mathrm{can}}$ upon inverting N, and hence the existence of $X_\mu(N)$ is established by using finite étale descent with a suitable action of $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$ on $X(N)^{\mathrm{can}}$. We likewise get $Y_\mu(N)$ by descending the open affine complement $Y(N)^{\mathrm{can}}$ of the cuspidal subscheme in $X(N)^{\mathrm{can}}$.

3. Canonical models

For our purposes, we need to know that the modular curves $X_\mu(N)_{\mathbf{Q}}$ over $\mathbf{Q}$ are both moduli spaces (as explained above) as well as canonical models in the sense of Shimura (and hence have well-understood Galois-theoretic behavior at CM points). The link with Shimura's theory rests on a q-expansion principle for rational functions:

Lemma 3.1. *Let $\zeta = e^{\pm 2\pi i/N}$ with $i \in \mathbf{C}$ satisfying $i^2 + 1 = 0$. Using $\pi_\zeta : \mathbf{C} - \mathbf{R} \to Y_\zeta(N)$ to identify the meromorphic function field of $X_\zeta(N)$ with the level-N modular functions on $\mathbf{C} - \mathbf{R}$, the function field $\mathbf{Q}(X_\mu(N))$ consists of the level-N modular functions f such that the q-expansion of f at ∞ (in the parameter $q_\tau^{1/N}$) has coefficients in $\mathbf{Q}$.*

Proof. The arithmetic theory of the Tate curve provides a canonical isomorphism of complete local rings $\widehat{\mathscr{O}}_{X_\mu(N),\infty} \simeq \mathbf{Q}[\![q^{1/N}]\!]$. The analytic theory of the Tate curve and our two choices for ζ ensure that applying $\mathbf{C}\widehat{\otimes}_{\mathbf{Q}}(\cdot)$ to this isomorphism yields *the same* calculation of the completed analytic local ring on $X_\zeta(N)(\mathbf{C})$ at ∞ as is obtained via π_ζ and the analytic parameter $q_\tau^{1/N}$. Thus, the problem is purely algebraic: we must prove that if $f \in \mathbf{C}(X_\mu(N)_{\mathbf{C}})$ then $f \in \mathbf{Q}(X_\mu(N))$ if the image of f in the local field $\mathbf{C}(X_\mu(N)_{\mathbf{C}})_\infty \simeq \mathbf{C}(\!(q^{1/N})\!)$ lies in the subfield $\mathbf{Q}(X_\mu(N))_\infty \simeq \mathbf{Q}(\!(q^{1/N})\!)$. Such an f is invariant under the action of $\mathrm{Aut}(\mathbf{C}/\mathbf{Q})$, so we just have to prove that the fixed field of $\mathrm{Aut}(\mathbf{C}/\mathbf{Q})$ in $\mathbf{C}(X_\mu(N)_{\mathbf{C}})$ is $\mathbf{Q}(X_\mu(N))$.

More generally, let L/k be an extension of fields and $K, E \subseteq L$ intermediate extensions linearly disjoint over k such that k is perfect, k is algebraically closed in E, and K is algebraically closed (e.g., $k = \mathbf{Q}$, $K = \mathbf{C}$, $E = \mathbf{Q}(X_\mu(N))$, $L = \mathbf{C}(X_\mu(N)_{\mathbf{C}})$). By linear disjointness, the ring $K \otimes_k E$ is a domain and its fraction field is naturally isomorphic to the subfield $KE \subseteq L$, so KE admits a natural action of $\mathrm{Aut}(K/k)$. It is a standard fact in the theory of linearly disjoint extensions that the $\mathrm{Aut}(K/k)$-invariants in KE must be precisely the elements of E, and this gives what we need. ■

To apply this lemma, we use Shimura's canonical models for modular curves. Fix a connected component $\mathfrak{H}$ of $\mathbf{C} - \mathbf{R}$, and let $i = \sqrt{-1} \in \mathfrak{H}$. We are now going to apply Shimura's reciprocity law on canonical models, but we first need to explain why the moduli scheme $X_\mu(N)_{\mathbf{Q}}$ equipped with its canonical isomorphism

$$X_\mu(N)(\mathbf{C}) \simeq \Gamma(N)\backslash(\mathfrak{H} \cup \mathbf{P}^1(\mathbf{Q}))$$

is a canonical model in the sense of Shimura. This requires some preliminary notation, as follows.

Let $G = \mathrm{GL}_2$ and let $Z = \mathbf{G}_m$ be its center. We write $\mathbf{A}_L$ to denote the adele ring of a number field L, and $\mathbf{A}_L^\infty = L \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$ to denote the ring of finite adeles for L. Let U be an open subgroup of $G(\mathbf{A}_{\mathbf{Q}})$ whose projection into $G(\mathbf{R})$ lies in $G(\mathbf{R})^0 = \mathrm{GL}_2^+(\mathbf{R})$ and such that U contains $Z(\mathbf{Q})G(\mathbf{R})^0 = \mathbf{Q}^\times \mathrm{GL}_2^+(\mathbf{R})$ and $G(\mathbf{A}_{\mathbf{Q}})/U$ is compact. Let $\Gamma_U = U \cap G(\mathbf{Q})$. This is a discrete subgroup in $G(\mathbf{R})^0$ that is commensurable with $Z(\mathbf{Q}) \cdot (G(\mathbf{Z}) \cap G(\mathbf{R})^0) = \mathbf{Q}^\times \mathrm{SL}_2(\mathbf{Z})$. The analytic quotient $\Gamma_U\backslash\mathfrak{H}$ is the complement of finitely many points in a unique compact connected Riemann surface X_{Γ_U} whose meromorphic function field is the field of modular functions on $\mathfrak{H}$ that are invariant under Γ_U for the standard action of $\Gamma_U \subseteq G(\mathbf{R})^0$ on $\mathfrak{H}$. By Shimura's theory of canonical models (see [19, §6.7], especially [19, Prop. 6.27]), X_{Γ_U} admits a model X_U that is a smooth proper geometrically-connected curve defined over a number field $k_U \subseteq \mathbf{C}$ such that $k_U/\mathbf{Q}$ is abelian and, at CM-points of X_U, the arithmetic properties of special values of any $h \in k_U(X_U)$ may be read off from Shimura's reciprocity law [19, 6.31]. Let us see how these generalities work out in a special case.

The subgroups U of most interest to us are

$$V_N = Z(\mathbf{Q})G(\mathbf{R})^0 \cdot \left\{ g \in G(\widehat{\mathbf{Z}}) \mid g \equiv \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \bmod N \right\}. \tag{3.1}$$

By [19, Prop. 6.9(3), Rem. 6.28], X_{V_N} is a canonical model for $X_{e^{2\pi i/N}}(N) = X(N)^{\mathrm{can}}_{\mathbf{C}}$ via the embedding $\mathbf{Z}[\zeta_N] \to \mathbf{C}$ that sends ζ_N to $e^{2\pi i/N}$, and $k_{V_N} = \mathbf{Q}$ and $\mathbf{Q}(X_{V_N})$ is the field of level-N modular functions on $\mathfrak{H}$ whose q-expansion at ∞ (in the parameter $q_\tau^{1/N}$) has coefficients in $\mathbf{Q}$. Thus, by Lemma 3.1, $X_\mu(N)_{\mathbf{Q}}$ equipped with its canonical isomorphism $X_\mu(N)(\mathbf{C}) \simeq X_{e^{2\pi i/N}}(N)$ *is* Shimura's canonical model X_{V_N} for $X_{e^{2\pi i/N}}(N)$.

Let $y \in X_\mu(N)(\mathbf{C})$ be a CM-point (so we may identify y with a closed point, also denoted y, on $X_\mu(N)$ with residue field $\mathbf{Q}(y)$ embedded into $\mathbf{C}$). Choose $\tau \in \mathbf{C} - \mathbf{R}$ with $\pi_{e^{2\pi i_\tau/N}}(\tau) = y$, and consider the finite-dimensional $\mathbf{Q}$-algebras $K = \mathbf{Q}(\tau)$ and $A = \mathrm{End}_{\mathbf{Q}}(K)$ as ring-schemes over $\mathrm{Spec}\,\mathbf{Q}$. Let $\rho : K^\times \to A^\times$ be the natural map of algebraic unit-groups induced by the natural ring-scheme map $K \to A$; note that the determinant $\det\rho : K^\times \to \mathbf{Q}^\times$ is the norm. Use the ordered $\mathbf{Q}$-basis $\{\tau, 1\}$ of K to identify A with a matrix-algebra over $\mathbf{Q}$, and hence to identify $A^\times$ with GL_2 as algebraic groups over $\mathbf{Q}$. On $\mathbf{A}_{\mathbf{Q}}$-points, ρ

therefore defines a continuous homomorphism

$$\rho_\tau : \mathbf{A}_K^\times \to \mathrm{GL}_2(\mathbf{A}_\mathbf{Q}) \tag{3.2}$$

that lands inside $\mathrm{GL}_2^+(\mathbf{A}_\mathbf{Q}) = \mathrm{GL}_2^+(\mathbf{R}) \times \mathrm{GL}_2(\mathbf{A}_\mathbf{Q}^\infty)$ and carries $K^\times$ into $\mathbf{Q}^\times$ and $K_\infty^\times$ into $\mathrm{GL}_2^+(\mathbf{R})$. As a special case of [19, 6.33], we thereby obtain:

Theorem 3.2 (Shimura)**.** *Let $\overline{\mathbf{Q}} \subseteq \mathbf{C}$ be the algebraic closure of $\mathbf{Q}$. For any CM-point $y \in X_\mu(N)(\overline{\mathbf{Q}}) \subseteq X_\mu(N)(\mathbf{C})$ and $\tau \in \mathbf{C} - \mathbf{R}$ with $\pi_{e^{2\pi i\tau/N}}(\tau) = y$, the compositum $\mathbf{Q}(\tau, y) \subseteq \mathbf{C}$ of $K = \mathbf{Q}(\tau)$ and $\mathbf{Q}(y)$ is the finite abelian extension of K that is the class field associated to the open subgroup*

$$(K^\times \cdot \{s \in \mathbf{A}_K^\times \,|\, \rho_\tau(s) \in V_N\})/K^\times \subseteq \mathbf{A}_K^\times/K^\times,$$

with V_N as in (3.1)*. In particular, this extension is unramified at finite places away from $N[\mathscr{O}_K : \mathscr{O}_\tau]$ where $\mathscr{O}_\tau$ is the CM-order of $\mathbf{C}^\times/q_\tau^\mathbf{Z}$.*

Let us record a useful easy corollary (to be applied with $p = 5$):

Corollary 3.3. *Let $\tau \in \mathbf{C} - \mathbf{R}$ be imaginary quadratic, and assume $N = p \geq 3$ is prime. Let $K = \mathbf{Q}(\tau)$, $y = \pi_{e^{2\pi i\tau/p}}(\tau) \in X_\mu(N)(\overline{\mathbf{Q}}) \subseteq X_\mu(N)(\mathbf{C})$, and $\mathscr{O}_\tau = \mathrm{End}(\mathbf{C}^\times/q_\tau^\mathbf{Z}) \subseteq \mathbf{C}$ the CM order for the fiber of the universal elliptic curve over y.*

The finite abelian extension $K(y)/K$ is associated to the open subgroup

$$K^\times \cdot (K_\infty^\times \times U_\tau)/K^\times \subseteq \mathbf{A}_K^\times/K^\times,$$

where $U_\tau \subseteq \prod_{v\nmid\infty} \mathscr{O}_{K,v}^\times = \prod_{\ell\nmid\infty}(\mathbf{Z}_\ell \otimes_\mathbf{Z} \mathscr{O}_K)^\times$ is the group of finite ideles $s = (s_\ell)$ whose ℓ-component $s_\ell \in (\mathbf{Z}_\ell \otimes_\mathbf{Z} \mathscr{O}_K)^\times$ lies in $(\mathbf{Z}_\ell \otimes_\mathbf{Z} \mathscr{O}_\tau)^\times$ for $\ell \neq p$ and whose p-component $s_p \in (\mathbf{Z}_p \otimes_\mathbf{Z} \mathscr{O}_K)^\times$ satisfies

$$s_p \equiv 1 \bmod \frac{p}{\tau} \cdot \mathbf{Z}_p \otimes_\mathbf{Z} \mathscr{O}_\tau, \ \ s_p \in \mathbf{Z}_p^\times + p(\mathbf{Z}_p \otimes_\mathbf{Z} \mathscr{O}_\tau).$$

In particular, $K(y)/K$ is unramified away from $p[\mathscr{O}_K : \mathscr{O}_\tau]$ and if τ is p-integral then $K(y)$ is contained in the ray class field of conductor $p[\mathscr{O}_K : \mathscr{O}_\tau]$ over K, with equality if moreover $\mathscr{O}_\tau = \mathscr{O}_K$ and τ is a p-unit.

4. Klein Forms and j_5

Let ζ be a primitive 5th root of unity in $\mathbf{C}$. Recall that in §2 we defined the rational parameter $j_{5,\zeta}$ for $X_\zeta(5)$ by the requirements that $\mathrm{div}(j_{5,\zeta}) = 0_\zeta - \infty_\zeta$ and that the Laurent expansion of $j_{5,\zeta}$ at ∞_ζ has leading coefficient 1 with respect to a canonical local coordinate q_{∞_ζ}. We also noted that the holomorphic function $j_5 = j_{5,\zeta} \circ \pi_\zeta$ on $\mathbf{C} - \mathbf{R}$ is independent of ζ. We need to give two explicit formulas for j_5, using Klein forms and a q-product; both will be useful in examples (e.g., the description via Klein forms makes it easy to compute the action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on j_5). Thus, we first shall give a rapid review of the basics of Klein forms, partly to give a convenient reference for formulas and partly to set the notation we shall use.

Let us begin with a review of some basic formulas from the theory of elliptic functions. Let Λ be a lattice in $\mathbf{C}$. Recall that the Weirstrass σ-function on $\mathbf{C}$ is

$$\sigma(z, \Lambda) \stackrel{\mathrm{def}}{=} z \prod_{\omega \in \Lambda - \{0\}} \left(1 - \frac{z}{\omega}\right) e^{z/\omega + \frac{1}{2}(z/\omega)^2},$$

and (see [20, I.5]) for any $\omega \in \Lambda$ we have

$$\frac{\sigma(z + \omega, \Lambda)}{\sigma(z, \Lambda)} = \varepsilon_\Lambda(\omega) e^{\eta_\Lambda(\omega)(z+\omega/2)},$$

where $\varepsilon_\Lambda(\omega) = 1$ (resp. $\varepsilon(\omega) = -1$) if and only if $\omega \in 2\Lambda$ (resp. $\omega \in \Lambda - 2\Lambda$), and $\eta_\Lambda : \Lambda \to \mathbf{C}$ is the additive *quasi-period* map that measures the failure of the Weierstrass function $-\wp_\Lambda$ to integrate to a Λ-periodic function on $\mathbf{C}$. If we let

$$\Lambda_\tau = \mathbf{Z}\tau \oplus \mathbf{Z}$$

for $\tau \in \mathbf{C} - \mathbf{R}$, then $(z, \tau) \mapsto \wp_{\Lambda_\tau}(z)$ is holomorphic, and so $\tau \mapsto \eta_{\Lambda_\tau}(1)$ and $\tau \mapsto \eta_{\Lambda_\tau}(\tau)$ are holomorphic. Let $\eta(\cdot, \Lambda) : \mathbf{C} = \mathbf{R} \otimes_{\mathbf{Z}} \Lambda \to \mathbf{C}$ be the $\mathbf{R}$-linear extension of η_Λ; this is not holomorphic, but clearly

$$\tau \mapsto \eta(a_1\tau + a_2, \mathbf{Z}\tau \oplus \mathbf{Z}) = a_1\eta_{\Lambda_\tau}(\tau) + a_2\eta_{\Lambda_\tau}(1)$$

is holomorphic on $\mathbf{C} - \mathbf{R}$ for a fixed $a = (a_1, a_2) \in \mathbf{R}^2$.

Let $\mathrm{Isom}_{\mathbf{R}}(\mathbf{R}^2, \mathbf{C})$ denote the set of $\mathbf{R}$-linear isomorphisms $\mathbf{R}^2 \simeq \mathbf{C}$. For $\tau \in \mathbf{C} - \mathbf{R}$ we define $W_\tau : \mathbf{R}^2 \simeq \mathbf{C}$ by $W_\tau(0,1) = 1$ and $W_\tau(1,0) = \tau$; these are exactly the $W \in \mathrm{Isom}_{\mathbf{R}}(\mathbf{R}^2, \mathbf{C})$ such that $W(0,1) = 1$, and $W_\tau(\mathbf{Z}^2) = \Lambda_\tau$.

Definition 4.1. Choose $a \in \mathbf{Q}^2$ and $W \in \mathrm{Isom}_{\mathbf{R}}(\mathbf{R}^2, \mathbf{C})$, and let $z = W(a) \in \mathbf{C}$ and $\Lambda = W(\mathbf{Z}^2)$. The *Klein form* $\kappa_a : \mathrm{Isom}_{\mathbf{R}}(\mathbf{R}^2, \mathbf{C}) \to \mathbf{C}$ is

$$\kappa_a(W) \stackrel{\text{def}}{=} e^{-\eta(W(a), W(\mathbf{Z}^2))\cdot W(a)/2}\sigma(W(a), W(\mathbf{Z}^2)) = e^{-\eta(z,\Lambda)z/2}\sigma(z, \Lambda). \tag{4.1}$$

We shall write $\kappa_a(\tau)$ to denote $\kappa_a(W_\tau)$, so $\tau \mapsto \kappa_a(\tau)$ is holomorphic on $\mathbf{C} - \mathbf{R}$. The transformation law $\kappa_{(a_1,a_2)}(-\tau) = -\kappa_{(a_1,-a_2)}(\tau)$ is immediate from the definitions, and this lets us pass between connected components of $\mathbf{C} - \mathbf{R}$ when working with Klein forms.

The Klein forms satisfy several additional well-known obvious properties that we shall use, and so for ease of reference we summarize the properties that we will need:

- They are homogenous of degree 1:

$$\kappa_a(\lambda W) \ = \ \lambda \kappa_a(W) \tag{4.2}$$

  for any $\lambda \in \mathbf{C}^\times$. This allows us to systematically pass between $\kappa_a(\tau)$'s and $\kappa_a(W)$'s.
- For $a \in \mathbf{Q}^2$, $W \in \mathrm{Isom}_{\mathbf{R}}(\mathbf{R}^2, \mathbf{C})$, and $b = (b_1, b_2) \in \mathbf{Z}^2$, we have

$$\kappa_{a+b}(W) = \epsilon_W(a, b)\kappa_a(W)$$

  for an explicit root of unity $\epsilon_W(a, b)$ (determined by Legendre's period relation for η_Λ). If $W = W_\tau$ and $a = (a_1, a_2)$ then

$$\kappa_{a+b}(\tau) \ = \ \epsilon_\tau(a, b)\kappa_a(\tau) \tag{4.3}$$

  for $b = (b_1, b_2) \in \mathbf{Z}^2$, where

$$\epsilon_\tau(a, b) = (-1)^{b_1+b_2+b_1b_2} \exp(\pi i_\tau(a_1b_2 - b_1a_2)) \tag{4.4}$$

  with $i_\tau^2 = -1$ and i_τ in the connected component of τ in $\mathbf{C} - \mathbf{R}$.
- For $\gamma \in \mathrm{Aut}(\mathbf{Z}^2) = \mathrm{GL}_2(\mathbf{Z})$, we have $\kappa_a(W \circ \gamma) \ = \ \kappa_{\gamma(a)}(W)$. An equivalent formulation is

$$\kappa_a(\gamma(\tau)) \ = \ j(\gamma, \tau)\kappa_{\gamma(a)}(\tau), \tag{4.5}$$

  where $j(\gamma, \tau) = u\tau + v$ is the standard automorphy factor for $\gamma = \left(\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right)$.
- Fix $\tau \in \mathbf{C} - \mathbf{R}$ and $a = (a_1, a_2) \in \mathbf{Q}^2$. Define $q = e^{2\pi i_\tau z}$ with $z = W_\tau(a) \in \mathbf{C}$. We have

$$\kappa_a(\tau) \ = \ -\frac{q_\tau^{(1/2)(a_1^2 - a_1)}}{2\pi i_\tau} e^{\pi i_\tau a_2(a_1 - 1)}(1 - q)\prod_{n=1}^{\infty} \frac{(1 - q_\tau^n q)(1 - q_\tau^n/q)}{(1 - q_\tau^n)^2}. \tag{4.6}$$

This follows from the product formula in [14, §18.2, Thm. 4].

We will need to explicitly construct level-N modular functions for $N = 5$, and this is most easily done by using Klein forms and the criterion in:

Lemma 4.2. *Fix a positive integer $N \geq 1$ and a finite subset $\mathscr{A} \subseteq (N^{-1}\mathbf{Z})^2$. Let $m : \mathscr{A} \to \mathbf{Z}$ be a function. Define the mermorphic function*

$$f = \prod_{\alpha \in \mathscr{A}} \kappa_a^{m(a)}$$

on $\mathbf{C}-\mathbf{R}$*. Let* $Q:(N\mathbf{Z})^2\to\mathbf{Z}$ *be the quadratic form*

$$Q(x)=\sum_{a\in\mathscr{A}} m(a)\langle a,x\rangle^2,$$

where $\langle\cdot,\cdot\rangle:(N^{-1}\mathbf{Z})^2\times(N\mathbf{Z})^2\to\mathbf{Z}$ *is the evident duality pairing.*

The function f *is an automorphic form on* $\Gamma(N)$ *of weight* $-\sum_{a\in\mathscr{A}} m(a)$ *if and only if* Q *vanishes modulo* $N/\gcd(N,2)$*. If* $\mathscr{A}$ *is stable under* $(a_1,a_2)\mapsto(a_1,-a_2)$*, then* f *is invariant under* $\tau\mapsto-\tau$ *if* $m(a_1,a_2)=m(a_1,-a_2)$ *for all* $a=(a_1,a_2)\in\mathscr{A}$*.*

Proof. The vanishing of the quadratic form amounts to a vanishing condition on coefficients, and the equivalence of f being an automorphic form on $\Gamma(N)$ and such vanishing of coefficients is proved in [13, p. 68]. The final part concerning invariance under $\tau\mapsto-\tau$ is trivial. ■

Theorem 4.3. *On* $\mathbf{C}-\mathbf{R}$*, we have*

$$j_5=\frac{\kappa_{(\frac{2}{5},0)}\kappa_{(\frac{2}{5},\frac{1}{5})}\kappa_{(\frac{2}{5},\frac{2}{5})}\kappa_{(\frac{2}{5},-\frac{2}{5})}\kappa_{(\frac{2}{5},-\frac{1}{5})}}{\kappa_{(\frac{1}{5},0)}\kappa_{(\frac{1}{5},\frac{1}{5})}\kappa_{(\frac{1}{5},\frac{2}{5})}\kappa_{(\frac{1}{5},-\frac{2}{5})}\kappa_{(\frac{1}{5},-\frac{1}{5})}}\tag{4.7}$$

and

$$j_5(\tau)=q_\tau^{-1/5}\prod_{n=1}^{\infty}\frac{(1-q_\tau^{5n-2})(1-q_\tau^{5n-3})}{(1-q_\tau^{5n-4})(1-q_\tau^{5n-1})}.\tag{4.8}$$

Proof. Let us define $\mathscr{J}_5$ to be the ratio of products of Klein forms in (4.7); we will prove that $\mathscr{J}_5$ satisfies the properties that uniquely characterize j_5. The invariance $\mathscr{J}_5(-\tau)=\mathscr{J}_5(\tau)$ follows from the identity $\kappa_{(a_1,a_2)}(-\tau)=\kappa_{(a_1,-a_2)}(\tau)$. The product formula (4.8) for $\mathscr{J}_5$ follows easily from (4.6). By Lemma 4.2 with $N=5$, taking

$$\mathscr{A}=\{(\ell/5,k/5):-2\le k\le 2,\ \ell=1,2\},\ \ m(\ell/5,k/5)=(-1)^\ell,$$

we deduce that $\mathscr{J}_5$ is a level-5 modular function. The canonical surjection $\pi_\zeta:\mathbf{C}-\mathbf{R}\twoheadrightarrow Y_\zeta(5)$ lets us consider $\mathscr{J}_5$ as a meromorphic function $\mathscr{J}_{5,\zeta}$ on $X_\zeta(5)$. By construction, we have $\mathscr{J}_{5,\zeta}\circ\pi_\zeta=\mathscr{J}_5$, and so the isomorphism $\alpha_{\zeta',\zeta}:X_\zeta(5)\simeq X_{\zeta'}(5)$ as in Remark 2.5 carries $\mathscr{J}_{5,\zeta}$ to $\mathscr{J}_{5,\zeta'}$.

The product expansion (4.8) makes it clear that $\mathscr{J}_{5,\zeta}$ has no poles on $Y_\zeta(5)$. Thus, the only possible poles are at the cusps. From the q-expansion (4.8) we see that

$$\mathrm{ord}_{\infty_\zeta}\mathscr{J}_{5,\zeta}=-1$$

and that the q-expansion of $\mathscr{J}_{5,\zeta}$ at ∞_ζ begins with $1/q_{\infty_\zeta}=1/q^{1/5}$. It remains to show that $\mathscr{J}_{5,\zeta}$ has no poles at the other cusps, and that its unique zero is at the cusp 0_ζ. Moreover, it is enough to consider a single ζ. We shall choose a connected component $\mathfrak{H}$ of $\mathbf{C}-\mathbf{R}$ and work with $\zeta=e^{2\pi i/5}$ and $\tau\in\mathfrak{H}$ where $i\in\mathfrak{H}$ is the unique point satisfying $i^2=-1$; this choice yields the standard formulas on $\mathfrak{H}$ when (via π_ζ) we lift the action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X_\zeta(5)$.

The transformation formulas for Klein forms under $\mathrm{SL}_2(\mathbf{Z})$ make it easy to express $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$-conjugates of $\mathscr{J}_5$ in terms of Klein forms. In this way, the transitivity of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on the 12 cusps of $X_\zeta(5)$ enables us to compute the q-expansion of $\mathscr{J}_5$ at each cusp. This computation shows that $\mathscr{J}_5$ has no poles at cusps away from ∞_ζ and it only vanishes at the cusp $\pi_\zeta(2/5)$ for $\zeta=e^{2\pi i/5}$. In §2 we showed $\pi_\zeta(2/5)=0_\zeta$ for any ζ. ■

Using the well-known Rogers–Ramanujan identities, it can be shown [17, p. 155] that

$$F(\tau)=q_\tau^{1/5}\prod_{n=1}^{\infty}\frac{(1-q_\tau^{5n-1})(1-q_\tau^{5n-4})}{(1-q_\tau^{5n-2})(1-q_\tau^{5n-3})}.$$

By (4.8), this proves the identity $F=1/j_5$. Unfortunately, we do not know a more direct way to verify that Ramanujan's F is a (level-5) modular function.

5. Application of arithmetic models

By construction, j_5 induces an isomorphism of Riemann surfaces $j_{5,\zeta} : X_\zeta(5) \simeq \mathbf{CP}^1$ for each primitive 5th root of unity ζ in $\mathbf{C}$. By Lemma 3.1, this descends to an algebraic isomorphism $j_{5,\mu} : X_\mu(5)_{\mathbf{Q}} \simeq \mathbf{P}^1_{\mathbf{Q}}$. Since $X_\mu(5)$ is a proper smooth $\mathbf{Z}[1/5]$-scheme with geometrically connected fibers of genus 0, the isomorphism $j_{5,\mu}$ must uniquely extend to an isomorphism $X_\mu(5) \simeq \mathbf{P}^1_{\mathbf{Z}[1/5]}$ over $\mathbf{Z}[1/5]$ that we also denote $j_{5,\mu}$. To deduce arithmetic properties of j_5 over $\mathbf{Z}$, it is essential to remove the denominators at 5 in this latter isomorphism. For this purpose, we will now work over $\mathbf{Z}[\zeta_5]$ by using Theorem 2.2 with $N = 5$.

Let X denote the $\mathbf{Z}[\zeta_5]$-scheme $X(5)^{\mathrm{can}}$, and let $j_X \in \mathbf{Q}(\zeta_5)(X)$ be the rational function obtained from $j_{5,\mu}$ by extension of scalars (or by descent of any $j_{5,\zeta}$ over $\mathbf{C}$). All fibers of X over $\operatorname{Spec} \mathbf{Z}[\zeta_5]$ are geometrically connected (by Stein factorization), as the $\mathbf{C}$-fiber is connected.

The $\mathbf{Z}[\zeta_5]$-scheme X is smooth (and hence regular) near the cusps, so the ideal sheaf of the section ∞ is invertible, and hence the inverse sheaf $\mathscr{O}(\infty)$ makes sense on X. The key to integrality results for j_5 is:

Lemma 5.1. *The rational function j_X on the $\mathbf{Z}[\zeta_5]$-scheme X is a regular funtion on $X - \{\infty\}$, and $\{j_X, 1\}$ is a pair of generating sections of the line bundle $\mathscr{O}(\infty)$ on X.*

Proof. The q-expansion of j_5 at ∞ has integral coefficients and a simple pole with leading coefficient 1, so the rational function j_X on X induces a local generator of $\mathscr{O}(\infty)$ along $\infty \in X(\mathbf{Z}[\zeta_5])$. It therefore remains to show that j_X is a regular function on $X - \{\infty\}$. Since $X - \{\infty\}$ is a connected normal noetherian scheme, it suffices to check that j_X is defined in codimension ≤ 1 on $X - \{\infty\}$. The situation along the generic fiber is clear via the analytic theory (see (2.3)), and so we only need to study j_X at the generic points of the geometrically connected fiber X_s of X over each closed point $s = \mathfrak{m} \in \operatorname{Spec} \mathbf{Z}[\zeta_5]$. Note that if s is not the unique point of residue characteristic 5, then the connected X_s is smooth and hence irreducible. Since $\infty \in X(\mathbf{Z}[\zeta_5])$ is supported in the smooth locus of X over $\operatorname{Spec} \mathbf{Z}[\zeta_5]$, the section $\infty_s \in X_s(\mathbf{F}_5)$ in the unique fiber X_s of characteristic 5 lies in a unique irreducible component of X_s.

Fix a choice of closed point $s \in \operatorname{Spec} \mathbf{Z}[\zeta_5]$. The local ring $\mathscr{O}_{X,\eta}$ at each generic point η of X_s is a discrete valuation ring with uniformizer given by a local parameter in $\mathbf{Z}[\zeta_5]_{\mathfrak{m}}$. Thus, the integral structure of the q-expansion of j_5 at ∞ ensures that for every closed point s of $\operatorname{Spec} \mathbf{Z}[\zeta_5]$, j_X is a local unit at the generic point of the unique irreducible component of X_s that contains ∞_s. It remains to work near the generic points η of the unique fiber in characteristic 5 such that $\overline{\{\eta\}}$ does not meet ∞. It suffices to find a section $\sigma_\eta \in X(\mathbf{Z}[\zeta_5])$ supported in the smooth locus and passing through the chosen mod-5 component $\overline{\{\eta\}}$ such that j_X lies in the coordinate ring of the formal completion of X along σ_η.

Finiteness of X over the usual j-line implies that $\overline{\{\eta\}}$ must contain some cusp, so it suffices to check that the q-expansion of j_5 at each cusp has coefficients in $\mathbf{Z}[\zeta_5]$. This is a purely analytic problem on $X_\zeta(5)$ for any primitive 5th root of unity $\zeta \in \mathbf{C}$, and it suffices to consider a single choice of ζ. We choose $\zeta = e^{2\pi i/5}$ for $i = \sqrt{-1}$ in a chosen connected component $\mathfrak{H}$ of $\mathbf{C} - \mathbf{R}$, as this makes the action of $\mathrm{SL}_2(\mathbf{Z})$ on $X_\zeta(5)$ lift (via π_ζ) to the standard action on $\mathfrak{H}$ via linear fractional transformations. The action of $\mathrm{SL}_2(\mathbf{Z})$ on $X_\zeta(5)$ is transitive on the set of cusps, so it suffices to prove that the coefficients of the q-expansion of $j_5 \circ \gamma$ at ∞ lies in $\mathbf{Z}[\zeta]$ for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$. By (4.7) and (4.8), this desired integrality follows immediately from the product formula (4.6) and the transformation law (4.5) for the standard action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{C} - \mathbf{R}$. ■

Let $(\mathscr{O}(1); s_0, s_1)$ be the universal line bundle on $\mathbf{P}^1$ equipped with an ordered pair of generating sections s_0 and s_1. By Lemma 5.1 and the universal property of the projective line, there is a unique morphism

$$J_5 : X(5)^{\mathrm{can}} \to \mathbf{P}^1_{\mathbf{Z}[\zeta_5]}$$

over $\mathbf{Z}[\zeta_5]$ such that there is an isomorphism $J_5^*(\mathscr{O}(1)) \simeq \mathscr{O}(\infty)$ carrying $J_5^*(s_0)$ to j_X and $J_5^*(s_1)$ to 1. In particular, $J_5^{-1}([1:0]) = \infty$ as subschemes of $X(5)^{\mathrm{can}}$.

Theorem 5.2. *The map J_5 is an isomorphism over $\mathbf{Z}[\zeta_5][1/5]$, and on the unique characteristic-5 fiber it contracts all irreducible components except for the unique fibral irreducible component C_∞ containing ∞. The* *reduced irreducible component C_∞ contains the cusp* 0 *as its only other cusp and it is mapped isomorphically onto $\mathbf{P}^1_{\mathbf{F}_5}$ under J_5. The other* 5 *irreducible components of the mod-$(1-\zeta_5)$ fiber of $X(5)^{\rm can}$ map onto a common point in $\mathbf{F}_5^\times \in \mathbf{P}^1(\mathbf{F}_5)$.*

Remark 5.3. One immediate consequence of this theorem is the numerical fact that the q-expansion of $j_{5,\zeta}$ at each cusp other than ∞_ζ and 0_ζ has all higher-degree coefficients divisible by $1-\zeta_5$. Another immediate consequence is that both the zero and polar schemes of J_5 lie entirely in the cuspidal subscheme. This second consequence generalizes (2.3).

Proof. By passing to the complex-analytic fiber relative to an embedding $\mathbf{Z}[\zeta_5] \to \mathbf{C}$ defined by some primitive 5th root of unity $\zeta \in \mathbf{C}$, the map J_5 induces the map $j_{5,\zeta} : X_\zeta(5) \simeq \mathbf{CP}^1$. Thus, the analytic isomorphism property for $j_{5,\zeta}$ over $\mathbf{C}$ implies that J_5 is an algebraic isomorphism on $\mathbf{Q}(\zeta_5)$-fibers, and so by properness the map J_5 is surjective. If we work over $\mathbf{Z}[\zeta_5][1/5]$, then J_5 is therefore a surjective birational map between proper smooth curves over $\mathbf{Z}[\zeta_5][1/5]$, and these curves have (geometrically) connected fibers. Thus, after inverting 5 we see that the proper J_5 must become quasi-finite and hence finite, so (by normality) it is an isomorphism over $\mathbf{Z}[\zeta_5][1/5]$.

There is a unique supersingular j-value in characteristic 5, so [10, 13.2.2] implies that the mod-$(1-\zeta_5)$ fiber $X_{\mathbf{F}_5}$ of $X = X(5)^{\rm can}$ is reduced and is scheme-theoretically constructed by gluing some $\mathbf{P}^1_{\mathbf{F}_5}$'s transversally at a single $\mathbf{F}_5$-point. It follows from [10, 13.8.4] that there are exactly $6 = \#\mathbf{P}^1(\mathbf{F}_5)$ irreducible components in $X_{\mathbf{F}_5}$ and that these are in natural bijection with the lines in $(\mathbf{Z}/5\mathbf{Z})^2$ in such a way that the action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5)^{\rm can}$ is compatible with the natural transitive action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on the set of such lines. In particular, this action on $X(5)^{\rm can}$ is transitive on the set of irreducible components of $X_{\mathbf{F}_5}$, so there are $12/6 = 2$ cusps on each component. The geometric points (E, ι) of $X(5)^{\rm can}$ satisfying $\iota(1, 0) = 0$ define one of these components. This component contains the cusps ∞ and 0, and so it is C_∞.

Let us show that the map $J_5 : C_\infty \to \mathbf{P}^1_{\mathbf{F}_5}$ between smooth proper connected curves is an isomorphism when C_∞ is given its reduced structure. Since $J_5^{-1}([1:0]) = \infty$ with ramification degree $e_{\infty|[1:0]} = 1$ (due to the structure of the q-expansion of j_5 at ∞), we conclude that the map $C_\infty \to \mathbf{P}^1_{\mathbf{F}_5}$ between integral proper curves is birational with generic degree 1. Thus, it is an isomorphism.

Let C be an irreducible component of $X_{\mathbf{F}_5}$ distinct from C_∞. The map $J_5 : C \to \mathbf{P}^1_{\mathbf{F}_5}$ is not surjective (it cannot hit $[1:0]$), so $J_5(C)$ is a single closed point in $\mathbf{A}^1_{\mathbf{F}_5}$. Since all C's pass through a common $\mathbf{F}_5$-point in $X_{\mathbf{F}_5}$ (namely, a supersingular point), it follows that the $J_5(C)$'s for $C \neq C_\infty$ are equal to a common point in $\mathbf{A}^1(\mathbf{F}_5)$. It remains to show that $J_5(C) \neq 0$ for $C \neq C_\infty$.

Let $\gamma = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ with $c = \pm 2$, so $[\gamma](\infty) = 0$ by definition. Hence, $[\gamma]$ must preserve C_∞. It follows that via the contraction map J_5, the involution $[\gamma]$ of $X(5)^{\rm can}$ is intertwined with an involution of $\mathbf{P}^1_{\mathbf{Z}[\zeta_5]}$ that switches $[1:0]$ and $[0:1]$. Such an involution must be $t \mapsto u/t$ for $u \in \mathbf{Z}[\zeta_5]^\times$. That is, $J_5 \circ [\gamma] = u/J_5$. It follows that $J_5^{-1}([0:1]) = [\gamma](J_5^{-1}([1:0])) = \{0\}$. This is disjoint from all $C \neq C_\infty$, so $J_5(C) \neq 0$ for $C \neq C_\infty$. ■

Remark 5.4. For irreducible components C of $X_{\mathbf{F}_5}$ distinct from C_∞, the common point $J_5(C) \in \mathbf{F}_5^\times$ is equal to -2. To verify this fact (which we will not use), it suffices to compute $j_{5,\zeta}$ on $X_\zeta(5)$ at any cusp other than 0_ζ and ∞_ζ (for a single choice of ζ). In Table B.1 we list of values of $j_{5,\zeta}$ at the cusps when using $\zeta = e^{2\pi i/5}$ and working with τ in the connected component of $\mathbf{C} - \mathbf{R}$ that contains $i = \sqrt{-1}$. By inspection of the table we see that these values have reduction -2 in $\mathbf{F}_5$ except at the cusps 0_ζ and ∞_ζ.

We have noted in Remark 5.3 that the zero and polar schemes for J_5 are equal to the cuspidal sections 0 and ∞ respectively. These two sections are switched by the involution w of $X(5)^{\rm can}$ that is induced by $\pm\begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$, and a key fact is that J_5 intertwines w with an involution of $\mathbf{P}^1_{\mathbf{Z}[\zeta_5]}$:

Corollary 5.5. *The identity $J_5 \circ w = -1/J_5$ holds.*

Proof. By Theorem 5.2 and Remark 5.3, $J_5 \circ w = u/J_5$ for some $u \in \mathbf{Z}[\zeta_5]^\times$. Just as $X(5)^{\mathrm{can}}$ and J_5 descend to $X_\mu(5)$ and $j_{5,\mu}$ over $\mathbf{Z}[1/5]$, it is clear that the action on $X(5)^{\mathrm{can}}$ by diagonal matrices in $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ also descends over $\mathbf{Z}[1/5]$. In particular, w descends, and so $u \in \mathbf{Q}$. Thus, $u = \pm 1$. To compute u, we use analysis as follows. For the lift $\widetilde{\gamma} = \begin{pmatrix} 2 & 5 \\ 5 & 13 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ of $\begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$, we must have $j_5 \circ \widetilde{\gamma} = u/j_5$. However, via (4.6) and (4.7), it is a simple analytic calculation with the transformation law (4.5) to check that $j_5 \circ \widetilde{\gamma}$ has q-expansion with initial term $-q_\tau^{1/5}$. Thus, $u = -1$. ∎

We now obtain a geometric proof of [1, Thm. 6.2]:

Corollary 5.6. *If $\tau \in \mathbf{C} - \mathbf{R}$ is quadratic over $\mathbf{Q}$, then $F(\tau)$ is an algebraic integral unit; equivalently, $j_5(\tau)$ is an algebraic integral unit.*

Proof. Fix a primitive 5th root of unity $\zeta \in \mathbf{C}$, and use this to consider $\mathbf{C}$ as a $\mathbf{Z}[\zeta_5]$-algebra. The point τ maps to a point $x_\tau = \pi_\zeta(\tau) \in X_\zeta(5) = X(5)^{\mathrm{can}}(\mathbf{C})$, and $j_5(\tau) = J_5(x_\tau)$. Since τ is imaginary quadratic, $\mathbf{C}^\times/q_\tau^{\mathbf{Z}}$ is a CM elliptic curve. Thus, x_τ must be an algebraic point. Let $K \subseteq \mathbf{C}$ be a number field containing $\mathbf{Q}(\zeta)$ such that x_τ is a K-point of $X(5)^{\mathrm{can}}$, and hence $J_5(x_\tau) \in \mathbf{P}^1(K) \subseteq \mathbf{P}^1(\mathbf{C})$. We wish to investigate the properties of $J_5(x_\tau)$.

The ring of integers $\mathscr{O}_K$ of K is Dedekind, so we may use the valuative criterion for properness to uniquely extend x_τ to a map $\widetilde{x}_\tau : \operatorname{Spec} \mathscr{O}_K \to X(5)^{\mathrm{can}}$. We want to prove that $J_5(\widetilde{x}_\tau) \in \mathbf{P}^1(\mathscr{O}_K)$ is disjoint from the sections $[0:1]$ and $[1:0]$ in $\mathbf{P}^1$. By construction $J_5^{-1}([1:0]) = \{\infty\}$. By Corollary 5.5, $J_5^{-1}([0:1]) = \{0\}$. Thus, to prove that $j_5(\tau)$ is an algebraic integral unit it suffices to prove that (the image of) $\widetilde{x}_\tau$ is disjoint from the cuspidal subscheme. This disjointness is clear, since specialization into a cusp forces multiplicative reduction, yet CM elliptic curves have potentially good reduction at all places. ∎

We would like to determine the field $\mathbf{Q}(\tau, j_5(\tau)) \subseteq \mathbf{C}$ for any imaginary quadratic $\tau \in \mathbf{C} - \mathbf{R}$. Since $\mathbf{Q}(X_\mu(5)) = \mathbf{Q}(j_{5,\mu})$ and $j_{5,\mu} = j_{5,\zeta} \circ \pi_\zeta$ for $\zeta = e^{\pm 2\pi i/5}$, Theorem 3.2 and Corollary 3.3 yield:

Corollary 5.7. *Let $\tau \in \mathbf{C} - \mathbf{R}$ be quadratic over $\mathbf{Q}$. Let $K = \mathbf{Q}(\tau)$, and let $\rho_\tau : \mathbf{A}_K^\times \to \mathrm{GL}_2(\mathbf{A}_\mathbf{Q})$ be the canonical representation in* (3.2)*. Let $\mathscr{O}_\tau \subseteq \mathbf{C}$ be the CM-order of $\mathbf{C}^\times/q_\tau^{\mathbf{Z}}$, and let*

$$V = \mathbf{Q}^\times \cdot \left\{ g = (g_\infty, g^\infty) \in \mathrm{GL}_2(\mathbf{R}) \times \mathrm{GL}_2(\mathbf{A}_\mathbf{Q}^\infty) \mid \det g_\infty > 0,\ g^\infty \in \mathrm{GL}_2(\widehat{\mathbf{Z}}),\ g^\infty \equiv \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \bmod 5 \right\}.$$

The extension $K(j_5(\tau))/K$ is the abelian extension of K with associated open subgroup

$$(K^\times \cdot \{ s \in \mathbf{A}_K^\times \mid \rho_\tau(s) \in V \})/K^\times \subseteq \mathbf{A}_K^\times/K^\times. \tag{5.1}$$

In particular, $K(j_5(\tau))/K$ is unramified away from $5[\mathscr{O}_K : \mathscr{O}_\tau]$.

If τ is 5-integral then $K(j_5(\tau))$ is contained in the ray class field of conductor $5[\mathscr{O}_K : \mathscr{O}_\tau]$ for K, and $K(j_5(\tau))$ is equal to this ray class field if moreover $\mathscr{O}_\tau = \mathscr{O}_K$ and τ is a 5-unit.

6. Modular Equations

In this section we use the integral models from §2 and our work in §5 to show that for any positive integer n relatively prime to 5, $j_5(\tau)$ and $j_5(n\tau)$ satisfy a "modular equation" $F_n(j_5(\tau), j_5(n\tau)) = 0$ for a suitable primitive $F_n \in \mathbf{Z}[X, Y]$ that is absolutely irreducible over $\mathbf{Q}$. We then establish a Kronecker congruence for such F_n's and we analyze the case $n = 5$. This is motivated by the algebro-geometric treatment of the classical modular polynomials, except that there are two complications: $X_\zeta(5)$ has more than one cusp, and we need to use *two* moduli schemes to get a result over $\mathbf{Z}$.

The modular polynomials F_n are going to be constructed by geometric methods, as this provides the clearest way to analyze the properties of F_n (such as absolute irreducibility over $\mathbf{Q}$ and congruences modulo p). This construction rests on the interaction of $\Gamma_\mu(N)$-structures and $\Gamma_0(n)$-structures for $N = 5$ and $\gcd(n, N) = 1$, so let us begin by defining a moduli functor that mixes both kinds of structures. For $N \geq 3$, consider the enhanced moduli functor $\mathscr{M}$ that classifies triples (E, ι, C) where E is an elliptic curve, ι is a $\Gamma_\mu(N)$-structure, and $C \hookrightarrow E$ is a $\Gamma_0(n)$-structure in the sense of [10, §3.4] (so if n is a unit on the base then C is an order-n finite étale subgroup of E such that C is cyclic on geometric fibers). The $\Gamma_0(n)$-moduli problem on elliptic curves is relatively representable and finite flat [10, §4.5, 6.6.1]; applying this to the universal object over $Y_\mu(N)$ yields the existence of a fine moduli scheme $Y(\Gamma_\mu(N), \Gamma_0(n))$ for $\mathscr{M}$ on the category of $\mathbf{Z}[1/N]$-schemes, with a forgetful map

$$\pi_n : Y(\Gamma_\mu(N), \Gamma_0(n)) \to Y(\Gamma_\mu(N)) = Y_\mu(N)$$

that is finite and flat. By [10, 6.6.1], $Y(\Gamma_\mu(N), \Gamma_0(n))$ is an affine curve over $\operatorname{Spec} \mathbf{Z}[1/N]$ and it is regular.

The finite flat j-maps to $\mathbf{A}^1_{\mathbf{Z}[1/N]}$ allow us to define compactifications $X(\Gamma_\mu(N), \Gamma_0(n))$ and $X_\mu(N)$ by normalizing $\mathbf{P}^1_{\mathbf{Z}[1/N]}$ in the function fields of the affine normal modular curves $Y(\Gamma_\mu(N), \Gamma_0(n))$ and $Y_\mu(N)$ (this recovers the same $X_\mu(N)$ that we defined in §2 via moduli-theoretic methods). Thus, we get a natural finite map

$$\overline{\pi}_n : X(\Gamma_\mu(N), \Gamma_0(n)) \to X_\mu(N)$$

between normal proper $\mathbf{Z}[1/N]$-curves, and over the open subscheme $Y_\mu(N) \subseteq X_\mu(N)$ this recovers π_n. Since $\gcd(n, N) = 1$, there is a natural automorphism w_n on $Y(\Gamma_\mu(N), \Gamma_0(n))$ whose action on moduli is

$$w_n : (E, \iota, C) \mapsto (E/C, \iota', E[n]/C)$$

with ι' defined as the composite isomorphism

$$\iota' : \mu_N \times \mathbf{Z}/N\mathbf{Z} \overset{n^{-1}\times 1}{\to} \mu_N \times \mathbf{Z}/N\mathbf{Z} \overset{\iota}{\to} E[N] \simeq (E/C)[N],$$

where the intervention of n^{-1} in the first step ensures that ι' is a symplectic isomorphism. Observe that we have a commutative diagram

$$\begin{array}{ccc} Y(\Gamma_\mu(N), \Gamma_0(n)) & \xrightarrow{w_n^2} & Y(\Gamma_\mu(N), \Gamma_0(n)) \\ \downarrow{\scriptstyle \pi_n} & & \downarrow{\scriptstyle \pi_n} \\ Y_\mu(N) & \xrightarrow[{[\delta_n]}]{} & Y_\mu(N) \end{array} \tag{6.1}$$

with

$$\delta_n = \begin{pmatrix} n & 0 \\ 0 & n^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}). \tag{6.2}$$

In terms of moduli, the finite flat covering $\pi'_n = \pi_n \circ w_n$ sends (E, ι, C) to $(E/C, \iota')$, where ι' is defined as above. Since the cuspidal locus is quasi-finite over the base $\operatorname{Spec} \mathbf{Z}[1/N]$, the involution w_n of the normal $\mathbf{Z}[1/N]$-curve $Y(\Gamma_\mu(N), \Gamma_0(n))$ uniquely extends to an involution $\overline{w}_n$ of the normal proper $\mathbf{Z}[1/N]$-curve $X(\Gamma_\mu(N), \Gamma_0(n))$. Thus, we may define the finite map $\overline{\pi}'_n = \overline{\pi}_n \circ \overline{w}_n$ extending π'_n. The compatibility (6.1) extends to compactified modular curves in the evident manner. The maps $\overline{\pi}_n$ and $\overline{\pi}'_n$ are analogues of the classical degeneracy maps for $N = 1$.

Consider the proper morphism

$$\overline{\pi}_n \times \overline{\pi}'_n : X(\Gamma_\mu(N), \Gamma_0(n)) \to X_\mu(N) \times_{\mathbf{Z}[1/N]} X_\mu(N).$$

This map is quasi-finite, since there are at most finitely many cyclic n-isogenies between a pair of elliptic curves over an algebraically closed field, and so it is finite. It is generically injective (since a generic pair of elliptic curves admit at most one cyclic isogeny of a given degree, up to sign), and hence it is generically a closed immersion because the irreducible $X(\Gamma_\mu(N), \Gamma_0(n))$ has generic characteristic zero. Thus, the regular $X(\Gamma_\mu(N), \Gamma_0(n))$ maps birationally onto its image under $\overline{\pi}_n \times \overline{\pi}'_n$, but this image generally has singularities.

Definition 6.1. The *Kroneckerian model* $Z_{N,n}$ of $X(\Gamma_\mu(N), \Gamma_0(n))$ is the scheme-theoretic image of the finite map $\overline{\pi}_n \times \overline{\pi}'_n$.

Since $X_\mu(N)$ has a moduli-theoretic interpretation for $N \geq 3$, the rigidity of generalized elliptic curves (i.e., the triviality of the deformation theory of morphisms) ensures that the map $X(\Gamma_\mu(N), \Gamma_0(n)) \to Z_{N,n}$ is formally unramified, and so $Z_{N,n}$ has much milder singularities than in the classical case $N = 1$.

The Krockerian model $Z_{N,n}$ is a proper flat $\mathbf{Z}[1/N]$-scheme that is reduced. The map $X(\Gamma_\mu(N), \Gamma_0(n))_{\mathbf{Q}} \to Z_{N,n,\mathbf{Q}}$ between integral proper $\mathbf{Q}$-curves expresses $X(\Gamma_\mu(N), \Gamma_0(n))_{\mathbf{Q}}$ as the normalization of $Z_{N,n,\mathbf{Q}}$. In particular, $Z_{N,n,\mathbf{Q}}$ is geometrically irreducible, and hence is geometrically connected. The fibers of the proper flat map $Z_{N,n} \to \operatorname{Spec} \mathbf{Z}[1/N]$ are therefore geometrically connected curves (and are reducible in characteristics dividing n). Motivated by the classical case $N = 1$, we will construct the modular polynomials F_n for j_5 by studying $Z_{5,n,\mathbf{Q}}$ as an irreducible curve on the surface

$$X_\mu(5)_{\mathbf{Q}} \times X_\mu(5)_{\mathbf{Q}} = \mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}.$$

Lemma 6.2. *For $N \geq 3$ and $\gcd(N, n) = 1$, the following properties hold.*

1. *The projections $Z_{N,n,\mathbf{Q}} \rightrightarrows X_\mu(N)_{\mathbf{Q}}$ are finite with generic degree $[\Gamma(1) : \Gamma_0(n)] = n \prod_{p|n}(1 + 1/p)$.*
2. *Let σ be the involution of $X_\mu(N) \times X_\mu(N)$ that switches the factors. Using (6.2), the self-map $\sigma \circ (1 \times [\delta_{n^{-1}}])$ on $X_\mu(N) \times X_\mu(N)$ restricts to the identity on $Z_{N,n}$. In particular, if $n \equiv \pm 1 \bmod N$ then σ acts as the identity on $Z_{N,n}$.*

Proof. Since $X(\Gamma_\mu(N), \Gamma_0(n))_{\mathbf{Q}} \to Z_{N,n,\mathbf{Q}}$ is the normalization, and so is a finite birational isomorphism, (1) follows from the fact that $\overline{\pi}_n$ and $\overline{\pi}'_n = \overline{\pi}_n \circ \overline{w}_n$ have common degree equal to the degree of the $\Gamma_0(n)$-moduli problem: $[\Gamma(1) : \Gamma_0(n)]$.

To establish (2), we first note that $Z_{N,n}$ is equal to the scheme-theoretic image of $(\overline{\pi}_n \times \overline{\pi}'_n) \circ \phi$ for any automorphism ϕ of $X(\Gamma_\mu(N), \Gamma_0(n))$. Taking $\phi = \overline{w}_n$, we see that $Z_{N,n}$ is the scheme-theoretic image of

$$(\overline{\pi}_n \times \overline{\pi}'_n) \circ \overline{w}_n = \overline{\pi}'_n \times (\overline{\pi}_n \circ \overline{w}_n^2) = \overline{\pi}'_n \times ([\delta_n] \circ \overline{\pi}_n) = (1 \times [\delta_n]) \circ (\overline{\pi}'_n \times \overline{\pi}_n).$$

Thus, if σ denotes the involution of $X_\mu(N) \times X_\mu(N)$ that switches the factors, then $\sigma \circ (1 \times [\delta_{n^{-1}}])$ is the identity on $Z_{N,n}$. ■

Now specialize to the case $N = 5$. By Theorem 5.2, $j_{5,\mu}$ defines an isomorphism $X_\mu(5) \simeq \mathbf{P}^1_{\mathbf{Z}[1/5]}$ carrying ∞ to $[1 : 0]$. Thus, for any n relatively prime to 5 we may consider the Kroneckerian model $Z_{5,n}$ as a reduced closed subscheme in $\mathbf{P}^1_{\mathbf{Z}[1/5]} \times \mathbf{P}^1_{\mathbf{Z}[1/5]}$ that is proper and flat over $\mathbf{Z}[1/5]$ with geometrically connected fibers of dimension 1, and with geometrically integral generic fiber over $\mathbf{Q}$. Let $\mathscr{Z}_n$ be the closure of $Z_{5,n}$ in $\mathbf{P}^1_{\mathbf{Z}} \times \mathbf{P}^1_{\mathbf{Z}}$, so this is a proper flat curve over $\operatorname{Spec} \mathbf{Z}$. In particular, it must be the closure of its irreducible generic fiber $Z_{5,n,\mathbf{Q}} \subseteq \mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}$. By Lemma 6.2(1), the projections

$$Z_{5,n,\mathbf{Q}} \rightrightarrows \mathbf{P}^1_{\mathbf{Q}}$$

are finite with generic degree equal to $\deg \pi_n$. Thus, $Z_{5,n,\mathbf{Q}} \subseteq \mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}$ is the zero-scheme of an irreducible bihomogeneous absolutely irreducible polynomial $\widetilde{F}_n(X_0, X_1; Y_0, Y_1)$ with degree $\deg \pi_n$ in both the X's and the Y's. Moreover, both X_0 and Y_0 must arise in $\widetilde{F}_n$ (since $Z_{N,n,\mathbf{Q}}$ meets $Y_\mu(N)_{\mathbf{Q}} \times Y_\mu(N)_{\mathbf{Q}}$) and so by irreducibility it follows that the dehomogenization $\widetilde{F}_n(X, 1; Y, 1)$ has degree $\deg \pi_n$ in each of X and Y.

Let $F_n(X, Y)$ be a primitive polynomial over $\mathbf{Z}$ that is a scalar multiple of $\widetilde{F}_n(X, 1; Y, 1)$ (this determines F_n up to sign), so $F_n \in \mathbf{Z}[X, Y]$ is geometrically irreducible over $\mathbf{Q}$ with degree $\deg \pi_n$ in each of X and Y. We claim that the *modular equation*

$$F_n(j_5(\tau), j_5(n\tau)) = 0$$

holds. In the complex-analytic theory, the map π'_n corresponds to $\tau \mapsto n\tau$, and hence the functions $j_{5,\mu} \circ \overline{\pi}_n$ and $j_{5,\mu} \circ \overline{\pi}'_n$ on $X(\Gamma_\mu(N), \Gamma_0(n))$ correspond to the functions $j_5(\tau)$ and $j_5(n\tau)$ on $\mathbf{C} - \mathbf{R}$. Thus, the modular equation follows from the definition of F_n. To remove the sign ambiguity in the definition of F_n, we first must prove:

Theorem 6.3. *There are unique monomial terms $X^{r_n}Y^{\deg \pi_n}$ and $Y^{s_n}X^{\deg \pi_n}$ in F_n with respective Y-degree and X-degree $\deg \pi_n$, and both occur in F_n with coefficient in $\mathbf{Z}^\times = \{\pm 1\}$.*

Proof. We may (and do) work over $\mathbf{Z}[\zeta_5]$, and we may work with the $\Gamma(5)^{\mathrm{can}}$-moduli functor instead of the $\Gamma_\mu(5)$-moduli functor. Consider the finite flat maps

$$\overline{\pi}_n, \overline{\pi}'_n : X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n)) \rightrightarrows X(5)^{\mathrm{can}}$$

over $\operatorname{Spec} \mathbf{Z}[\zeta_5]$ and the automorphism $\overline{w}_n$ of $X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n))$; these are defined just as we define the maps $\overline{\pi}_n$, $\overline{w}_n$, and $\overline{\pi}'_n$ over $\mathbf{Z}[1/5]$.

The key fact is that $\overline{w}_n$ preserves $\overline{\pi}_n^{-1}(\{0, \infty\})$. To verify this property, we first note that the cuspidal subscheme $X(5)^{\mathrm{can}}_\infty$ is a disjoint union of copies of $\operatorname{Spec} \mathbf{Z}[\zeta_5]$, and $\overline{\pi}_n^{-1}(X(5)^{\mathrm{can}}_\infty)$ is the cuspidal subscheme of $X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n))$; also, $\overline{w}_n$ restricts to an automorphism of the cuspidal subscheme. Since $\overline{\pi}_n$ is a finite flat surjection, it is therefore enough to verify that $\overline{w}_n$ preserves $\overline{\pi}_n^{-1}(\{0, \infty\})$ on fibers over a single point of $\operatorname{Spec} \mathbf{Z}[\zeta_5]$. We will work at the unique point of characteristic 5.

As we noted in the proof of Theorem 5.2, the fiber $X(5)^{\mathrm{can}}_{\mathbf{F}_5}$ consists of 6 copies of $\mathbf{P}^1_{\mathbf{F}_5}$ glued transversally at a unique (supersingular) $\mathbf{F}_5$-point, and there are exactly 2 cusps on each of these irreducible components, with one of the irreducible components C_∞ containing ∞ and 0 as its cusps. This component C_∞ is characterized by the property that its geometric points (E, ι) have $\iota(1, 0) = 0$.

We similarly find (using the methods as in the proof of [10, 13.7.6]) that $X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n))_{\mathbf{F}_5}$ is a reduced curve with 6 irreducible components that are glued at supersingular points, and that the finite flat projection

$$\overline{\pi}_n : X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n)) \to X(5)^{\mathrm{can}}$$

sets up a bijection between these 6 irreducible components and the 6 irreducible components of $X(5)^{\mathrm{can}}_{\mathbf{F}_5}$. Let C'_∞ be the irreducible component of $X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n))_{\mathbf{F}_5}$ whose non-cuspidal geometric points (E, ι, C) have $\iota(1, 0) = 0$, so $C'_\infty = \overline{\pi}_n^{-1}(C_\infty)$. An inspection of the definition of w_n shows that $\overline{w}_n$ preserves the vanishing property for the 5-torsion point $\iota(1, 0)$, so $\overline{w}_n$ carries C'_∞ to itself. Thus, $\overline{w}_n$ preserves $\overline{\pi}_n^{-1}(\{0, \infty\})$ in characteristic 5, and hence over $\mathbf{Z}[\zeta_5]$.

By Theorem 5.2, j_{5,ζ_5} identifies $\mathbf{P}^1_{\mathbf{Z}[\zeta_5]}$ with the contraction of $X(5)^{\mathrm{can}}$ along the mod-$(1-\zeta_5)$ components distinct from C_∞. Let $\widetilde{X}$ denote the normal proper flat $\mathbf{Z}[\zeta_5]$-curve obtained by contracting $X(\Gamma(5)^{\mathrm{can}}, \Gamma_0(n))$ along the mod-$(1 - \zeta_5)$ components distinct from C'_∞ (see [3, 6.7/3] for the existence of such a contraction, using some connected components of the cuspidal divisor to construct the divisor in the hypothesis in [3, 6.7/3]). Since the automorphism $\overline{w}_n$ preserves C'_∞, it uniquely factors through the contraction to define an automorphism $\widetilde{w}_n$ of $\widetilde{X}$. Likewise, $\overline{\pi}_n$ uniquely factors through the contraction to define a proper surjective map $\widetilde{\pi}_n : \widetilde{X} \to \mathbf{P}^1_{\mathbf{Z}[\zeta_5]}$ that must be quasi-finite, and hence finite, as well as flat (since it is a finite map from a normal surface to a regular surface; see [16, 23.1]). We define $\widetilde{\pi}'_n = \widetilde{\pi}_n \circ \widetilde{w}_n$, and let U be the common preimage of $\mathbf{G}_m = \mathbf{P}^1 - \{[0 : 1], [1 : 0]\}$ under $\widetilde{\pi}_n$ and $\widetilde{\pi}'_n$.

Using the structure map $\widetilde{\pi}_n$, all regular functions on U are integral over over $\mathbf{Z}[\zeta_5][j_5, 1/j_5]$. Using the structure map $\widetilde{\pi}'_n$, all regular functions on U are integral over $\mathbf{Z}[\zeta_5][j_5(n\tau), 1/j_5(n\tau)]$, where we adopt the usual abuse of notation by writing $j_5(n\tau)$ to denote the function $\tau \mapsto j_5(n\tau)$. We conclude that the irreducible minimal monic polynomial for the function $j_5(\tau)$ over the field $\mathbf{Q}(j_5(n\tau))$ has coefficients in $\mathbf{Z}[\zeta_5][j_5(n\tau), 1/j_5(n\tau)]$, and similarly with the roles of the functions $j_5(\tau)$ and $j_5(n\tau)$ reversed. These minimal polynomials are exactly the $\mathbf{Q}(Y)^\times$- and $\mathbf{Q}(X)^\times$-multiples of $F_n(X, Y)$ that are respectively monic in X and monic in Y, so it follows that the irreducible $F_n(X, Y) \in (\mathbf{Z}[X])[Y]$ has its dominant Y-term (with Y-degree $\deg \pi_n$) with a coefficient that is a unit in $\mathbf{Z}[X, 1/X]$. That is, there is a unique monomial term $X^{r_n}Y^{\deg \pi_n}$ in F_n and its $\mathbf{Z}$-coefficient is a unit; by the same argument, there is a unique monomial term $Y^{s_n}X^{\deg \pi_n}$ in F_n with X-degree $\deg \pi_n$ and its $\mathbf{Z}$-coefficient is a unit. ∎

The two unit coefficients in Theorem 6.3 need not be equal. We now make an arbitrary choice (that is meaningful because of Theorem 6.3):

Definition 6.4. The primitive polynomial $F_n \in \mathbf{Z}[X,Y]$ is the unique one that is absolutely irreducible over $\mathbf{Q}$, satisfies $F_n(j_5(\tau), j_5(n\tau)) = 0$, and has its unique monomial $X^{r_n}Y^{\deg \pi_n}$ with maximal Y-degree occur with coefficient equal to 1.

An important symmetry property of F_n is:

Theorem 6.5. *Let $n > 1$ be an integer. If $n \equiv \pm 1 \bmod 5$ then $F_n(Y,X) = F_n(X,Y)$. If $n \equiv \pm 2 \bmod 5$ then $X^{\deg \pi_n} F_n(Y, -1/X) = \varepsilon_n F_n(X,Y)$ with $\varepsilon_n = \pm 1$, where $\varepsilon_n = -1$ if and only if one of the following mutually exclusive conditions holds:*

1. *$n = 2m^2$ with $m \geq 1$ and the odd part m_{odd} satisfying $m_{\mathrm{odd}} \equiv \pm 1 \bmod 5$ when m is odd, $m_{\mathrm{odd}} \equiv \pm 2 \bmod 5$ when m is even and not a power of 2, and $m = 4^a$ with $a \geq 1$ when $m > 1$ and m is a power of 2,*
2. *$n = 4p^a$ with $a \equiv 3 \bmod 4$ and an odd prime $p \equiv \pm 2 \bmod 5$,*
3. *$n = 4^{2b+1}p^a m^2$ with odd $m \geq 1$ and an odd prime $p \nmid m$ such that $a \equiv 1 \bmod 4$, $p \equiv \pm 2 \bmod 5$, and $m > 1$ or $b > 0$.*

Remark 6.6. The least $n > 2$ such that $n \equiv \pm 2 \bmod 5$ and $\varepsilon_n = -1$ is $n = 32$; the second-smallest such n is $n = 72$. Note that the sign ε_n is invariant under replacing F_n with $-F_n$, and so it is independent of our arbitrary choice of sign-convention in the definition of F_n.

Proof. Since $[\delta_n]$ as in (6.1) acts on $\mathbf{P}^1_{\mathbf{Q}} = X_\mu(5)_{\mathbf{Q}}$ via the identity for $n \equiv \pm 1 \bmod 5$ and via $t \mapsto -1/t$ for $n \equiv \pm 2 \bmod 5$ (by Corollary 5.5), Lemma 6.2(2) implies that the zero schemes of $F_n(Y,X)$ and $F_n(X,Y)$ (say over $\mathbf{Q}$) coincide for $n \equiv \pm 1 \bmod 5$, and the zero schemes of $X^{\deg \pi_n} F_n(Y,-1/X)$ and $F_n(X,Y)$ (say over $\mathbf{Q}$) coincide for $n \equiv \pm 2 \bmod 5$. Thus, this gives the result up to a $\mathbf{Q}^\times$-multiple. By primitivity, there is in fact only an ambiguity of sign. We cannot have $F_n(X,Y) = -F_n(Y,X)$, as then $F_n(X,X) = 0$ and this contradicts the fact that the irreducible $F_n(X,Y)$ cannot be divisible by $X - Y$ (F_n has degree $\deg \pi_n$ in each variable, and $\deg \pi_n > 1$ since $n > 1$).

It remains to compute the sign ε_n such that $X^{\deg \pi_n} F_n(Y,-1/X) = \varepsilon_n F_n(X,Y)$ for $n \equiv \pm 2 \bmod 5$. Recall that we defined F_n by the property that the unique monomial in F_n with Y-degree $\deg \pi_n$ has coefficient of 1. That is, F_n modulo multiplication by $X^{\mathbf{Z}}$ is equivalent to a monic polynomial in Y in $\mathbf{Z}[X,1/X][Y]$, and this monic polynomial agrees with $\varepsilon_n F_n(Y,-1/X)$ up to multiplication by $X^{\mathbf{Z}}$. The unique monomial-term in $F_n(X,Y)$ with X-degree $\deg \pi_n$ has the form $u_n Y^{s_n} X^{\deg \pi_n}$ for some $u_n \in \{\pm 1\}$, so $F_n(Y,-1/X)$ has its top-degree Y-term equal to $(-1)^{s_n} u_n Y^{\deg \pi_n}$ modulo $X^{\mathbf{Z}}$. Thus, $\varepsilon_n = (-1)^{s_n} u_n$. Since $j_5(\tau) = q_\tau^{-1/5} + \dots$, if we write $F_n(j_5, Y) \bmod^\times j_5^{\mathbf{Z}}$ as a Y-monic element in $\mathbf{Z}[j_5, Y] \subseteq \mathbf{Z}(\!(q_\tau^{1/5})\!)[Y]$ then the unique monomial $(q_\tau^{-1/5})^{\alpha_n} Y^{\beta_n}$ with the highest q-pole has Y-degree s_n and coefficient $u_n = (-1)^{s_n}\varepsilon_n$ (note that generally $\alpha_n \neq \deg \pi_n$ because we have multiplied $F(j_5, Y)$ by a power of j_5 to make it monic in Y). We shall use this viewpoint to compute ε_n by studying $F_n(j_5, Y)$ over $\mathbf{Q}(\zeta)(\!(q_\tau^{1/5})\!)$.

Let $\Delta'_n = \Gamma(5)\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}\Gamma(5)$, so $\Gamma(5)\backslash\Delta'_n$ has size $\deg \pi_n = n\prod_{p|n}(1 + 1/p)$. Since $\gcd(n,5) = 1$, modulo multiplication by $j_5^{\mathbf{Z}}$ we have

$$F_n(j_5, Y) \equiv \prod_{\alpha \in \Gamma(5)\backslash\Delta'_n} (Y - j_5 \circ \alpha) \bmod^\times j_5^{\mathbf{Z}} \tag{6.3}$$

(where we are considering multiplicative congruence). To analyze $j_5 \circ \alpha$, we need to find a convenient set of coset representatives for $\Gamma(5)\backslash\Delta'_n$. To compute such a set, recall (as in [19, Prop. 3.36] in much greater generality) that a set of representatives for $\Gamma(5)\backslash\{\alpha \in \mathrm{End}_{\mathbf{Z}}(\mathbf{Z}^2) \mid \det \alpha = n\}$ is

$$\left\{ \sigma_a \cdot \begin{pmatrix} a & 5b \\ 0 & d \end{pmatrix} \mid ad = n,\ 0 \leq b < d,\ a > 0 \right\}, \tag{6.4}$$

where $\sigma_a \in \mathrm{SL}_2(\mathbf{Z})$ depends only on $a \bmod 5$ and is a lift of $\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$. For example, for definitiveness we can take

$$\sigma_{\pm 1} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_{\pm 2} = \pm \begin{pmatrix} 2 & 5 \\ 5 & 13 \end{pmatrix}. \tag{6.5}$$

We are interested in only the subset $\Gamma(5)\backslash\Delta'_n$, and obviously the representatives for such left-cosets must be primitive matrices and so a set of representatives for $\Gamma(5)\backslash\Delta'_n$ is contained in

$$\left\{ \sigma_a \cdot \begin{pmatrix} a & 5b \\ 0 & d \end{pmatrix} \mid ad = n, \ 0 \le b < d, \ a > 0, \ \gcd(a,b,d) = 1 \right\}; \tag{6.6}$$

an elementary count (via decomposition along the prime factorization of n) shows that the set (6.6) has size $n \cdot \prod_{p|n}(1 + 1/p)$, and so (6.6) is a set of representatives for $\Gamma(5)\backslash\Delta'_n$. Note that the preceding calculations are valid for any n relatively prime to 5 without requiring $n \equiv \pm 2 \bmod 5$ (and so we may and will use the above conclusions in our later analysis of the size of the coefficients of F_n for *any* large n).

For $\alpha_{a,b,d} = \sigma_a \begin{pmatrix} a & 5b \\ 0 & d \end{pmatrix}$ in the set (6.4), we have

$$j_5 \circ \alpha_{a,b,d} = (j_5 \circ \sigma_a)((a\tau + 5b)/d)$$

with $j_5 \circ \sigma_a$ only depending on $\pm a \bmod 5$. Since $a/d > 0$ and

$$-j_5 \circ \sigma_{\pm 1} = -q_\tau^{-1/5} + \dots, \ \ -j_5 \circ \sigma_{\pm 2} = q_\tau^{1/5} + \dots,$$

we see that $-j_5 \circ \alpha_{a,b,d}$ has a pole if and only if $a \equiv \pm 1 \bmod 5$. Thus, there is a unique set of $\alpha_{a,b,d}$'s in (6.6) such that the product of the corresponding $-j_5 \circ \alpha_{a,b,d}$'s has a maximal-order pole, namely the product for those $\alpha_{a,b,d}$'s with $a \equiv \pm 1 \bmod 5$.

We now restrict attention to $\alpha_{a,b,d}$'s with $\gcd(a,b,d) = 1$; these are the $\alpha_{a,b,d}$'s in the set (6.6). For a fixed factorization $n = ad$ with $a > 0$ and $a \equiv \pm 1 \bmod 5$, we have

$$\prod_{b \in B_d} -j_5 \circ \alpha_{a,b,d} = \prod_{b \in B_d} -(e^{-2\pi i(a\tau+5b)/d} + \dots) = (-1)^{|B_d|} \zeta_d^{\sum_{b \in B_d} -5b} q_\tau^{-a/d} + \dots, \tag{6.7}$$

with $B_d = \{b \,|\, 0 \le b < d, (b, n/d, d) = 1\}$. To compute the power of ζ_d in (6.7), we apply the following lemma to the primitive dth root of unity ζ_d^5:

Lemma 6.7. *For positive integers d and k with $k|d$, and ζ_d a primitive dth root of unity,*

$$\zeta_d^{\sum_{0 \le b < d, (b,k)=1} -b} = (-1)^{-1 + d/k + \delta_{k,2}}$$

where $\delta_{k,2} = 1$ for $k = 2$ and $\delta_{k,2} = 0$ otherwise.

Proof. The case $k = 1$ is straightforward, so we may assume $k > 1$. Thus, for $0 \le b < d$ we may use the division algorithm to write $b = kq + r$ with $0 \le q < d/k$ and $0 \le r < k$ with $(k, r) = 1$ (or more loosely, $r \in (\mathbf{Z}/k\mathbf{Z})^\times$). Since each such r shows up d/k times, if we define $\zeta_k = \zeta_d^{d/k}$ and $\zeta_{d/k} = \zeta_d^k$ then

$$\zeta_d^{\sum_{0 \le b < d, (b,k)=1} -b} = \zeta_{d/k}^{\sum_{0 \le q < d/k} q} \cdot \zeta_k^{\sum_{r \in (\mathbf{Z}/k\mathbf{Z})^\times} r} = (-1)^{d/k - 1} \cdot \zeta_k^{\sum_{r \in (\mathbf{Z}/k\mathbf{Z})^\times} r} = (-1)^{d/k-1}(-1)^{\varphi(k)}\Phi_k(0)$$

where $\Phi_k(0)$ is the constant term of the kth cyclotomic polynomial Φ_k that has degree $\varphi(k)$. Since $\Phi_k = \prod_{e|k}(X^e - 1)^{\mu(k/e)}$, we have $\Phi_k(0) = (-1)^{\sum_{e|k} \mu(k/e)} = 1$ since $k > 1$. Since $\varphi(k)$ is even for $k > 2$ whereas $\varphi(2) = 1$, we are done. ∎

By the lemma, for $a|n$ and $d = n/a$ with $a > 0$ and $a \equiv \pm 1 \bmod 5$, we get

$$\prod_{0 \le b < d, (b,(a,d))=1} -j_5 \circ \alpha_{a,b,d} = (-1)^{|B_d| - 1 + d/(a,d) + \delta_{(a,d),2}} q_\tau^{-a/d} + \dots. \tag{6.8}$$

The product of the terms in (6.8) over all a's gives the unique most polar contribution in the coefficients of F_n, so the product of the sign-coefficients on the right side of 6.8 over all factorizations $n = ad$ with $a > 0$ and $a \equiv \pm 1 \bmod 5$ is

$$\prod_{d|n, d\equiv \pm 2 \bmod 5} (-1)^{d/(n/d,d)+\delta_{(n/d,d),2}} = u_n \tag{6.9}$$

(with the product taken over positive divisors), and this dominant term arises from a product of t_n distinct $j_5 \circ \alpha$'s with

$$t_n = \sum_{d|n, d\equiv \pm 2 \bmod 5} |B_d| \tag{6.10}$$

(with the sum taken over positive divisors), so the most polar term occurs against $Y^{\deg \pi_n - t_n}$ in (6.3). Hence, $s_n = \deg \pi_n - t_n$. The case $n = 2$ is trivial, so we may assume $n > 2$, and so

$$\deg \pi_n = [\Gamma(1) : \Gamma_0(n)] = n \prod_{p|n} (1 + 1/p)$$

is even. Thus, $s_n \equiv t_n \bmod 2$, and so $(-1)^{s_n} = (-1)^{t_n}$. Using (6.9) and (6.10), we thereby get

(6.11)

$$\varepsilon_n = (-1)^{s_n} u_n = (-1)^{t_n} u_n = \prod_{d|n, d\equiv \pm 2 \bmod 5} (-1)^{-1+d/(n/d,d)+\delta_{(n/d,d),2}} = \prod_{d|n} \left(\frac{d}{5}\right)^{-1+d/(n/d,d)+\delta_{(n/d,d),2}}.$$

The exponent $-1 + d/(n/d, d) + \delta_{(n/d,d),2}$ is even when d is odd, so $\varepsilon_n = 1$ for odd n. This shows that if $\varepsilon_n = -1$ then n must be even; we will proceed by analyzing the cases $\mathrm{ord}_2(n) = 1$, $\mathrm{ord}_2(n) = 2$, and $\mathrm{ord}_2(n) > 2$.

Now we may suppose $n = 2^e n'$ with odd n' relatively prime to 5 and arbitrary $e \geq 1$. If $e = 1$, then $n' \equiv \pm 1 \bmod 5$ and $n' > 1$ (since $n > 2$). The contribution at $d = 2d'$ in (6.11) is $(d|5)$ and hence pairing up the contributions at $2d'$ and $2n'/d'$ (except if $d' = n'/d'$) gives a product of $(n'|5) = 1$ for each such pair of terms. Thus, the total product ε_n is equal to 1 if n' is not a square and is equal to $(m|5)$ if $n' = m^2$. This shows that if $\mathrm{ord}_2(n) = 1$ and $n > 2$ then $\varepsilon_n = -1$ if and only if $n = 2m^2$ with $m \equiv \pm 1 \bmod 5$, as desired.

If $e = 2$, then $n' \equiv \pm 2 \bmod 5$ (so n' is not a square) and the only possible non-trivial contributions to the product for ε_n in (6.11) are $(d|5) = -(d'|5)$ at $d = 2d'$ with $(d', n'/d') = 1$ and $(d|5) = (d'|5)$ at $d = 4d'$ without restriction on the divisor d' of n'. For the product of the first collection of such terms (at all $d = 2d'$ with $(d', n'/d') = 1$) we can pair up $2d'$ and $2n'/d'$ to get $(n'|5) = -1$ appearing half as many times as there are subsets of the set of prime factors of n'; any such power set has even size since $n' > 1$ (as then n' has a non-empty set of prime factors), and has size divisible by 4 if and only if n' has at least two prime factors. Thus, the divisors $d = 2d'$ with $(d', n'/d') = 1$ contribute a total product of -1 to ε_n in (6.11) when $n' > 1$ is an odd prime power (with the prime necessarily $\equiv \pm 2 \bmod 5$), and otherwise these divisors contribute a total product of 1 to ε_n; similarly, the total contribution to ε_n for the set of divisors $d = 4d'$ is

$$\prod_{d'|n'} \left(\frac{d'}{5}\right) = (-1)^{\sigma_0(n')/2}.$$

Thus, when $n = 4n'$ with odd n' we see that $\varepsilon_n = -1$ if and only if one of the following mutually exclusive conditions holds:

- $n = 4p^a$ for an odd prime $p \equiv \pm 2 \bmod 5$ and $a \equiv 3 \bmod 4$ (this ensures that $n \equiv \pm 2 \bmod 5$ and that $-(-1)^{\sigma_0(p^a)/2} = (-1)^{(a+3)/2}$ is equal to -1),
- $n = 4p^a m^2$ with an odd prime $p \equiv \pm 2 \bmod 5$ and an odd $m > 1$ not divisible by p such that $a \equiv 1 \bmod 4$ (this ensures that $n \equiv \pm 2 \bmod 5$ and that $(-1)^{\sigma_0(p^a m^2)/2} = (-1)^{(a+1)/2}$ is equal to -1).

It remains to consider $n = 2^e n'$ with n' odd and $e \geq 3$. Writing an even divisor d of n in the form $2^{e'}d'$ with $e' \geq 1$ and $d'|n'$, we get a contribution of $(d|5)$ at d in (6.11) in each of the following mutually exclusive cases:

- $(d, n/d) = 1$ (that is, $e' = e$ and $(d', n'/d') = 1$),
- $(d, n/d) = 2$ with $d/2$ odd (that is, $e' = 1$ and $(d', n'/d') = 1$),
- $(d, n/d) > 2$ with $d/(n/d, d)$ even (that is, $e/2 < e' \leq e - 1$ with the extra condition $(d', n'/d') \neq 1$ when $e' = e - 1$).

Note in particular that terms with $e/2 < e' < e - 1$ (vacuous for $e = 3$) contribute $(d|5)$ in (6.11) without restriction on d'. All other d's not mentioned in the preceding list make trivial contribution to ε_n (due to evenness on the exponent of $(d|5)$ in (6.11) for such d).

We first consider the case when e is even (so $e \geq 4$), so n' is odd and $n' \equiv \pm 2 \bmod 5$ (so n' is a nonsquare, and hence $\sigma_0(n')$ is even and $n' > 1$). For each $d'|n'$, we get a contribution of $(2d'|5) = -(d'|5)$ at terms $d = 2d'$ in (6.11) if $(d', n'/d') = 1$ and we get a contribution of $(2^{e-1}d'|5) = -(d'|5)$ at terms $d = 2^{e-1}d'$ in (6.11) if $(d', n'/d') \neq 1$. Thus, the combined contributions in (6.11) for $e' = 1$ and $e' = e - 1$ is the product of $-(d'|5)$'s with each divisor d' of n' appearing exactly once. Since n' is a nonsquare, the number of such divisors is even (namely, $\sigma_0(n')$) and we may pair up d' with n'/d' (contributing a product of $(n'|5) = -1$) to arrive at a total product of $(-1)^{\sigma_0(n')/2}$ by the terms with $e' = 1$ and $e' = e - 1$. At the terms $d = 2^{e'}d'$ with $e/2 < e' < e - 1$ and $e' = e$ the contribution in (6.11) is $(d|5) = (-1)^{e'}(d'|5)$ without restriction on d', so taking the product of these contributions with fixed e' gives $(-1)^{\sigma_0(n')/2}$ since the sign $(-1)^{e'}$ appears an even number of times. Hence, we conclude that

$$\varepsilon_n = (-1)^{(e/2)\sigma_0(n')/2}$$

when $e = \mathrm{ord}_2(n)$ is even. This is equal to -1 if and only if $e/2$ is odd and $\sigma_0(n')/2$ is odd, and this gives rise to exactly the listed cases when $\mathrm{ord}_2(n)$ is both even and larger than 2.

Finally, suppose $e > 2$ is odd, so $n' \equiv \pm 1 \bmod 5$. Since now $(n'|5) = 1$, a computation as for the case of even e shows that the total contribution of all terms $d = 2^{e'}d'$ in (6.11) with a fixed e' satisfying $(e+1)/2 \leq e' < e - 1$ or $e' = e$ is 1 when n' is not a square and is $(-1)^{e'}(m|5)$ when $n' = m^2$. There are $(e - 1)/2$ such terms, with total product 1 when n' is not a square and total product $(-1)^e(-1)^{(e-3)/2}(m|5)^{(e-1)/2} = (-(m|5))^{(e-1)/2}$ when $n' = m^2$; when $n' = 1$ this is $(-1)^{(e-1)/2}$. We also have to account for contributions in (6.11) at terms $d = 2^{e'}d'$ with $e' = 1$ and $e' = e - 1$. For $e' = 1$ we get contributions $(2d'|5) = -(d'|5)$ when $(d', n'/d') = 1$, and for $e' = e - 1$ we get contributions $(2^{e-1}d'|5) = (d'|5)$ when $(d', n'/d') \neq 1$. In particular, when $n' = 1$ we find that $\varepsilon_n = (-1)^{(e+1)/2}$; this gives the asserted list of possibilities when n is a power of 2 that is divisible by 8. Assuming now that $n' > 1$ (*i.e.*, n is not a power of 2), so n' has a non-empty set of prime factors, the number of divisors $d'|n'$ with $(d', n'/d') = 1$ is even. Thus, the product of the contributions for $e' = 1$ and $e' = e - 1$ is equal to $\prod_{d'|n'}(d'|5)$, and by pairing d' with n'/d' (when $d' \neq n'/d'$) and recalling that $(n'|5) = 1$ we see that this product is 1 when n' is a nonsquare and is $(m|5)$ when $n' = m^2$. Thus, when $n' > 1$ is a nonsquare we get $\varepsilon_n = 1$ and when $n' = m^2 > 1$ we get $\varepsilon_n = -(-(m|5))^{(e+1)/2}$. Setting this equal to -1 gives the elements on the desired list of possibilities that have not yet been obtained. ∎

We next wish to establish an analogue of Kronecker's congruence.

Theorem 6.8 (Kronecker's congruence). *Let $p \neq 5$ be prime. If $p \equiv \pm 1 \bmod 5$ then*

$$F_p(X, Y) \equiv (Y - X^p)(Y^p - X) \mod p\mathbf{Z}[X, Y], \tag{6.12}$$

and if $p \equiv \pm 2 \bmod 5$ then

$$F_p(X, Y) \equiv (Y - X^p)(XY^p + 1) \mod p\mathbf{Z}[X, Y]. \tag{6.13}$$

These congruences are sensitive to the arbitrary choice of sign in Definition 6.4.

Proof. Since the map π_p has degree $p+1$, by Theorem 6.3 we know *a priori* that $F_p \bmod p$ has degree $p+1$ in each of X and Y. Thus, if we can prove that the right sides of (6.12) and (6.13) divide $F_p \bmod p$ then degree considerations force the congruence up to a nonzero scalar $c_p \in \mathbf{F}_p^\times$. Since $F_p \in \mathbf{Z}[X,Y]$ has a unique monomial term $X^{r_p}Y^{p+1}$ and this term appears in F_p with coefficient equal to 1, the same holds under reduction modulo p (with the same r_p), and so the Y-monicity of the right sides of (6.12) and (6.13) shows that such a nonzero scalar ambiguity $c_p \in \mathbf{F}_p^\times$ is necessarily trivial. That is, it suffices to prove that $F_p \bmod p$ is divisible by the right sides of (6.12) and (6.13).

The symmetry properties of F_p in Theorem 6.5 reduce the divisibility claim to the assertion that $Y - X^p$ divides $F_p \bmod p$. That is, we claim that one of the irreducible components of $\operatorname{Spec} \mathbf{F}_p[X,Y]/(F_p)$ is defined by the vanishing of $Y - X^p$. We will construct such an irreducible component by studying irreducible components of the mod-p fiber of $Y(\Gamma_\mu(5), \Gamma_0(p))$.

By the definition of F_p, the quasi-finite Kronecker map

$$j_{5,\mu} \times (j_{5,\mu} \circ w_p) : Y(\Gamma_\mu(5), \Gamma_0(p)) \to \mathbf{A}^2_{\mathbf{Z}[1/5]}$$

over $\operatorname{Spec} \mathbf{Z}[1/5]$ factors through the zero-scheme of $F_p(X,Y)$. Passing to mod-p fibers, the quasi-finite map

$$j_{5,\mu} \times (j_{5,\mu} \circ w_p) : Y(\Gamma_\mu(5), \Gamma_0(p))_{\mathbf{F}_p} \to \mathbf{A}^2_{\mathbf{F}_p}$$

factors through $\operatorname{Spec} \mathbf{F}_p[X,Y]/(F_p)$. Thus, to prove that $F_p \bmod p$ is divisible by $Y - X^p$, it is enough to find an irreducible component Y' of $Y(\Gamma_\mu(5), \Gamma_0(p))_{\mathbf{F}_p}$ such that $j_{5,\mu}(E,\iota)^p = j_{5,\mu}(E/C,\iota')$ for geometric points $y = (E,\iota,C)$ of Y', where $w_p(y) = (E/C, \iota', E[p]/C)$; we may also ignore finitely many points y (such as supersingular points). There are two irreducible components of $Y(\Gamma_\mu(5), \Gamma_0(p))_{\mathbf{F}_p}$, corresponding to C being étale or multiplicative. Let Y' be the component corresponding to multiplicative C, so for ordinary geometric points $y \in Y'$ we see that there is an isomorphism $E/C \simeq E^{(p)}$ carrying the p-isogeny $E \to E/C$ to the relative Frobenius morphism $E \to E^{(p)}$. If $P = \iota(1,0)$ and $Q = \iota(0,1)$ in the finite étale group $E[5]$, then $\iota'(1,0) = p^{-1}P^{(p)}$ and $\iota'(0,1) = Q^{(p)}$ in $E^{(p)}$.

Let k be the field over which the geometric point y lives. By the definition of the $\Gamma_\mu(5)$-moduli functor, the point $w_p(y) = (E^{(p)}; p^{-1}P^{(p)}, Q^{(p)}) \in Y_\mu(5)(k)$ is the image of $y \in Y_\mu(5)(k)$ under the Frobenius morphism of the $\mathbf{F}_p$-scheme $Y_\mu(5)$. Since the isomorphism $j_{5,\mu} : Y_\mu(5)_{\mathbf{F}_p} \simeq \mathbf{P}^1_{\mathbf{F}_p}$ commutes with absolute Frobenius morphisms (as do all maps of $\mathbf{F}_p$-schemes), and the absolute Frobenius morphism on $\mathbf{P}^1_{\mathbf{F}_p}$ is given by $t \mapsto t^p$ in terms of the standard coordinate on $\mathbf{P}^1$, we conclude that $j_{5,\mu}(w_p(y)) = j_{5,\mu}(y)^p$ as desired. ■

To construct an analogue of F_n for all n, the key issue is to formulate a good enhanced moduli functor that allows n to be divisible by 5. We will explain the case $n = 5$, because in this case the polynomial F_5 relating $j_5(\tau)$ and $j_5(5\tau)$ has a very special form. The general case is left to the interested reader (and will not be used later).

Theorem 6.9. *There is a unique rational function $h \in \mathbf{Q}(x)$ such that $j_5(\tau/5)^5 = h(j_5(\tau))$, and h is not a polynomial.*

This theorem says that we may find an F_5 with the form $h_1(Y)X^5 - h_2(Y)$ for relatively prime $h_1, h_2 \in \mathbf{Z}[Y]$ with $\deg h_1 > 0$. Such explicit h_1 and h_2 are provided by a famous identity of Ramanujan [24, Theorem 3.2], but we prefer to suppress the explicit description of $h = h_2/h_1$ until we have provided a geometric proof of its existence.

Proof. We begin by constructing a geometrically-connected finite cover of $Y_\mu(5)_{\mathbf{Q}}$ that replaces the role of $Y(\Gamma_\mu(N), \Gamma_0(n))$ in our study of F_n for n relatively prime to 5. Let us work more generally at the outset with any $N \geq 3$ instead of with $N = 5$. Over the $\mathbf{Q}$-scheme $Y_\mu(N)$ there is a universal elliptic curve $E \to Y_\mu(N)$ equipped with an isomorphism

$$\iota : \mu_N \times (\mathbf{Z}/N\mathbf{Z}) \simeq E[N]$$

as $Y_\mu(N)$-groups. Let $Q = \iota(1,1) \in E[N](Y_\mu(N))$, so the fiber $[N]^{-1}(Q) \to Y_\mu(N)$ is an $E[N]$-torsor over $Y_\mu(N)$. Via ι, $[N]^{-1}(Q)$ acquires a structure of torsor over $\mu_N \times (\mathbf{Z}/N\mathbf{Z})$. Passing to the quotient by the action of $\mathbf{Z}/N\mathbf{Z}$ defines a μ_N-torsor $Y'_\mu(N) \to Y_\mu(N)$. This torsor is geometrically connected over $\mathbf{Q}$ because it is dominated by the geometrically-connected cover $Y_\mu(N^2)$. Our moduli-theoretic construction of $Y'_\mu(N)$ extends across the cusps, so we get a geometrically-connected proper smooth curve $X'_\mu(N)$ over $\operatorname{Spec}\mathbf{Q}$ that is a μ_N-torsor over $X_\mu(N)$.

We shall need to carry out some calculations with analytic models for modular curves. Thus, we choose a connected component $\mathfrak{H}$ of $\mathbf{C} - \mathbf{R}$ and (without loss of generality) take $\zeta = e^{2\pi i/N}$ with $i = \sqrt{-1} \in \mathfrak{H}$. We will use only $\tau \in \mathfrak{H}$ because the action of $\mathrm{SL}_2(\mathbf{Z})$ on $X_\zeta(N)$ lifts via π_ζ to the usual action on $\mathfrak{H}$.

Define $\Gamma^0(m) \subseteq \Gamma(1)$ to be the preimage of the subgroup of matrices in $\mathrm{SL}_2(\mathbf{Z}/m\mathbf{Z})$ with vanishing upper-right corner. The normal subgroup $\Gamma'(N) = \Gamma^0(N^2) \cap \Gamma(N)$ in $\Gamma(N)$ has the property that the quotient $\Gamma(N)/\Gamma'$ is cyclic of order N, and this quotient of $\Gamma(N)/\Gamma(N^2)$ is naturally identified with the geometric Galois group of the covering $X'_\mu(N) \to X_\mu(N)$. In terms of analytic models, $\mathbf{C}(X'_\mu(N))$ is identified with the field of level-N^2 modular functions that are $\Gamma'(N)$-invariant, and a generator of the Galois group of $\mathbf{C}(X'_\mu(N))$ over $\mathbf{C}(X_\mu(N))$ is represented by the action induced by $\tau \mapsto \tau + N$ on $\mathfrak{H}$. In particular, since

$$\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \Gamma'(N) \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}^{-1} \subseteq \Gamma(N),$$

for any $f \in \mathbf{C}(X_\mu(N))$ the function $g_f(\tau) \stackrel{\text{def}}{=} (f \circ \pi_\zeta)(\tau/N)$ lies in $\mathbf{C}(X'_\mu(N))$ and a generator of the Galois group of $\mathbf{C}(X'_\mu(N))$ over $\mathbf{C}(X_\mu(N))$ acts on g_f via the operation $\tau \mapsto \tau + N$.

Let us specialize these considerations to the case $N = 5$. We conclude that the function $g(\tau) = j_5(\tau/5)$ lies in a degree-5 extension $K = \mathbf{Q}(X'_\mu(5))$ of $\mathbf{Q}(X_\mu(5)) = \mathbf{Q}(j_5)$ with $\mathbf{Q}$ algebraically closed in K, and that $K(\zeta_5)/\mathbf{Q}(\zeta_5, j_5)$ a Galois extension such that the Galois-orbit of g consists of the elements ζg for $\zeta \in \mu_5$. Thus, g^5 is Galois-invariant, and so

$$g^5 \in K \cap \mathbf{Q}(\zeta_5, j_5) = \mathbf{Q}(j_5).$$

This produces the desired $h \in \mathbf{Q}(x)$, except for the fact that h cannot be a polynomial. That is, we must prove that $g^5 \notin \mathbf{Q}[j_5]$. Assuming otherwise, it would follow that g only has poles at cusps on $X'_\mu(5)_{\mathbf{Q}}$ lying over the unique point $\infty \in X_\mu(5)_{\mathbf{Q}}$ where j_5 has a pole. This is a contradiction since $g(\tau) = j_5(\tau/5)$ has a pole at the cusp $1/2$ that is not $\Gamma(5)$-equivalent to ∞. ■

It is natural to want to make the rational function h in Theorem 6.9 explicit. Ramanujan discovered the answer:

$$h(x) = x \cdot \frac{x^4 + 3x^3 + 4x^2 + 2x + 1}{x^4 - 2x^3 + 4x^2 - 3x + 1}. \tag{6.14}$$

In Example B.3 in Appendix B we will give an easy derivation of this identity by using the definition of j_5 in terms of Klein forms; h could also be determined by pole- and cusp-chasing via Table B.1.

7. Estimates on coefficients of F_n

Since the classical modular polynomials $\Phi_n(X, Y)$ are notoriously impossible to compute, due to the gigantic height of these polynomials, one might expect the F_n's to be equally useless in practice. Remarkably, this is not so: an inspection of the table of F_n's in Appendix C shows that (for $\gcd(n, 5) = 1$) the coefficients are rather small!

Computation of F_n for larger values of n, however, reveals that the coefficients of F_n do grow quickly with n. Nonetheless, a comparison of the coefficients of F_n and the coefficients of the classical modular polynomial Φ_n of level n shows that the coefficients of F_n are *dramatically* smaller than those of Φ_n. This has the practical consequence that for moderate n we can work computationally with F_n.

In this section we use the methods of Cohen and Rademacher (that estimate the coefficients of the Φ_n's and the q-expansion coefficients of j) to estimate the q-expansion coefficients of j_5 and to prove that F_n has small coefficients (with respect to n) in comparison to Φ_n when $\gcd(n, 5) = 1$.

For any nonzero $P = \sum a_I z^I \in \mathbf{C}[z_1, \ldots, z_m]$, we define the *logarithmic height*

$$h(P) = \log(\max_I |a_I|).$$

Observe that for positive $c \in \mathbf{R}^\times$, $h(cP) = \log(c) + h(P)$. In this section, we will prove

Theorem 7.1. *For $(n, 5) = 1$,*

$$h(F_n) = \frac{1}{10}[\Gamma(1) : \Gamma_0(n)] \left(\log n - 2 \sum_{p|n} \frac{\log p}{p} + O(1) \right)$$

as $n \to \infty$.

Before we prove Theorem 7.1, let us record a corollary that compares the coefficients of F_n against coefficients of Φ_n for n relatively prime to 5.

Corollary 7.2. *For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbf{Z})$, let $\overline{\Gamma}$ denote the image of Γ in $\mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}$. We have*

$$\lim_{\substack{n \to \infty \\ (n,5)=1}} \frac{h(\Phi_n)}{h(F_n)} = [\overline{\Gamma}(1) : \overline{\Gamma}(5)] = 60.$$

Proof. This follows at once from Theorem 7.1 and the asymptotic formula for $h(\Phi_n)$ analogous to Theorem 7.1 as given in the main theorem in [4]. ■

Remark 7.3. Since $h(F_n)$ is the *logarithmic* height, Corollary 7.2 shows that the largest coefficient (in absolute value) of Φ_n is comparable to the 60th power of the largest coefficient (in absolute value) of F_n.

We now prove Theorem 7.1. In what follows, it is understood that n denotes a positive integer relatively prime to 5. We also fix $i = \sqrt{-1} \in \mathbf{C}$. Our proof closely follows Cohen's paper [4] that establishes a similar estimate for the coefficients of the classical modular polynomial Φ_n.

Let $t \in \mathbf{R}$. Since $|j_5(it)| \to \infty$ as $t \to \infty$, there exist $s \in \mathbf{R}$ and distinct positive $t_0, t_1 \in \mathbf{R}$ with $t_0, t_1 \geq 1$ and $s \geq 1$ such that $|j_5(it_0)| = s$ and $|j_5(it_1)| = 2s$. Since $\Gamma(5)$ acts without fixed points on $\mathbf{C} - \mathbf{R}$ and j_5 thereby realizes each connected component of $\mathbf{C} - \mathbf{R}$ as a covering space of the complement of a finite subset of $\mathbf{CP}^1$, it follows that the derivative j_5' is nonvanishing on $\mathbf{C} - \mathbf{R}$. Since $j_5 = q^{-1/5} + \ldots$ has real coefficients, so j_5 has real-analytic restriction to each connected component of the imaginary axis with deleted origin, the derivative of j_5 on each such component (as parameterized by $\pm it$ with $t \in (0, \infty)$) is positive because j_5 blows up to ∞ as $q \to 0$. Thus, $j_5(it)$ is strictly increasing in $t \in (0, \infty)$, so $t_0 < t_1$ and $j_5(it)$ is strictly increasing for $t_0 \leq t \leq t_1$. We fix, once and for all, any such s and corresponding $t_0 < t_1$ as above.

Lemma 7.4. *For $t_0 \leq t \leq t_1$ we have*

$$h(F_n(j_5(it), Y)) = \sum_{ad=n,\ a>0} S_d(t) + O([\Gamma(1) : \Gamma_0(n)])$$

as $n \to \infty$, where

$$S_d(t) = \sum_{\substack{0 \leq b < d \\ (a,b,d)=1}} \log \max\{1, |j_5((ait + b)/d)|^{\chi_5(a)}\}, \tag{7.1}$$

and $\chi_5 : \mathbf{Z} - 5\mathbf{Z} \to \{\pm 1\}$ is the unique quadratic Dirichlet character modulo 5. The implicit O-constant depends only on t_0, t_1.

Proof. It is well-known that the coefficients of a monic polynomial $P(x) = (x - \omega_1)\cdots(x - \omega_d)$ are bounded between $2^{-d}M$ and $2^d M$ where $M = \prod_{j=1}^{d} \max\{1, |\omega_j|\}$. Taking logarithms yields

$$h(P) = \sum_{j=1}^{d} \log \max\{1, |\omega_i|\} + O(d)$$

with an implicit absolute O-constant that is independent of d and P. We now apply this general estimate to suitable specializations of F_n in the first variable.

By (6.3) and (6.6),

$$F_n(j_5(it), Y) = j_5(it)^{r_n} \prod_{\substack{ad=n,\ a>0 \\ 0\le b'<d \\ (a,b',d)=1}} (Y - j_5 \circ \sigma_a((ait + 5b')/d)) \tag{7.2}$$

with σ_a as in (6.5) and r_n defined by the condition that $\pm X^{r_n} Y^{\deg \pi_n}$ is the unique monomial term appearing in $F_n(X, Y)$ with Y-degree $\deg \pi_n$ (see Theorem 6.3). By Corollary 5.5, we have $|j_5 \circ \sigma_a| = |j_5|^{\chi_5(a)}$, and since $F_n(j_5(it), Y)$ has degree $[\Gamma(1) : \Gamma_0(n)]$ in Y we obtain

$$h(F_n(j_5(it), Y)) = r_n \log j_5(it) + \sum_{ad=n,\ a>0} \sum_{\substack{0\le b'<d \\ (a,b',d)=1}} \log \max\{1, |j_5((ait + 5b')/d)|^{\chi_5(a)}\} + O([\Gamma(1) : \Gamma_0(n)]).$$

Since $\log(2s) = \log(j_5(it_1)) \ge \log j_5(it)$ and $1 \le r_n \le \deg \pi_n = [\Gamma(1) : \Gamma_0(n)]$, we can absorb the first term into $O([\Gamma(1) : \Gamma_0(n)])$. By the division algorithm, we may write $5b' = dq + b$ with $0 \le b < d$. From Theorem A.3, for any integer k we have $j_5(z + k) = \zeta j_5(z)$ for some fifth root of unity ζ. It follows that the function $|j_5(z)|$ is invariant under integer translations, so

$$|j_5((ait + 5b')/d)| = |j_5((ait + b)/d + q)| = |j_5((ait + b)/d)|.$$

Finally, since $(n, 5) = 1$ and $ad = n$, multiplication by 5 on $\mathbf{Z}/d\mathbf{Z}$ is an isomorphism. Thus, we have

$$\sum_{\substack{0\le b'<d \\ (a,b',d)=1}} \log \max\{1, |j_5((ait + 5b')/d)|^{\chi_5(a)}\} = \sum_{\substack{0\le b<d \\ (a,b,d)=1}} \log \max\{1, |j_5((ait + b)/d)|^{\chi_5(a)}\} = S_d(t).$$

■

Our next goal is to estimate the sums $S_d(t)$ for fixed t between t_0 and t_1. In order to do this, we must bound $|j_5((ait + b)/d)|^{\chi_5(a)}$ for factorizations $n = ad$ with $a, d > 0$, $0 \le b < d$, and $(a, b, d) = 1$. This will be straightforward if at/d is sufficiently large, but slightly complicated when at/d is small. When at/d is close to 0, then $(ait + b)/d$ is close to b/d. In these cases, we will use our knowledge of the behavior of j_5 near the cusps of $X(5)$ to provide an upper bound for $|j_5((ait + b)/d)|^{\chi_5(a)}$.

Recall that the *Farey sequence* $\mathcal{F}_N$ is the ordered list

$$\mathcal{F}_N = \{h/k \in [0, 1] \mid h, k \in \mathbf{Z},\ \gcd(h, k) = 1,\ 1 \le k \le N\}$$

whose elements are enumerated in increasing order. We will estimate $|j_5((ait+b)/d)|^{\chi_5(a)}$ when b/d is "close" to $h/k \in \mathscr{F}_N$ and $at/d \le 1/2$ by expanding j_5 in a local parameter about the cusp h/k. Equivalently, we shall find some $\gamma_{h/k} \in \mathrm{SL}_2(\mathbf{Z})$ taking h/k to the cusp ∞ and use our knowledge of the q-expansion of $j_5 \circ \gamma_{h/k}$ to estimate $|j_5((ait+b)/d)|^{\chi_5(a)}$. First, we need to make precise what we mean by "close" to h/k. To do this, put $N = \lfloor d/(nt)^{1/2} \rfloor$; evidently $N \ge 1$. We will partition the interval $I(N) = [1/(N + 1), (N + 2)/(N + 1))$ into disjoint intervals $I_N(h/k)$ containing h/k for each $h/k \in \mathcal{F}_N$ and consider b/d "close" to h/k when $b/d \in I_N(h/k)$.

Let us enumerate the Farey fractions $\mathcal{F}_N$ as $\lambda_0, \dots, \lambda_K$. Recall that for any consecutive Farey fractions $h_1/k_1 = \lambda_{i-1}$ and $h_2/k_2 = \lambda_i$ the mediant $\mu_i = (h_1 + h_2)/(k_1 + k_2)$ satisfies $\lambda_{i-1} < \mu_i < \lambda_i$. We set $\mu_0 = 0$ and define the interval

$$I_N(\lambda_i) = \begin{cases} [\mu_i, \mu_{i+1}) & i < K \\ [N/(N+1), (N+2)/(N+1)) & i = K \end{cases}, \tag{7.3}$$

so $\lambda_i \in I_N(\lambda_i)$. Since $\mu_1 = 1/(N+1)$, we have the disjoint-union decomposition

$$I(N) = [1/(N+1), (N+2)/(N+1)) = \bigcup_{h/k \in \mathcal{F}_N - \{0\}} I_N(h/k). \tag{7.4}$$

By [4, Lemma 3] , with $\lambda_i = h/k \neq 0$,

$$\begin{aligned} \frac{1}{2Nk} &\leq \lambda_i - \mu_{i-1} \leq \frac{1}{(N+1)k} \\ \frac{1}{2Nk} &\leq \mu_i - \lambda_i \leq \frac{1}{(N+1)k}. \end{aligned} \tag{7.5}$$

We can now provide good estimates for $j_5((ait+b)/d)$. For convenience, we adopt the notation of [4, §3.1] and put

$$g_{h,k}(x) = 2\pi \cdot \frac{nt/(dk)^2}{(at/d)^2 + (x - h/k)^2}.$$

Lemma 7.5. *For $\sigma, t \in \mathbf{R}$, let $q = e^{2\pi i(\sigma+it)}$. Assume $g(\sigma + it) := \sum_{j\geq 0} a_j q^j$ is absolutely convergent and nonzero for $t > 0$. There is a constant $C_1 \geq 0$ depending only on g such that*

$$|g(\sigma + it)| \leq C_1 \tag{7.6}$$

for $t \geq 1/2$ and all σ. If further $a_0 \neq 0$, then there is a positive constant $C_0 > 0$ depending only on g such that

$$C_0 \leq |g(\sigma + it)| \tag{7.7}$$

for $t \geq 1/2$ and all σ. In particular, if $at/d \geq 1/2$ then

$$\log \max\{1, |j_5((ait + b)/d)|^{\chi_5(a)}\} = \begin{cases} (2\pi/5)(nt/d^2) + O(1) & \text{if } a \equiv \pm 1 \bmod 5 \\ O(1) & \text{otherwise} \end{cases}. \tag{7.8}$$

If $at/d \leq 1$, put $N = \lfloor d/(nt)^{1/2} \rfloor$ and let I_N be defined by (7.3). For $b/d \in I_N(h/k)$,

$$\log \max\{1, |j_5((ait + b)/d)|^{\chi_5(a)}\} = \begin{cases} \frac{1}{5} g_{h,k}(b/d) + O(1) & \text{if } (h,k) \equiv (\pm a, 0) \bmod 5 \\ O(1) & \text{otherwise} \end{cases}. \tag{7.9}$$

The implicit O-constants are independent of all parameters a, b, d, t, h, k.

Remark 7.6. Observe that there is an overlap in the range of applicability of (7.8) and (7.9), namely $1/2 \leq at/d \leq 1$. For these values of t, both (7.8) and (7.9) give the same estimate of $O(1)$, as is readily verified by (7.5). Indeed, it is not difficult to see from the definition of $g_{h,k}(x)$ that (7.8) and (7.9) differ by at most a constant when at/d is in any compact interval bounded away from 0. Thus, for values of at/d in this range of overlap, we shall use whichever of these two estimates is more convenient.

Proof. Since the sum defining $g(\sigma+it)$ is absolutely convergent for $t > 0$, we have $g(\sigma+it) \to a_0$ as $t \to \infty$. We may therefore find $T \geq 1/2$ such $|a_0|/2 \leq |g(\sigma + it)| \leq |a_0| + 1$ for all $t > T$. This proves (7.6) and (7.7) when $t > T$. To handle $T \leq t \leq 1/2$, we observe that $g(\sigma + it)$ is periodic under $\sigma \mapsto \sigma + 1$, so since the region $K = \{|\sigma| \leq 1/2\} \cap \{1/2 \leq t \leq T\}$ is compact and $g(z)$ is continuous and nonzero on K, we have

$C_0 \leq |g(z)| \leq C_1$ for some absolute constants $C_0 > 0$ and C_1 as claimed. The estimate (7.8) now follows from (7.6) when $a \equiv \pm 1 \bmod 5$ and from (7.7) when $a \equiv \pm 2 \bmod 5$ upon taking $g = (q^{1/5} j_5)^{\chi_5(a)}$.

To prove (7.9), suppose that $b/d \in I_N(h/k)$ and put

$$\gamma_{h/k} := \begin{pmatrix} v & u \\ -k & h \end{pmatrix},$$

where $uk + hv = 1$, and we require $5|u$ if $5|k$ (so $\gamma_{h,k}$ and σ_h^{-1} have the same image in $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ when $5|k$). The usual calculation shows that

$$\mathrm{Im}\left(\gamma_{h/k}((ait+b)/d)\right) = \frac{nt/(dk)^2}{(at/d)^2 + (b/d - h/k)^2} = \frac{1}{2\pi} g_{h,k}(b/d). \tag{7.10}$$

Now by (7.5) we have $|b/d - h/k| \leq 1/(N+1)k$, and since $N = \lfloor d/(nt)^{1/2} \rfloor$ satisfies $1/(N+1) \leq (nt)^{1/2}/d$, it follows (using an easy direct check when $h/k = 0$) that

$$|b/d - h/k| \leq 1/(N+1)k \leq (nt)^{1/2}/(dk). \tag{7.11}$$

Since $h/k \in \mathcal{F}_N$ we have $k \leq N \leq d/(nt)^{1/2}$, which implies $1 \leq d/(k(nt)^{1/2})$, whence multiplying by nt/d^2 and recalling that $ad = n$ yields

$$at/d = nt/d^2 \leq (nt)^{1/2}/(dk). \tag{7.12}$$

Combining (7.10) with (7.11), and (7.12), we obtain

$$\mathrm{Im}\left(\gamma_{h/k}((ait+b)/d)\right) = \frac{nt/(dk)^2}{(at/d)^2 + (b/d - h/k)^2} \geq \frac{nt/(dk)^2}{nt/(dk)^2 + nt/(dk)^2} = 1/2.$$

If $k \not\equiv 0 \bmod 5$, then from our calculations in Table B.1 we have

$$j_5 \circ \gamma_{h/k}^{-1} = c(h/k) + O(q),$$

where $c(h/k) \neq 0$ is constant. Since $j_5((ait+b)/d) = j_5 \circ \gamma_{h/k}^{-1}(\gamma_{h/k}((ait+b)/d))$ and $\mathrm{Im}\left(\gamma_{h/k}((ait+b)/d)\right) \geq 1/2$, we apply (7.6) and (7.7) to $g = j_5 \circ \gamma_{h/k}^{-1}$ to find that $|j_5((ait+b)/d)|^{\chi_5(a)} = O(1)$ for all $b/d \in I_N(h/k)$.

It remains to estimate $|j_5((ait+b)/d)|^{\chi_5(a)}$ when $k \equiv 0 \bmod 5$. In these cases, $\gamma_{h,k}$ and σ_h^{-1} have the same image in $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$, so

$$|j_5((ait+b)/d)|^{\chi_5(a)} = |j_5(\gamma_{h,k}(ait+b)/d)|^{\chi_5(ah)}.$$

If $h \not\equiv \pm a \bmod 5$, then $ah \not\equiv \pm 1 \bmod 5$, and since $\mathrm{Im}\left(\gamma_{h/k}((ait+b)/d)\right) \geq 1/2$, we can apply (7.8) to obtain $|j_5((ait+b)/d)|^{\chi_5(a)} = O(1)$. On the other hand, if $h \equiv \pm a \bmod 5$ then $ah \equiv \pm 1 \bmod 5$, so another application of (7.8) and (7.10) yields (7.9). ■

Using Lemma 7.5, we can estimate the sums $S_d(t)$:

Lemma 7.7. *If $d < (nt)^{1/2}$ then*

$$S_d = O(n/d) \tag{7.13}$$

and if $d \geq (nt)^{1/2}$ then

$$S_d = \frac{1}{10}\frac{d}{(a,d)}\varphi((a,d))\log(d^2/n) + O(\sigma_1(d/(a,d))) + O(d\sigma_1((a,d))/(a,d)), \tag{7.14}$$

where the implicit O-constants depends only on t_0, t_1.

Proof. The estimate (7.13) follows immediately from (7.8). To obtain (7.14), we set $N = \lfloor d/(nt)^{1/2} \rfloor$ and observe that $N \geq 1$. Recall the definition of $I(N)$ given in (7.4). By Theorem A.3, we have $|j_5(z+m)| = |j_5(z)|$ for any integer m, so we may reindex the sum in (7.1) via

$$b \mapsto \begin{cases} b & \text{if } b/d \in [1/(N+1), 1] \\ b+d & \text{if } b/d \in [0, 1/(N+1)) \end{cases},$$

so that our original sum $S_d(t)$ over all $b/d \in [0,1]$ is now a sum over all

$$b/d \in I(N) = [1/(N+1), (N+2)/(N+1)).$$

We therefore obtain

$$S_d(t) = \sum_{\substack{0 \leq b < d \\ (a,b,d)=1}} \log \max\{1, |j_5((ait+b)/d)|^{\chi_5(a)}\} = \sum_{\substack{b/d \in I(N) \\ (a,b,d)=1}} \log \max\{1, |j_5((ait+b)/d)|^{\chi_5(a)}\}.$$

Since (7.4) gives a partition of $I(N)$ into the disjoint intervals $I_N(h/k)$ for $h/k \in \mathcal{F}_N - \{0\}$, we have

$$\begin{aligned} S_d(t) &= \sum_{h/k \in \mathcal{F}_N - \{0\}} \sum_{\substack{b/d \in I_N(h/k) \\ (a,b,d)=1}} \log \max\{1, |j_5((ait+b)/d)|^{\chi_5(a)}\} \\ &= \sum_{k=1}^{N} \sum_{\substack{h=1 \\ (h,k)=1}}^{k} \sum_{\substack{b/d \in I_N(h/k) \\ (a,b,d)=1}} \log \max\{1, |j_5((ait+b)/d)|^{\chi_5(a)}\}. \end{aligned}$$

We split this sum up into sums over $(h,k) \equiv \pm(a,0) \bmod 5$ and over $(h,k) \not\equiv \pm(a,0) \bmod 5$, and use (7.9) to estimate the terms occurring in each sum:

$$S_d(t) = \sum_{\substack{1 \leq h \leq k \leq N \\ (h,k)=1 \\ (h,k) \equiv (\pm a, 0) \bmod 5}} \sum_{\substack{b/d \in I_N(h/k) \\ (a,b,d)=1}} \frac{1}{5}\left(g_{h,k}(b/d) + O(1)\right) + \sum_{\substack{1 \leq h \leq k \leq N \\ (h,k)=1 \\ (h,k) \not\equiv (\pm a, 0) \bmod 5}} \sum_{\substack{b/d \in I_N(h/k) \\ (a,b,d)=1}} O(1)$$

Since the intervals $I_N(h/k)$ for $h/k \in \mathcal{F}_N - \{0\}$ partition $I(N)$, the second double sum above is at most $\sum_{b/d \in I(N)} O(1)$; since this sum has at most d terms, we get a contribution of $O(d)$. Exactly the same reasoning shows that the $O(1)$-term in the first double sum contributes $O(d)$, for a total error term of $O(d)$, with an implicit constant that depends only on t_0 and t_1. Thus,

$$S_d(t) = \frac{1}{5} \sum_{\substack{1 \leq h \leq k \leq N \\ (h,k)=1 \\ (h,k) \equiv (\pm a, 0) \bmod 5}} \sum_{\substack{b/d \in I_N(h/k) \\ (a,b,d)=1}} g_{h,k}(b/d) + O(d), \tag{7.15}$$

where the $O(d)$-term lies outside of the double summation. Now by [4, Lemma 6], we have

$$\sum_{\substack{b/d \in I_N(h/k) \\ (a,b,d)=1}} g_{h,k}(b/d) = k^{-2} \sum_{f \mid (a,d)} \mu(f) F_f(dh/fk) + O\left(n^{1/2} \sigma_1((a,d))/(k(a,d))\right),$$

where

$$F_f(\theta) = \frac{2\pi^2 d}{f} \sum_{v \in \mathbf{Z}} e^{-2\pi |v| nt/df} e^{2\pi i v \theta} \tag{7.16}$$

and the O-constant depends only on t_0, t_1. Therefore,

$$S_d(t) = \frac{1}{5} \sum_{\substack{1\le h\le k\le N\\ (h,k)=1\\ (h,k)\equiv(\pm a,0) \bmod 5}} \left(k^{-2} \sum_{f\mid(a,d)} \mu(f)F_f(dh/fk) + O\left(n^{1/2}\sigma_1((a,d))/(k(a,d))\right)\right) + O(d),$$

where again the $O(d)$-term lies outside of the double summation.

The sum of the error terms in the double summation is bounded above by

$$\frac{Cn^{1/2}\sigma_1((a,d))}{(a,d)} \cdot \sum_{\substack{1\le h\le k\le N\\ (h,k)=1}} \frac{1}{k} \le \frac{Cn^{1/2}\sigma_1((a,d))}{(a,d)} \cdot \sum_{1\le k\le N} \frac{\varphi(k)}{k} \le \frac{Cn^{1/2}\sigma_1((a,d))}{(a,d)} N$$
$$\le \frac{Cn^{1/2}\sigma_1((a,d))}{(a,d)} \frac{d}{(nt)^{1/2}} \le Cd\sigma_1((a,d))/(a,d)$$

with some constant C depending only on t_0, t_1; in the last line we have used the fact that $1 \le t_0 \le t$. This estimate also absorbs the additional $O(d)$-term, so we obtain

$$S_d(t) = \frac{1}{5} \sum_{f\mid(a,d)} \mu(f) \sum_{\substack{1\le h\le k\le N\\ (h,k)=1\\ (h,k)\equiv(\pm a,0) \bmod 5}} k^{-2}F_f(dh/fk) + O(d\sigma_1((a,d))/(a,d)). \tag{7.17}$$

with the error term outside of the double summation. We still need to estimate the sum

$$\sum_{\substack{1\le h\le k\le N\\ (h,k)=1\\ (h,k)\equiv(\pm a,0) \bmod 5}} k^{-2}F_f(dh/fk),$$

which by (7.16) is

$$\frac{2\pi^2 d}{f} \sum_{v\in\mathbf{Z}} C_N(d|v|/f)e^{-2\pi|v|nt/df}, \tag{7.18}$$

where

$$C_N(m) = \sum_{\substack{1\le k\le N\\ k\equiv 0 \bmod 5}} k^{-2}c_k(m) \qquad \text{and} \qquad c_k(m) = \sum_{\substack{1\le h\le k\\ (h,k)=1\\ h\equiv\pm a \bmod 5}} e^{2\pi i hm/k}.$$

By Lemma D.3, we have $|c_k(m)| \le (k,m)$ when $m \ne 0$, and so

$$|C_N(m)| \le \sum_{k=1}^{\infty} k^{-2}(k,m) \le \sum_{d\mid m} d \sum_{j=1}^{\infty} (jd)^{-2} = O(\sigma_1(|m|)/|m|) \tag{7.19}$$

for an absolute implicit O-constant. When $m = 0$, Lemma D.3 tells us that

$$C_N(0) = \sum_{\substack{1\le k\le N\\ k\equiv 0 \bmod 5}} k^{-2} \sum_{\substack{1\le h\le k\\ (h,k)=1\\ h\equiv\pm a \bmod 5}} 1$$
$$= \sum_{\substack{1\le k\le N\\ k\equiv 0 \bmod 5}} k^{-2} \left(\frac{1}{2}\varphi(k)\right),$$

which by Lemma D.1 is

$$= \frac{1}{2\pi^2}\log N + O(1), \tag{7.20}$$

with an absolute implicit O-constant.

Putting (7.19) and (7.20) together and using (7.18), we see that

$$\sum_{\substack{1\le h\le k\le N\\(h,k)=1\\(h,k)\equiv(\pm a,0)\bmod 5}} k^{-2}F_f(dh/fk) = \frac{d}{f}\log N + O(d/f) + O\left(\sum_{v\in\mathbf{Z}-\{0\}} f\frac{\sigma_1(d|v|/f)}{d|v|}e^{-2\pi|v|nt/df}\right) \tag{7.21}$$

(7.22)

with absolute implicit O-constants. Now since $f|(a,d)$ and $(a,d)|(n/d)$ we clearly have $df \le n$ so that

$$e^{-2\pi|v|nt/df} \le e^{-2\pi|v|t} \le e^{-2\pi|v|}$$

since $1 \le t_0 \le t$. Therefore, putting $C_1 = \sum_{v\in\mathbf{Z}-\{0\}} \frac{\sigma_1(|v|)}{|v|}e^{-2\pi(|v|-1)}$ and using the fact that $\sigma_1(d|v|/f) \le \sigma_1(d/f)\sigma_1(|v|)$, we have

$$\sum_{v\in\mathbf{Z}-\{0\}} f\frac{\sigma_1(d|v|/f)}{d|v|}e^{-2\pi|v|nt/df} \le C_1(f/d)\sigma_1(d/f)e^{-2\pi nt/df} \le C_1\sigma_1(d/f)e^{-2\pi n/df},$$

where we have again used the inequality $t \ge t_0 \ge 1$ and the fact that $f|d$ (so $f/d < 1$). Thus,

$$\sum_{v\in\mathbf{Z}-\{0\}} f\frac{\sigma_1(d|v|/f)}{d|v|}e^{-2\pi|v|nt/df} = O(\sigma_1(d/f)e^{-2\pi n/df}) \tag{7.23}$$

with an absolute implicit O-constant, and since $N = \lfloor\sqrt{d^2/nt}\rfloor$ we see that $\log N = \frac{1}{2}\log(d^2/n) + O(1)$ with an implicit O-constant that depends only on t_0 and t_1 since $1 \le t_0 \le t \le t_1$.

Incorporating the estimate (7.23) into (7.21) therefore gives

$$\sum_{\substack{1\le h\le k\le N\\(h,k)=1\\(h,k)\equiv(\pm a,0)\bmod 5}} k^{-2}F_f(dh/fk) = \frac{d}{2f}\log(d^2/n) + O(d/f) + O\left(\sigma_1(d/f)e^{-2\pi n/df}\right), \tag{7.24}$$

where the implicit O-constants depend only on t_0, t_1. Combining (7.24) with (7.17), we have

$$S_d(t) = \frac{1}{5}\sum_{f|(a,d)}\mu(f)\left(\frac{d}{2f}\log(d^2/n) + O(d/f) + O\left(\sigma_1(d/f)e^{-2\pi n/df}\right)\right) + O(d\sigma_1((a,d))/(a,d)). \tag{7.25}$$

Now,

$$\sum_{f|(a,d)}\mu(f)\sigma_1(d/f)e^{-2\pi n/df} \le \sum_{f|(a,d)}\sigma_1(d/f)e^{-2\pi n/df} \le \sum_{f|(a,d)}\sigma_1(df/(a,d))e^{-2\pi nf/(d(a,d))},$$

and since $\sigma_1(df/(a,d)) \le \sigma_1(d/(a,d))\sigma_1(f)$ and $e^{-2\pi nf/(a,d)} \le e^{-2\pi f}$ we have

$$\sum_{f|(a,d)}\mu(f)\sigma_1(d/f)e^{-2\pi n/df} \le \sigma_1(d/(a,d))\sum_{f=1}^{\infty}\sigma_1(f)e^{-2\pi f}. \tag{7.26}$$

Finally, using the well-known identity

$$\sum_{f|(a,d)}\mu(f)(d/f) = (d/(a,d))\sum_{f|(a,d)}\mu(f)(a,d)/f = d/(a,d)\varphi((a,d))$$

we see from (7.25) and (7.26) that

$$S_d(t) = \frac{1}{10}\frac{d}{(a,d)}\varphi((a,d))\log(d^2/n) + O(d\varphi(a,d)/(a,d)) + O\left(\sigma_1(d/(a,d))\right) + O(d\sigma_1((a,d))/(a,d)),$$

where all implicit O-constants depend only on t_0 and t_1. The trivial inequality $\varphi((a,d)) \leq \sigma_1((a,d))$ therefore completes the proof. ∎

Lemma 7.8. *For $1 \leq t_0 \leq t \leq t_1$,*

$$h(F_n(j_5(it),Y)) = \frac{1}{10}[\Gamma(1):\Gamma_0(n)]\left(\log n - 2\sum_{p|n}\frac{\log p}{p} + O(1)\right)$$

as $n \to \infty$, where the O-constant depends only on t_0, t_1.

Proof. Using Lemmas 7.7 and 7.4, we see that

$$\begin{aligned} h(F_n(j_5(it),Y)) &= \sum_{ad=n,\ a>0} S_d(t) + O([\Gamma(1):\Gamma_0(n)]) \\ &= H_1 + H_2 + O([\Gamma(1):\Gamma_0(n)]), \end{aligned}$$

where

$$H_1 = \sum_{\substack{d|n \\ d<(nt)^{1/2}}} O(n/d) = O(\sum_{d|n} n/d) = O(\sigma_1(n)) = O([\Gamma(1):\Gamma_0(n)])$$

from [4, A2], and

$$\begin{aligned} H_2 &= \sum_{\substack{d|n \\ d\geq(nt)^{1/2}}} \left(\frac{1}{10}\frac{d}{(a,d)}\varphi((a,d))\log(d^2/n) + O(\sigma_1(d/(a,d))) + O(d\sigma_1((a,d))/(a,d))\right) \\ &= \sum_{\substack{d|n \\ d\geq(nt)^{1/2}}} \frac{1}{10}\frac{d}{(a,d)}\varphi((a,d))\log(d^2/n) + O([\Gamma(1):\Gamma_0(n)]) \end{aligned}$$

by (A2) and (A3) of [4]. We can rewrite this as

$$H_2 = \frac{1}{10}\sum_{d|n}\frac{d}{(a,d)}\varphi((a,d))(\log n - 2\log(n/d)) + O([\Gamma(1):\Gamma_0(n)]).$$

Finally, applying (A1) and Lemma A1 of [4], we obtain

$$H_2 = \frac{1}{10}[\Gamma(1):\Gamma_0(n)]\left(\log n - 2\sum_{p|n}\frac{\log p}{p} + O(1)\right),$$

as desired. ∎

We have thus estimated $h(F_n(j_5(it),Y))$. Using the next lemma, this estimate will enable us to obtain Theorem 7.1.

Lemma 7.9. *Let $P \in \mathbf{C}[Y]$ be any nonzero polynomial of degree $\leq D$. For any $\theta > 0$ there exists an absolute constant $c_\theta > 0$ depending only on θ such that*

$$|h(P) - \log \sup_{\theta\leq y\leq 2\theta}|P(y)|| \leq c_\theta D.$$

Proof. This follows from the proof of [4, Lemma 9] which establishes the result for $\theta = 1728$ but is in fact completely general. ■

We now prove Theorem 7.1. For convenience, we define $h(0) = -\infty$ and use the usual conventions with the symbol $-\infty$ in estimates below. Let $D = [\Gamma(1) : \Gamma_0(n)]$ and write

$$F_n(X,Y) = P_0(X)Y^D + P_1(X)Y^{D-1} + \cdots + P_D(X)$$

with $P_j \in \mathbf{Z}[X]$ and $P_0 \neq 0$. In what follows, we implicitly omit any P_j's that equal zero.

Certainly, $h(F_n) = \max_{0\le j\le D} h(P_j)$. Since the degree of P_j is at most D, Lemma 7.9 with $\theta = s \geq 1$ yields

$$h(F_n) = \max_{0\le j\le D} \log \sup_{s\le x\le 2s} |P_j(x)| + O(D) = \sup_{s\le x\le 2s} \max_{0\le j\le D} \log |P_j(x)| + O(D)$$

with an $O(D)$-term that lies outside of the supremum and has an O-constant depending only on s. Since $\max_{0\le j\le D} \log|P_j(x)| = h(F_n(x,Y))$ we get $h(F_n) = \sup_{s\le x\le 2s} h(F_n(x,Y)) + O(D)$. By the choice of s, the interval $[t_0, t_1]$ corresponds bijectively under $t \mapsto j_5(it)$ to the interval $[s, 2s]$, so any $x \in [s, 2s]$ satisfies $x = j_5(it)$ for some $t \in [t_0, t_1]$. Lemma 7.8 now completes the proof as $n \to \infty$ since $D = [\Gamma(1) : \Gamma_0(n)]$ and

$$\log n - 2\sum_{p|n} \frac{\log p}{p} \to \infty$$

as $n \to \infty$.

Remark 7.10. Let us illustrate Theorem 7.1. We have the following table, in which Φ_n denotes the classical modular polynomial of level n and H is the non-logarithmic height $H(\sum_I a_I X^I) = \max_I |a_I|$:

Level	$H(\Phi_n)$
32	$2^{12} \cdot 3^{144} \cdot 5^{144} \cdot 11^{72} \cdot 17^{18} \cdot 23^{36} \cdot 29^{36} \cdot 47^{27} \cdot 53^{18} \cdot 59^{18} \cdot 71^{9} \cdot 83^{18} \cdot 89^{18}$
41	$2^{684} \cdot 3^{126} \cdot 5^{126} \cdot 11^{36} \cdot 17^{18} \cdot 23^{27} \cdot 29^{36} \cdot 41^{3} \cdot 47^{18} \cdot 59^{9} \cdot 71^{18} \cdot 107^{9}$
47	$2^{774} \cdot 3^{144} \cdot 5^{153} \cdot 11^{72} \cdot 17^{36} \cdot 23^{27} \cdot 29^{27} \cdot 41^{9} \cdot 47^{3} \cdot 89^{18} \cdot 113^{18} \cdot 137^{9}$
53	$2^{900} \cdot 3^{162} \cdot 5^{162} \cdot 11^{54} \cdot 17^{54} \cdot 23^{18} \cdot 29^{18} \cdot 41^{18} \cdot 47^{18} \cdot 53^{3} \cdot 59^{9} \cdot 83^{18} \cdot 107^{18} \cdot 131^{18}$
59	$2^{972} \cdot 3^{180} \cdot 5^{198} \cdot 11^{81} \cdot 17^{18} \cdot 23^{36} \cdot 29^{36} \cdot 41^{18} \cdot 47^{18} \cdot 53^{18} \cdot 59^{3} \cdot 101^{18} \cdot 113^{9} \cdot 149^{18} \cdot 173^{9}$

Level	$H(F_n)$	$\log(H(\Phi_n))/\log(H(F_n))$
32	$2 \cdot 5 \cdot 937 \cdot 1997 \cdot 5381$	$51.4514292315\ldots$
41	$2^9 \cdot 3^4 \cdot 5^3 \cdot 41 \cdot 1459$	$52.7001592098\ldots$
47	$3^4 \cdot 5 \cdot 47 \cdot 311 \cdot 337 \cdot 4129$	$55.3569927370\ldots$
53	$2^3 \cdot 53 \cdot 843701 \cdot 2543873$	$55.1097204607\ldots$
59	$2^2 \cdot 59 \cdot 127 \cdot 22369 \cdot 231573773$	$54.3504335762\ldots$

Remark 7.11. One might be interested in comparing the q-series coefficients of j_5 with those of j. Indeed, we have

$$j_5 = q^{-1/5}\left(1 + q - q^3 + q^5 + q^6 - q^7 - 2q^8 + 2q^{10} + 2q^{11} - q^{12} - 3q^{13} - q^{14} + 3q^{15} + 3q^{16} - 2q^{17} + \cdots\right),$$

while

$$j = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + 333202640600q^5 + \cdots,$$

so it seems that the q-coefficients of j_5 are very small in comparison to those of j. Let us write $q^{1/5}j_5 = \sum_{n=0}^{\infty} c_n q^n$ and $j = q^{-1} + \sum_{n=0}^{\infty} b_n q^n$ with $b_n, c_n \in \mathbf{Z}$. One can adapt Rademacher's improvement of the Hardy-Littlewood circle method to obtain the (divergent) asymptotic expansion

$$c_n = \frac{2\pi}{5\sqrt{5n-1}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_1\left(\frac{4\pi}{25k}\sqrt{5n-1}\right) \tag{7.27}$$

as $n \to \infty$, where

$$I_1(u) = \int_{1-i\infty}^{1+i\infty} t^{-2} e^{t+u^2/4t}\, dt$$

is the I Bessel-function of order 1 and

$$A_k(n) = \sum_{\substack{h \in (\mathbf{Z}/5k\mathbf{Z})^\times \\ h \equiv \pm 1 \bmod 5}} e^{\frac{2\pi i}{25k}(h + \bar{h} - 5nh)}$$

with $h\bar{h} \equiv 1 \bmod 25k$. By "divergent" expansion we mean that at any finite truncation the series (7.27) gives a genuine asymptotic expansion for c_n as $n \to \infty$, and that we can prescribe an optimal cut-off point (depending on n) for any particular n.

Using the well-known estimate

$$I_1(u) \sim \frac{e^u}{(2\pi u)^{1/2}}$$

as $u \to \infty$ and taking the truncation at $k = 1$ in (7.27) yields

$$c_n \sim \frac{\sqrt{2}}{(5n-1)^{3/4}} \cos\left(\frac{2\pi}{25}(5n-2)\right) e^{\frac{4\pi}{25}\sqrt{5n-1}}. \tag{7.28}$$

It is *remarkable* how accurately this asymptotic on the first-term truncation approximates c_n. Indeed, we have the following table:

n	c_n	$\frac{\sqrt{2}}{(5n-1)^{3/4}} \cos\left(\frac{2\pi}{25}(5n-2)\right) e^{\frac{4\pi}{25}\sqrt{5n-1}}$
10	2	1.98558
21	5	4.90972
32	-7	-7.13225
43	-37	-37.055
54	-15	-14.4614
65	131	131.995
76	204	204.887
87	-216	-215.274
98	-875	-875.131
109	-279	-280.932
⋮	⋮	⋮
150	7939	7932.7
⋮	⋮	⋮
197	-23562	-23555.2

It is worth comparing the asymptotic formula (7.28) for c_n with that for b_n:

$$c_n \sim \frac{\sqrt{2}}{(5n)^{3/4}} \cos\left(\frac{2\pi}{25}(5n-2)\right) e^{\frac{4\pi}{5\sqrt{5}}\sqrt{n}},$$

$$b_n \sim \frac{1}{\sqrt{2}n^{3/4}} e^{4\pi\sqrt{n}},$$

so

$$\lim_{n\to\infty} \frac{\log b_n}{\log c_n} = 5\sqrt{5} = 11.1803398874989\ldots.$$

This explains why the coefficients of the q-expansion of j seem to be so much larger than the coefficients of the q-expansion of j_5.

8. Radical formulas for singular values in $\mathbf{R}$

An interesting question in the context of radical formulas for singular values of j_5 (or of Ramanujan's F) is whether such formulas can be given inside of $\mathbf{R}$ when the singular value lies in $\mathbf{R}$.

Definition 8.1. An finite extension of subfields $E \subseteq E'$ inside of $\mathbf{R}$ is *solvable in real radicals* if there exists a finite tower

$$E = E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$$

in $\mathbf{R}$ with $E' \subseteq E_n$ and $E_i = E_{i-1}(a_i)$ with $a_i^{d_i} \in E_{i-1}$ for $1 < i \leq n$ and some positive integers d_i. A real algebraic number $\alpha \in \mathbf{R}$ is *solvable in real radicals* if $\mathbf{Q}(\alpha)/\mathbf{Q}$ is solvable in real radicals.

Remark 8.2. Despite appearances, this definition is a property of the abstract extension E'/E: it is independent of how E' is embedded in $\mathbf{R}$. Indeed, due to the existence and (non-canonical) uniqueness of real closures of real fields, and the evident fact that E'/E is an algebraic extension of real fields, we see that Definition 8.1 says exactly that E' admits an E-embedding into a radical tower in a real closure of E.

Pick $\tau \in \mathbf{C} - \mathbf{R}$ that is quadratic over $\mathbf{Q}$, and assume $j_5(\tau) \in \mathbf{R}$ (or equivalently, assume τ is $\Gamma(5)$-equivalent to $-\overline{\tau}$; the typical example is a purely imaginary τ, which is to say $\tau^2 \in \mathbf{Q}$). Let $K = \mathbf{Q}(\tau)$, so $K(j_5(\tau))/K$ is an abelian extension and clearly

$$[\mathbf{Q}(j_5(\tau)) : \mathbf{Q}] = [K(j_5(\tau)) : K]. \tag{8.1}$$

The question we wish to address is whether or not $j_5(\tau)$ is solvable in real radicals. Our analysis will only be applicable when $K(j_5(\tau))$ is Galois over $\mathbf{Q}$, and the description of the associated open subgroup in $\mathbf{A}_K^\times/K^\times$ provided by Corollary 3.3 shows that this condition holds when $\tau^2 \in \mathbf{Q}$. The solvability of such real singular values in real radicals is quite rare, as the following theorem makes clear:

Theorem 8.3. *Let $\tau \in \mathbf{C} - \mathbf{R}$ be quadratic over $\mathbf{Q}$ and assume τ is $\Gamma(5)$-equivalent to $-\overline{\tau}$. If $j_5(\tau) \in \mathbf{R}$ is solvable in real radicals then all odd prime factors of $[\mathbf{Q}(j_5(\tau)) : \mathbf{Q}]$ are Fermat primes, and if $[\mathbf{Q}(j_5(\tau)) : \mathbf{Q}]$ is a power of 2 then $j_5(\tau)$ lies in a tower of quadratic extensions over $\mathbf{Q}$ inside $\mathbf{R}$.*

In particular, if τ is a 5-unit and $\mathbf{C}^\times/q_\tau^{\mathbf{Z}}$ has CM by $\mathscr{O}_K$, then $j_5(\tau)$ is solvable in real radicals only if the size of the the ray class group of conductor 5 for $\mathbf{Q}(\tau)$ is of the form $2^e \prod_j p_j^{e_j}$ where the p_j's are Fermat primes.

The final part of the theorem follows from the rest because of (8.1) and the fact that the given additional conditions on τ imply that $\mathbf{Q}(\tau, j_5(\tau))$ is the ray class field of conductor 5 for $\mathbf{Q}(\tau)$ (by Corollary 5.7). In fact, the Fermat criterion on the size of the ray class group of conductor 5 may be replaced with the Fermat criterion for the usual class group because the ratio of the size of the two groups has only 2, 3, and 5 as possible prime factors. We also remark that the theorem is true for the classical j-function (with 5 replaced by 1 everywhere), using the same proof.

Example 8.4. A simple example where the necessary criterion of Theorem 8.3 is violated is $\tau = \sqrt{-101}$. Indeed, the ring of integers of $\mathbf{Q}(\sqrt{-101})$ is $\mathbf{Z}[\sqrt{-101}]$ and $\sqrt{-101}$ is a 5-unit, so $[\mathbf{Q}(j_5(\sqrt{-101})) : \mathbf{Q}]$ is the order of the the ray class group of conductor 5 for $\mathbf{Q}(\sqrt{-101})$. This group is $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/28\mathbf{Z}$, and the prime 7 is not a Fermat prime. Thus, $j_5(\sqrt{-101}) \in \mathbf{R}$ is not solvable in real radicals. Of course, it is solvable in complex radicals.

Other examples of the form $\tau = \sqrt{-n}$ with squarefree $n \equiv 1 \bmod 4$ and $5 \nmid n$ (so $\mathbf{Q}(\tau)$ has ring of integers $\mathbf{Z}[\tau]$ with τ a 5-unit) are $n = 149, 173, 341, 349$ with the prime 7 intervening, $n = 269, 389, 829, 1021$ with the prime 11 intervening, and $n = 941, 1181, 2837, 3401$ with the prime 23 intervening.

In view of the preceding remarks, Theorem 8.3 is a consequence of the following general result (with $K^+ = \mathbf{Q}$, $K = \mathbf{Q}(\tau)$, $L^+ = \mathbf{Q}(j_5(\tau))$, $L = \mathbf{Q}(\tau, j_5(\tau))$):

Theorem 8.5. *Let K^+ be a number field in $\mathbf{R}$ that is solvable in real radicals over $\mathbf{Q}$, and let K be a quadratic extension of K^+ in $\mathbf{C}$ with K not contained in $\mathbf{R}$. Let L/K be a finite abelian extension inside of $\mathbf{C}$ such that L/K^+ is Galois. Let $L^+ = L \cap \mathbf{R}$, so $[L : K] = [L^+ : K^+]$ and $L = K \otimes_{K^+} L^+$.*

If $[L : K]$ is a power of 2, then L^+/K^+ is a tower of quadratic extensions. If the real number field L^+ is solvable in real radicals over K^+ (or, equivalently, over $\mathbf{Q}$), then all odd prime factors of $[L : K]$ are Fermat primes.

This purely algebraic theorem can be formulated and proved in terms of a choice of real closure of a real number field K^+, but we prefer to work with the more concrete (but operationally equivalent) language of subfields of $\mathbf{R}$ and $\mathbf{C}$.

Proof. Let $\Gamma = \mathrm{Gal}(L/K)$. We may assume $\Gamma \neq \{1\}$. Since we have a short exact sequence

$$1 \to \Gamma \to \mathrm{Gal}(L/K^+) \to \mathrm{Gal}(K/K^+) \to 1$$

with Γ abelian, we may view Γ as a finite-length nonzero $\mathbf{Z}[\mathrm{Gal}(K/K^+)]$-module. Since $\mathrm{Gal}(K/K^+)$ has order 2, by decomposing Γ into its primary components it is clear that we can find a $\mathrm{Gal}(K/K^+)$-stable filtration by subgroups

$$1 = \Gamma_0 \subseteq \Gamma_1 \subseteq \cdots \subseteq \Gamma_n = \Gamma$$

such that $[\Gamma_i : \Gamma_{i-1}] = q_i$ is prime for all $1 \leq i \leq n$. We may clearly arrange for q_1 to be any prime factor q of the order of the abelian group Γ.

Let L_i be the fixed field of Γ_i in L, so the L_i's are a decreasing chain of subfields of L containing the subfield $K \not\subseteq \mathbf{R}$ and each L_i is Galois over K^+. Thus, $L_i^+ = L_i \cap \mathbf{R}$ is a decreasing chain of subfields of L^+ that contain K^+, and clearly $K \otimes_{K^+} L_i^+ \to L_i$ is an isomorphism. Thus, $[L_{i-1}^+ : L_i^+] = q_i$ for all i and L_i is Galois over $L_{i'}^+$ for $i' \geq i$. If $[L : K]$ is a power of 2 then $q_i = 2$ for all i and we have therefore expressed L^+ as a tower of quadratic extensions of K^+. This settles the existence result when $[L : K]$ is a power of 2. For the proof that when such a formula exists then all odd prime factors of $[L : K]$ are Fermat primes, we may now assume that $q_1 = q$ is any choice of odd prime factor of $[L : K]$ and we want to show that it is a Fermat prime. We can rename L_1^+ as K^+ (note that $L_1^+/\mathbf{Q}$ is solvable in real radicals!) and L_1 as K to reduce to the case when $[L : K] = [L^+ : K^+]$ is equal to q.

Let

$$K^+ = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m$$

be a tower of subfields of $\mathbf{R}$ such that $L^+ \subseteq E_m$ and $E_i = E_{i-1}(a_i)$ with $a_i^{d_i} = b_i \in E_{i-1}$ for $1 \leq i \leq m$ and positive integers d_i. Obviously we can assume that each $d_i = p_i$ is prime and that $[E_i : E_{i-1}] > 1$ for all i (so $b_i \neq 0$ for all i). We can also assume that L^+ is not contained in E_{m-1} (the case $L^+ = K^+$ is trivial). For each i, we claim that $[E_i : E_{i-1}] = p_i$. This is obvious if $p_i = 2$, so suppose p_i is odd. If $[E_i : E_{i-1}] < p_i$ then $T^{p_i} - b_i \in E_{i-1}[T]$ is reducible, and so b_i has a p_ith root $\beta \in E_{i-1}$ (see [15, Thm. 9.1, Ch. VI]). However, $a_i \in E_i - E_{i-1}$ is also a p_ith root of b_i, so the ratio $a_i/\beta \in E_i$ is a nontrivial p_ith root of unity. Since p_i is odd, this contradicts the fact that E_i is a subfield of $\mathbf{R}$. Thus, $[E_i : E_{i-1}] = p_i$ for all i.

Since $[L^+ : K^+] = q$ is prime and L^+ is not contained in E_{m-1}, the inclusion $K^+ \subseteq L^+ \cap E_{m-1}$ must be an equality. Consider the composite L^+E_{m-1} inside of E_m. This is an intermediate extension over E_{m-1} and is strictly larger than E_{m-1}, so since $[E_m : E_{m-1}] = p_m$ is prime we obtain $L^+E_{m-1} = E_m$. Thus, $[L^+E_{m-1} : E_{m-1}] = p_m$. However, we claim that $L^+ \otimes_{K^+} E_{m-1} \to L^+E_{m-1}$ is an isomorphism, and hence $p_m = [L^+ : K^+] = q$. To prove this isomorphism assertion it is enough to check after applying $K \otimes_{K^+} (\cdot)$ to both sides. We have $K \otimes_{K^+} L^+ = L$ since K/K^+ is a non-real quadratic extension, and similarly $K \otimes_{K^+} (L^+E_{m-1}) = KL^+E_{m-1} = LE_{m-1}$ (composites formed inside $\mathbf{C}$). Thus, we wish to show that the surjection

$$L \otimes_{K^+} E_{m-1} \twoheadrightarrow LE_{m-1}$$

is an isomorphism, and since L/K^+ is a Galois extension satisfying

$$L \cap E_{m-1} = (L \cap \mathbf{R}) \cap E_{m-1} = L^+ \cap E_{m-1} = K^+$$

it follows (see Lemma 8.7 below) that $L \otimes_{K^+} E_{m-1}$ is a field. This establishes the isomorphism claim.

We have proved that $E_m = L^+ \otimes_{K^+} E_{m-1}$, so by applying $K \otimes_{K^+} (\cdot)$ we see that

$$KE_m = K \otimes_{K^+} E_m = L \otimes_{K^+} E_{m-1} = L \otimes_K (K \otimes_{K^+} E_{m-1}) = L \otimes_K (KE_{m-1})$$

is a degree-q extension of KE_{m-1} that is Galois (since L/K is Galois) and generated by adjoining a qth root of a nonzero element $b_m \in E_{m-1}^\times \subseteq KE_{m-1}$ (since $E_m = E_{m-1}(a_m)$). Hence, KE_m must contain a primitive qth root of unity! Thus, $KE_m \cap \mathbf{R} = E_m$ must contain $\mathbf{Q}(\zeta_q)^+$. However, our initial hypothesis that K^+ be solvable in real radicals over $\mathbf{Q}$ implies the same for E_m, and hence $\mathbf{Q}(\zeta_q)^+$ is solvable in real radicals over $\mathbf{Q}$. Since $[\mathbf{Q}(\zeta_q)^+ : \mathbf{Q}] = (q-1)/2$, it is therefore enough to show that a *Galois* extension of $\mathbf{Q}$

inside of $\mathbf{R}$ that is solvable in real radicals must have degree over $\mathbf{Q}$ equal to a power of 2. This is a special case of the next theorem (with $E = \mathbf{Q}$ and $K = \mathbf{Q}(\zeta_q)^+$). ■

Theorem 8.6. *Let E be a field, and let K/E be a finite Galois extension. Assume that $[K : E]$ has order divisible by a prime p. If F is a radical tower over E into which K admits an E-embedding, then either F contains a root of unity of order p (so the characteristic is distinct from p) or F contains a primitive root of unity of odd prime order. In particular, if E is a real field and $[K : E]$ is odd and > 1, then F is not a real field.*

Some aspects of the proof of this theorem will be similar to steps in the proof of Theorem 8.5. However, the nature of the hypotheses are sufficiently different that it seems simpler to just repeat the similar steps and not to axiomatize the situation too much.

Proof. Since $\mathrm{Gal}(K/E) = [K : E]$ has order divisible by p, there must be a subgroup of order p. Thus, there is an intermediate field E' between K and E with K/E' Galois of degree p. By using an E-embedding of K into F, we may rename E' as E to reduce to the case $[K : E] = p$.

We may express the radical tower F/E in steps

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = F$$

where $E_{i+1} = E_i(a_i)$ with $a_i^{p_i} \in E_i$ for primes p_i. We may certainly assume $[E_{i+1} : E_i] > 1$ for all i without loss of generality. *Fix* an E-embedding of K into F. Consider the intersection $K \cap E_{n-1}$, a field between K and E. Since $[K : E]$ is prime, either $K \cap E_{n-1} = K$ or $K \cap E_{n-1} = E$. If the former, then $K \subseteq E_{n-1}$ so we can rename E_{n-1} as F and induct on n (once we handle the case $n = 1$!). On the other hand, if $K \cap E_{n-1} = E$ then consider the composite field KE_{n-1} inside of F. This is finite Galois over E_{n-1} of degree > 1. The following well-known lemma (using $k = E$, $F_0 = E_{n-1}$) ensures that $[KE_{n-1} : E_{n-1}] = [K : E] = p$.

Lemma 8.7. *Let F/k be an extension of fields and let K/k be a subextension that is finite Galois. Let F_0/k be another intermediate extension with $K \cap F_0 = k$. The natural map $K \otimes_k F_0 \to KF_0$ is an isomorphism.*

Proof. Let y be a primitive element for K/k, say with minimal polynomial $f \in k[T]$. Note that K/k is a splitting field of f over k. Since KF_0/F_0 is generated by a root of f, it is necessary and sufficient to prove that $f \in F_0[T]$ is irreducible. Suppose $f = gh$ is a monic factorization of f over F_0; it suffices to show that this factorization is trivial. Since f splits over K and hence over F, when we consider the factorization $f = gh$ in $F[T]$ we see that g and h split over F and hence their coefficients may be expressed as $\mathbf{Z}$-polynomials in the roots of f (recall that g and h were chosen to be monic). But the roots of f in F lie in K, so the coefficients of g and h in F lie in K. Hence, g and h as elements in $F[T]$ lie in $(K \cap F_0)[T] = k[T]$, so our factorization of f takes place in $k[T]$. But f is irreducible in $k[T]$, so our factorization is indeed trivial. ■

Thus, by renaming E_{n-1} as E and KE_{n-1} as K, we get to the special case $n = 1$, which is to say that $F = E(a)$ with $a^{p'} = b \in F^\times$ for some prime p' and K/E is an intermediate Galois extension of prime degree p. We claim that either $[F : E] = p'$ or else $F = E(\zeta)$ with ζ a primitive p'th root of unity (and the characteristic is distinct from p'). Consider the polynomial $T^{p'} - b$ in $E[T]$. If this is irreducible, then clearly F is E-isomorphic to $E[T]/(T^{p'} - b)$ and hence $[F : E] = p'$. On the other hand, if $T^{p'} - b$ is reducible over E then $b = c^{p'}$ for some $c \in E^\times$ (by [15, Thm. 9.1, Ch. VI]). In this case, $\zeta = a/c$ is a nontrivial p'th root of unity (since $a \notin E$, as $F = E(a)$ with $[F : E] > 1$). In particular, the characteristic is not equal to p' and $F = E(\zeta)$ is generated by a primitive p'th root of unity.

If $[F : E] = p'$, then since $p = [K : E]$ must divide $[F : E]$, we get $p' = p$ and $K = F$, so in fact F/E is a finite Galois extension of degree p. However, this extension is generated by extracting a pth root a of an element $b \in E^\times$, so the characteristic cannot be p. Since $[F : E] > 1$, the minimal polynomial of a over E is a factor of $T^p - b \in E[T]$ with degree larger than 1 and this factor must split over the normal extension F. Any other root in F for this factor has to have the form $a\zeta$ with $\zeta \neq 1$ a pth root of unity. Hence, we deduce that F contains a primitive pth root of unity when $[F : E] = p'$. But in the case $[F : E] \neq p'$ we must have

$F = E(\zeta)$ for a primitive p'th root of unity (with p' distinct from the characteristic), and K/E is a degree-p subextension. Hence, $[F : E] > 1$, so $p' > 2$. Thus, F contains a root of unity of odd prime order. ∎

Appendix A. The Action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ on j_5

Choose $N \geq 1$ and let $\zeta \in \mathbf{C}^\times$ be a primitive Nth root of unity. Since $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generate $\mathrm{SL}_2(\mathbf{Z})$ and hence generate the quotient $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, we can determine the action of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ on $\mathbf{C}(X_\zeta(N))$ by determining the action of S and T on this function field. In genus-zero cases, it is enough to describe how S and T act on a rational parameter.

Example A.1. The rational parameter $j_{5,\zeta}$ on $X_\zeta(5)$ is transformed under the action of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ according to a representation ρ_ζ^{an} of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ in $\mathrm{Aut}(\mathbf{CP}^1) \simeq \mathrm{PGL}_2(\mathbf{C})$.

In order to better understand the representations ρ_ζ^{an} in $\mathrm{Aut}(X_\zeta(N))$, particularly their use in proving some classical identities with coefficients in $\mathbf{Q}$ (and not only in $\mathbf{Q}(\zeta)$), as we shall discuss in Appendix C for $N = 5$, it is convenient to develop a variant of ρ_ζ^{an} over $\mathbf{Q}$ that recovers the ζ-dependent construction ρ_ζ^{an} over $\mathbf{C}$ (or over any field of characteristic 0 that splits $X^N - 1$). The main point is to replace the constant group $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ with a non-constant finite étale symplectic group over $\operatorname{Spec} \mathbf{Q}$

Fix $N \geq 1$. There is a canonical non-degenerate symplectic pairing of étale sheaves on $\operatorname{Spec} \mathbf{Q}$

$$\langle \cdot, \cdot \rangle : (\mu_N \times \mathbf{Z}/N\mathbf{Z}) \times (\mu_N \times \mathbf{Z}/N\mathbf{Z}) \to \mu_N$$

given by $\langle (\zeta, a), (\zeta', a') \rangle = \zeta^{a'} \zeta'^{-a}$. Let

$$G = \mathrm{Sp}(\mu_N \times \mathbf{Z}/N\mathbf{Z}) = \mathbf{Aut}(\mu_N \times \mathbf{Z}/N\mathbf{Z}, \langle \cdot, \cdot \rangle)$$

be the associated symplectic group, so G is a finite étale $\mathbf{Q}$-group. Over a splitting field $K_N/\mathbf{Q}$ of $X^N - 1$, a choice of primitive Nth root of unity $\zeta \in K_N^\times$ identifies μ_N with $\mathbf{Z}/N\mathbf{Z}$ and carries $\langle \cdot, \cdot \rangle$ to the determinant form on $(\mathbf{Z}/N\mathbf{Z})^2$, so this identifies $G_{/K_N}$ with the constant group $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Of course, changing ζ changes this identification with $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ (in a manner that we shall make explicit shortly).

Functorially, for a $\mathbf{Q}$-algebra R we can uniquely describe any point $\gamma \in G(R)$ as $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $a, d \in (\mathbf{Z}/N\mathbf{Z})^\times(R)$ are R-automorphisms of μ_N and $\mathbf{Z}/N\mathbf{Z}$ respectively, $b \in \mu_N(R)$, and $c : \mu_N \to \mathbf{Z}/N\mathbf{Z}$ is an R-group map. In this description, the preservation of $\langle \cdot, \cdot \rangle$ by γ says $ad - c(b) = 1$ and (following the conventions preceding Remark 2.5) there is a canonical left action

$$\rho : G \times X_\mu(N) \to X_\mu(N) \tag{A.1}$$

over $\mathbf{Q}$ given away from the cusps by

$$(\gamma, (E, \iota)) \mapsto (E, \iota \circ \gamma')$$

with $\gamma' = \left(\begin{smallmatrix} d & b \\ c & a \end{smallmatrix}\right)$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We can also describe ρ as a map of smooth $\mathbf{Q}$-groups

$$\rho : G \to \mathbf{Aut}(X_\mu(N)),$$

where $\mathbf{Aut}(Z)$ denotes the Aut-scheme of Grothendieck for any projective $\mathbf{Q}$-scheme Z (this is a quasi-projective $\mathbf{Q}$-group, and it is smooth by Cartier's theorem). The scheme-theoretic image $\rho(G)$ is a finite étale $\mathbf{Q}$-subgroup of $\mathbf{Aut}(X_\mu(N))$, and since $G \to \rho(G)$ is a finite étale surjection we see that a field splitting G also splits $\rho(G)$.

Upon extending scalars to a splitting field $K_N/\mathbf{Q}$ of $X^N - 1$ and using a primitive Nth root of unity $\zeta \in K_N^\times$ to identify μ_N and $\mathbf{Z}/N\mathbf{Z}$, we may describe $\rho_{/K_N}$ as a map of smooth K_N-groups

$$\rho_\zeta : \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) = G_{/K_N} \to \mathbf{Aut}(X_\zeta(N))_{/K_N},$$

and since the source group is a constant group we can equivalently consider ρ_ζ as a map of ordinary groups (of K_N-points)

$$\rho_\zeta : \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \to \mathrm{Aut}_{K_N}(X_\zeta(N)).$$

Upon choosing an embedding $\iota : K_N \hookrightarrow \mathbf{C}$, this recovers $\rho_{\iota(\zeta)}^{\mathrm{an}}$ as in Example A.1.

If $\zeta' = \zeta^e$ for $e \in (\mathbf{Z}/N\mathbf{Z})^\times$ then by using $\alpha_{\zeta',\zeta} : X_\zeta(N)_{/K_N} \simeq X_{\zeta'}(N)_{/K_N}$ as in Remark 2.5 (this isomorphism respects the canonical identifications of source and target with $X_\mu(N)_{/K_N}$) we see that ρ_ζ is carried to $\rho_{\zeta'} \circ c_e$ where c_e denotes the conjugation action

$$\gamma \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & e \end{smallmatrix}\right) \cdot \gamma \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{-1} \end{smallmatrix}\right)$$

on $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ (here we are using the intervention of $\gamma \mapsto \gamma'$ in the definition of ρ and the fact that $(\gamma_1\gamma_2)' = \gamma_2'\gamma_1'$).

Under the natural action of $\mathrm{Gal}(K_N/\mathbf{Q})$ on

$$\mathrm{Aut}_{K_N}(X_\mu(N)_{/K_N}) = \mathbf{Aut}(X_\mu(N))(K_N),$$

any $\sigma \in \mathrm{Gal}(K_N/\mathbf{Q})$ gives rise to an isomorphism

$$[\sigma] : \mathrm{Aut}_{K_N}(X_\zeta(N)_{/K_N}) = \mathbf{Aut}(X_\mu(N))(K_N) \overset{\sigma}{\simeq} \mathbf{Aut}(X_\mu(N))(K_N) = \mathrm{Aut}_{K_N}(X_{\sigma(\zeta)}(N)_{/K_N})$$

that is exactly intertwining with $\alpha_{\sigma(\zeta),\zeta}$. Thus, by looking back at the original definition of the $\mathbf{Q}$-group G we conclude that

$$[\sigma] \circ \rho_\zeta = \rho_{\sigma(\zeta)} = \rho_\zeta \circ c_{e^{-1}}. \tag{A.2}$$

We conclude the first part of:

Theorem A.2. *The subgroup* $\rho_\zeta(\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})) \subseteq \mathrm{Aut}_{K_N}(X_\zeta(N)) = \mathrm{Aut}_{K_N}(X_\mu(N)_{/K_N})$ *is independent of* ζ *and is* $\mathrm{Gal}(K_N/\mathbf{Q})$*-stable.*

When $N = 5$ *and we identify* $X_\mu(5)$ *with* $\mathbf{P}^1_{\mathbf{Q}}$ *by means of* $j_{5,\mu}$ *and thereby identify* $\mathbf{Aut}(X_\mu(5))$ *with* $\mathrm{PGL}_{2/\mathbf{Q}}$*, the resulting subgroups*

$$\rho_\zeta(\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})) \subseteq \mathrm{PGL}_2(\mathbf{Q}(\zeta_5))$$

are independent of the choice of primitive 5*th root of unity* ζ *in* $\mathbf{Q}(\zeta_5)$ *and this subgroup is* $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$*-stable.*

Proof. The only issue that requires clarification for the second part is that the classical action of $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$ on $\mathrm{PGL}_2(\mathbf{Q}(\zeta_5))$ agrees with the "base change" action denoted $[\sigma]$ above that rested on the functorial description of PGL_2 as the automorphism scheme of $\mathbf{P}^1_{\mathbf{Q}} = X_\mu(5)$ (where this final equality is defined by means of $j_{5,\mu} \in \mathbf{Q}(X_\mu(5))$). This agreement comes down to the evident fact that the standard identification of $\mathrm{GL}_n(k)/k^\times$ with $\mathrm{Aut}_k(\mathbf{P}^n_k)$ for a field k carries the $\mathrm{Aut}(k)$-action on matrices over to the base-change action on k-automorphisms of the k-scheme $\mathbf{P}^n_k$. ∎

For a primitive 5th root of unity ζ in $\mathbf{C}$, we shall now describe the images of $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{PGL}_2(\mathbf{Q}(\zeta))$ under ρ_ζ^{an} (*cf.* [7, vol. 2, p. 382]).

Theorem A.3. *The action of* $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ *on* $\mathbf{C}(X_\zeta(5))$ *satisfies*

$$Tj_{5,\zeta} = \zeta^{-1} j_{5,\zeta} \qquad Sj_{5,\zeta} = \frac{-(\zeta^2 + \zeta^{-2}) j_{5,\zeta} + 1}{j_{5,\zeta} + (\zeta^2 + \zeta^{-2})}. \tag{A.3}$$

Proof. Let $K \subseteq \mathbf{C}$ be the splitting field of $X^5 - 1$. The moduli-theoretic approach over $\mathrm{Spec}\, K$ shows that $Tj_{5,\zeta}$ and $Sj_{5,\zeta}$ must be degree-1 rational functions in $j_{5,\zeta}$ over K, and an application of (A.2) and the identity $\alpha^*_{\zeta',\zeta}(j_{5,\zeta'}) = j_{5,\zeta}$ ensure that these rational functions must compatible with change in ζ in the sense that if

$$\rho_\zeta(g)(j_{5,\zeta}) = \frac{a_\zeta j_{5,\zeta} + b_\zeta}{c_\zeta j_{5,\zeta} + d_\zeta}$$

for

$$M_\zeta = \begin{pmatrix} a_\zeta & b_\zeta \\ c_\zeta & d_\zeta \end{pmatrix} \in \mathrm{PGL}_2(K)$$

then for any $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ we have $\sigma(M_\zeta) = M_{\sigma(\zeta)}$ in $\mathrm{PGL}_2(K)$. Thus, it is enough to prove the result for a single choice of ζ in $\mathbf{C}$.

We shall now choose a connected component $\mathfrak{H}$ of $\mathbf{C} - \mathbf{R}$ and let $\zeta = e^{2\pi i/5}$ with $i = \sqrt{-1} \in \mathfrak{H}$; via π_ζ this lifts the $\mathrm{SL}_2(\mathbf{Z})$-action on $X_\zeta(5)$ to the standard action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathfrak{H}$ and carries $j_{5,\zeta}$ back to j_5. Hence, T and S lift through π_ζ to the respective automorphisms $[T] : \tau \mapsto \tau + 1$ and $[S] : \tau \mapsto -1/\tau$ on $\mathfrak{H}$. The first relation in (A.3) is therefore obvious on $\mathfrak{H}$ via the q-expansion of j_5 at ∞ (4.8).

For the second relation, observe that (4.3) and (4.5) give

$$([S]^* j_5)(\tau) = j_5(-1/\tau) = \frac{\kappa_{(0,\frac{2}{5})}\kappa_{(\frac{1}{5},-\frac{2}{5})}\kappa_{(\frac{2}{5},-\frac{2}{5})}\kappa_{(\frac{2}{5},\frac{2}{5})}\kappa_{(\frac{1}{5},\frac{2}{5})}}{\kappa_{(0,\frac{1}{5})}\kappa_{(\frac{1}{5},-\frac{1}{5})}\kappa_{(\frac{2}{5},-\frac{1}{5})}\kappa_{(\frac{2}{5},\frac{1}{5})}\kappa_{(\frac{1}{5},\frac{1}{5})}}$$

for $\tau \in \mathfrak{H}$. Now apply (4.6) to expand this as a q-series on $\mathfrak{H}$. One finds

$$([S]^* j_5)(\tau) = -(\zeta^2 + \zeta^{-2}) + q_\tau^{1/5}(3 + \zeta + \zeta^{-1}) + \cdots,$$

and since

$$j_5(\tau) = q_\tau^{-1/5} + q_\tau^{4/5} - q_\tau^{14/5} + \cdots,$$

it is not hard to deduce that

$$\frac{3 + \zeta + \zeta^{-1}}{Sj_{5,\zeta} + (\zeta^2 + \zeta^{-2})} - j_{5,\zeta}$$

is a meromorphic function on $X_\zeta(5)$ with no poles. It is therefore a constant. Inspection of the q-series at ∞ shows that this constant is $\zeta^2 + \zeta^{-2}$, and the proof of the theorem is complete upon simplification. ∎

Remark A.4. It is now an easy matter to prove Ramanujan's evaluation of $F(i)$ for a primitive 4th root of unity i in $\mathbf{C}$, without requiring Watson's identity (1.3). Indeed, i is fixed by $\tau \mapsto -1/\tau$, so we can use (A.3) with $\zeta = e^{\pm 2\pi i/5}$ to obtain

$$j_5(i) = \frac{-(\zeta^2 + \zeta^{-2})j_5(i) + 1}{j_5(i) + (\zeta^2 + \zeta^{-2})};$$

either of the specific choices of ζ ensure that $\tau \mapsto -1/\tau$ on $\mathbf{C} - \mathbf{R}$ lifts the S-action through π_ζ. For these choices of ζ, we have $\zeta^2 + \zeta^{-2} = -(1 + \sqrt{5})/2$ with $\sqrt{5} > 0$. The visibly positive $j_5(i)$ is therefore the unique positive root of

$$X^2 - (1 + \sqrt{5})X - 1 = 0,$$

so $F(i) = 1/j_5(i)$ is the unique positive root of $Y^2 + (1+\sqrt{5})Y - 1 = 0$. This yields (1.1). We can also similarly evaluate $F(\zeta_3)$ for a primitive 3rd root of unity $\zeta_3 = (-1 \pm \sqrt{-3})/2$, as ζ_3 is fixed by $ST : \tau \mapsto -1/(\tau + 1)$. The identity (1.2) may also be verified by these methods.

Appendix B. Values at cusps

To avoid confusion concerning how points in $\mathbf{P}^1(\mathbf{Q})$ are mapped into a modular curve, and to ensure that the moduli-theoretic action of $\mathrm{SL}_2(\mathbf{Z})$ on $X_\zeta(5)$ lifts (via π_ζ) to the standard linear-fractional action, fix a connected component $\mathfrak{H}$ in $\mathbf{C} - \mathbf{R}$ and take $\zeta = e^{2\pi i/5}$ with $i = \sqrt{-1} \in \mathfrak{H}$. We will identify $\mathfrak{H}$ with the quotient of $\mathbf{C} - \mathbf{R}$ under negation, and so we will work with the modular curve $X_\zeta(5)$ as a quotient of $\mathfrak{H}$. In particular, we consider $c \in \mathbf{P}^1(\mathbf{Q})$ as representing a cusp by means of punctured neighborhoods taken in the horocycle topology on $\mathfrak{H}$. Using [19, Lemma 1.42], we get a set of representatives:

$$\{0, 2/9, 1/4, 2/7, 1/3, 2/5, 1/2, 5/8, 2/3, 3/4, 1, \infty\}.$$

The points 0, 5/8, ∞, and 2/5 are each $\Gamma(5)$-equivalent to their negatives, and hence at cusps represented by these points we can expect to get a formula for the value of j_5 that is independent of the choice of $\mathfrak{H}$; this cannot be expected (and indeed, does not happen) at the other cusps. There are two methods that we can use to evaluate j_5 at the cusps. We can work algebraically via Theorem A.3 (this requires explicitly computing a word in S and T that carries ∞ to a chosen cusp) or we can work analytically with Klein forms. We shall present the analytic approach via Klein forms, and leave the computational details of the algebraic method to the interested reader.

Our list of transformation properties for Klein forms in §4 allows us to compute how the κ_a's transform under the action of $\mathrm{SL}_2(\mathbf{Z})$. Thus, via (4.7) we can compute the q-expansion for j_5 at any cusp and we can thereby compute the value of j_5 at each cusp. For example, the cusp $2/9$ is taken to ∞ by the matrix

$$\alpha = \begin{pmatrix} -4 & 1 \\ -9 & 2 \end{pmatrix}.$$

We apply (4.5) to the product (4.7) and employ the relation (4.3) together with (4.2) to obtain

$$j_5 \circ \alpha^{-1} = -\frac{\kappa_{(0,\frac{2}{5})}\kappa_{(\frac{2}{5},0)}\kappa_{(\frac{1}{5},\frac{1}{5})}\kappa_{(\frac{1}{5},\frac{2}{5})}\kappa_{(\frac{2}{5},\frac{1}{5})}}{\kappa_{(0,\frac{1}{5})}\kappa_{(\frac{1}{5},0)}\kappa_{(\frac{2}{5},\frac{2}{5})}\kappa_{(\frac{1}{5},-\frac{2}{5})}\kappa_{(\frac{2}{5},-\frac{1}{5})}}.$$

Using (4.6), we find that for $\tau \in \mathbf{C} - \mathbf{R}$,

$$j_5 \circ \alpha^{-1}(\tau) = -(1 + \zeta_\tau^{-1}) + (1 + 3\zeta_\tau + \zeta_\tau^2)q_\tau^{1/5} + O(q_\tau^{2/5})$$

with $\zeta_\tau = e^{2\pi i_\tau/5}$. Let us now take $\tau \in \mathfrak{H}$, so $\zeta_\tau = \zeta = e^{2\pi i/5} \in \mathfrak{H}$. We conclude that the value of j_5 at the cusp represented (via $\mathfrak{H}$) by $2/9$ is $-(1+\zeta^{-1})$. The computations for the other cusps are similar, and so we obtain the following table:

Table B.1

Cusp Representative	0	$2/9$	$1/4$	$2/7$	$1/3$	$2/5$
Value of j_5	$-(\zeta^2+\zeta^{-2})$	$-(1+\zeta^{-1})$	$-(\zeta^{-2}+\zeta^{-1})$	$-(1+\zeta^{-2})$	$-(\zeta^2+\zeta^{-1})$	0
Cusp Representative	$1/2$	$5/8$	$2/3$	$3/4$	1	∞
Value of j_5	$-(\zeta+\zeta^{-2})$	$-(\zeta+\zeta^{-1})$	$-(1+\zeta^2)$	$-(1+\zeta)$	$-(\zeta+\zeta^2)$	∞

Remark B.2. Observe that the cusps 0, $5/8$, ∞, and $2/5$ represent $\Gamma(5)$-orbits that are invariant under negation, and the values of j_5 at these cusps are independent of $\mathfrak{H}$, or equivalently are invariant under replacing $\zeta = e^{2\pi i/5}$ with $\zeta^{-1} = e^{-2\pi i/5}$ (as we knew they had to be). In contrast, at a pair of cusp representatives such as $2/9$ and $3/4$, with $3/4$ in the $\Gamma(5)$-orbit of $-2/9$, the values of j_5 are related by replacing ζ with ζ^{-1}.

By Lemma 4.2, we can construct many meromorphic functions on $X_\zeta(5)$. Indeed, the construction of suitable finite subsets $\mathscr{A} \subseteq (5^{-1}\mathbf{Z})^2$ and functions $m : \mathscr{A} \to \mathbf{Z}$ as in Lemma 4.2 requires nothing more than linear algebra. Given any such meromorphic function

$$f = \prod_{a \in \mathscr{A}} \kappa_a^{m(a)}$$

on $X_\zeta(5)$, we can readily determine the order of f at each of the 12 cusps of $X_\zeta(5)$, and it is clear from (4.6) that any such f has divisor supported on the cusps of $X_\zeta(5)$.

Explicitly, the product formula (4.6) tells us $f(\tau) = q_\tau^d(1 + \cdots)$, where

$$d = \frac{1}{2} \sum_{(a_1,a_2) \in \mathscr{A}} (a_1^2 - a_1)m(a_1, a_2).$$

Now let $g_c \in \mathrm{SL}_2(\mathbf{Z})$ take the cusp c to ∞, and write $g_c = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. The order of f at c must be

$$\frac{1}{2} \sum_{(a_1,a_2)\in\mathscr{A}} ((a_1\alpha + a_2\gamma \bmod 1)^2 - (a_1\alpha + a_2\gamma \bmod 1))m(a_1,a_2). \tag{B.1}$$

In Table B.1, we have listed the value of j_5 at each of the cusps of $X_\zeta(5)$, so for any cusp c we can explicitly write down the function

$$\varphi_c = \begin{cases} (j_5 - j_5(c))^{-1} & \text{if } c \neq \infty \\ j_5 & \text{if } c = \infty, \end{cases} \tag{B.2}$$

and since $\mathbf{C}(X_\zeta(5)) = \mathbf{C}(j_5)$ we see that φ_c has a simple pole at c and no other poles. Using these functions φ_c, the proof of any given modular identity is reduced to a finite q-series computation.

Example B.3. We illustrate the preceding considerations by proving the identity (6.14). By Theorem 6.9 we know that

$$f = j_5(\tau/5)^5 = \left(\frac{\kappa_{(\frac{2}{5},0)}}{\kappa_{(\frac{1}{5},0)}}\right)^5$$

is a rational function of j_5, though this also follows from Lemma 4.2 and Theorem 4.3. We find that f has simple poles at the cusps ∞, $1/4$, $1/3$, $1/2$, 1, and simple zeroes at $2/9$, $2/7$, $2/5$, $2/3$, $3/4$. Thus, by Table B.1,

$$\frac{f}{j_5} \cdot \frac{(j_5 + \zeta^{-2} + \zeta^{-1})(j_5 + \zeta^2 + \zeta^{-1})(j_5 + \zeta^{-2} + \zeta)(j_5 + \zeta^2 + \zeta)}{(j_5 + 1 + \zeta^{-1})(j_5 + 1 + \zeta)(j_5 + 1 + \zeta^{-2})(j_5 + 1 + \zeta^2)}$$

is constant. Evaluation at ∞ shows this constant is 1. Upon simplification we obtain

$$f = j_5 \cdot \frac{j_5^4 + 3j_5^3 + 4j_5^2 + 2j_5 + 1}{j_5^4 - 2j_5^3 + 4j_5^2 - 3j_5 + 1}.$$

Appendix C. Computing $F_n(X,Y)$

For any $n \geq 1$ relatively prime to 5, in §6 we proved the existence and uniqueness of a primitive polynomial $F_n \in \mathbf{Z}[X,Y]$ such that F_n is absolutely irreducible over $\mathbf{Q}$ and F_n is an algebraic relation satisfied by the functions $j_5(\tau)$ and $j_5(n\tau)$. We now turn to the task of explicitly computing $F_n(X,Y)$ for such n.

Klein [7, vol. 2, pp. 137–151] worked out $F_n(X,Y)$ for $n \leq 11$ and $n = 13$ with $\gcd(n,5) = 1$ using invariant theory and linear algebra on q-expansions. Some of these modular correspondences have been re-proved in recent years by other methods (see for example [23]). In this section, we aim to illustrate that modern computers allow us to apply Klein's far superior techniques to efficiently compute F_n for many values of n. Throughout this section, we closely follow the methods of Klein [7, vol. 2] but we systematically work over $\mathbf{Q}$ whenever possible (as this seems the best perspective for explaining why many of the polynomial-identity formulas we shall establish only involve $\mathbf{Q}$-coefficients).

We have seen in Appendix A that the action of the finite étale non-constant symplectic $\mathbf{Q}$-group $G = \mathrm{Sp}(\mu_5 \times \mathbf{Z}/5\mathbf{Z})$ on $X_\mu(5)$ together with the isomorphism $j_{5,\mu} : X_\zeta(5) \xrightarrow{\sim} \mathbf{P}^1_{\mathbf{Q}}$ gives a projective representation

$$\rho : G \longrightarrow \mathrm{PGL}_{2/\mathbf{Q}}$$

as $\mathbf{Q}$-groups. We refer the reader to Appendix A for the description of ρ upon extending scalars to a field that splits $X^5 - 1$. By inspecting the definition of ρ (and working on geometric points), we see that $\ker \rho$ is the order-2 center μ_2 of G.

Theorem C.1. *The projective representation ρ lifts uniquely to a representation*

$$\widetilde{\rho} : G \to \mathrm{SL}_{2/\mathbf{Q}},$$

and this representation is faithful. This uniqueness persists upon any extension of the ground field.

Of course, upon extending scalars to a field that splits $X^5 - 1$ and picking a primitive 5th root of unity ζ we can deduce from the theorem (and Theorem A.2) that the ordinary representation

$$\rho_\zeta : \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) \to \mathrm{PGL}_2(\mathbf{Q}(\zeta))$$

uniquely lifts to a representation

$$\widetilde{\rho}_\zeta : \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Q}(\zeta))$$

that is moreover faithful and has image that is both independent of ζ and Galois-stable.

Proof. We begin by giving a constructive proof of existence by means of modular forms, as this will be used later. The functorial left action of G on $X_\mu(5)$ lifts to an action on the universal generalized elliptic curve $f : E \to X_\mu(5)$. Whereas the kernel of ρ is the center μ_2 in G, clearly μ_2 actions by negation on the universal elliptic curve.

The pushforward $\omega = \omega_{E/X_\mu(5)}$ of the relative dualizing sheaf is a line bundle on $X_\mu(5)$ and its formation commutes with arbitrary change of base on $X_\mu(5)$, so we get an action of G on each tensor power $\omega^{\otimes k}$ covering the action on $X_\mu(5)$ for every $k \geq 0$. We thereby get a representation of G on the $\mathbf{Q}$-model

$$M_k = \mathrm{H}^0(X_\mu(5), \omega^{\otimes k}) \tag{C.1}$$

for the space of weight-k modular forms of full level 5.

Let $\mathcal{C} \hookrightarrow X_\mu(5)$ be the reduced degree-12 divisor of cusps of $X_\mu(5)$. The Kodaira–Spencer isomorphism over $Y_\mu(5)$ induces an isomorphism of sheaves on $X_\mu(5)$

$$\omega^{\otimes 2} \simeq \Omega^1_{X_\mu(5)}(\mathscr{C}). \tag{C.2}$$

Since $X_\mu(5) \simeq \mathbf{P}^1_{\mathbf{Q}}$, we know that $\Omega^1_{X_\mu(5)/\mathbf{Q}}$ has degree -2, and since $\mathscr{C}$ has degree 12 we conclude from (C.1) and (C.2) that ω has degree 5 and that $\dim M_k = 5k + 1$ for all $k \geq 0$.

Lemma C.2. *The subspace $V \subseteq M_5$ of cusp forms of level 5 and weight 5 with q-expansion coefficients in $\mathbf{Q}$ at ∞ and vanishing to order at least 2 along $\mathscr{C}$ is 2-dimensional, G-stable, and irreducible.*

A $\mathbf{Q}$-basis for V is

$$X_a = \left(\kappa_{(\frac{1+a}{5},0)}\kappa_{(\frac{1+a}{5},\frac{1}{5})}\kappa_{(\frac{1+a}{5},\frac{2}{5})}\kappa_{(\frac{1+a}{5},-\frac{2}{5})}\kappa_{(\frac{1+a}{5},-\frac{1}{5})}\right)^{-1}, \tag{C.3}$$

for $a = 0, 1$. Moreover, X_a has the q-product expansion

$$X_a = q^{(2+a)/5}\prod_{k=1}^{\infty}(1-q^{5k})(1-q^k)^9 \prod_{\substack{k>0 \\ k\equiv\pm(2-a) \bmod 5}} (1-q^k) \tag{C.4}$$

for $a = 0, 1$.

Proof. By our calculations above, for a G-stable effective divisor D on $X_\mu(5)$ we see that the G-stable subspace $\mathrm{H}^0(X_\mu(5), \omega^{\otimes 5}(-D))$ in M_5 has dimension $25 - \deg(D) + 1$. The j-map $X_\mu(5) \to X(1)$ is G-equivariant with fibers of order $60 = |\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})/\{\pm 1\}|$ away from $0, 1728, \infty \in X(1)$ and fibers of orders 30, 20, and 12 over $0, 1728, \infty \in X(1)$ respectively, and the only pair of such orders that add up to 24 is 12+12. Thus, the only degree-24 effective G-invariant divisor on $X_\mu(5)$ is $2\mathscr{C}$, and clearly $V = \mathrm{H}^0(X_\mu(5), \omega^{\otimes 5}(-2\mathcal{C}))$ is a 2-dimensional G-stable subspace of M_5. It is irreducible because otherwise there would be a G-stable line and hence a copy of the trivial representation, yet the center μ_2 acts on M_5 through negation and hence there is no trivial subrepresentation.

Lemma 4.2 shows that X_a is a modular form of weight 5 on $\Gamma(5)$ for $a = 0, 1$, and (4.5) may be employed to expand X_0, X_1 about each cusp to infer that X_0, X_1 have zeroes along $\mathscr{C}$ with order at least 2. Using (4.6), one finds that X_a has the q-product (C.4) for $a = 0, 1$, and it is clear from these q-expansions that X_0, X_1 are linearly independent. By the q-expansion principle, these elements of $\mathbf{C} \otimes_{\mathbf{Q}} V$ lie in the $\mathbf{Q}$-subspace $V \subseteq M_5$, and hence X_0 and X_1 are a basis of V. ■

Let $\widetilde{\rho} : G \to \mathrm{GL}(V)$ be the representation of G on V; since G has no nontrivial 1-dimensional characters, $\widetilde{\rho}$ is a representation into $\mathrm{SL}(V)$. We have computed that the line bundle $\mathscr{L} = \omega^{\otimes 5}(-2\mathscr{C})$ on $X_\mu(5)$ has degree 1, and since $X_\mu(5)$ is a projective line we therefore conclude that the basis X_0 and X_1 of $V = \mathrm{H}^0(X_\mu(5), \mathscr{L})$ generates $\mathscr{L}$. Thus, the data $(\mathscr{L}; X_0, X_1)$ defines a morphism

$$X_\mu(5) \to \mathbf{P}(V) = \mathbf{P}^1_{\mathbf{Q}}$$

over $\mathbf{Q}$ and this must be an isomorphism; in fact, a check of q-series shows $X_0/X_1 = j_{5,\mu}$, so this isomorphism is exactly the one that is defined by $j_{5,\mu}$. [1] In this way we see that we have lifted the G-action on $X_\mu(5)$ to an action on its homogeneous coordinate ring $\mathbf{Q}[X_0, X_1]$ with respect to the rational parameter $j_{5,\mu}$, and consequently we have lifted ρ to a representation into SL_2. This lift is faithful because $\ker \rho = \mu_2$ acts by negation on ω over the trivial action on $X_\mu(5)$ and so also acts by negation on odd tensor-powers of ω.

For uniqueness of the lift it is enough to work over fields K that split $X^5 - 1$ and to consider liftings of ρ_ζ for $\zeta \in K$ a primitive 5th root of unity. Let S and T be as in Appendix A.[2] Recalling the presentation

$$\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) = \langle S, T \mid T^5 = 1,\ S^2 = (ST)^3 = -1 \rangle,$$

lifting ρ_ζ is equivalent to giving matrices $\widetilde{\rho}_\zeta(S)$ and $\widetilde{\rho}_\zeta(T)$ satisfying the relations $\widetilde{\rho}_\zeta(T)^5 = 1$ and $\widetilde{\rho}_\zeta(S)^2 = (\widetilde{\rho}_\zeta(S)\widetilde{\rho}_\zeta(T))^3 = -1$. In Theorem A.3 we explicitly computed $\rho_\zeta(S), \rho_\zeta(T) \in \mathrm{PGL}_2(K)$. As we require $\widetilde{\rho}_\zeta$ to lift ρ_ζ, we see that our choices are

$$\text{(C.5)} \qquad \widetilde{\rho}_\zeta(T) = \pm \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta^3 \end{pmatrix} \qquad \widetilde{\rho}_\zeta(S) = \pm \frac{1}{\sqrt{5}} \begin{pmatrix} \zeta^{-1} - \zeta & \zeta^{-2} - \zeta^2 \\ \zeta^{-2} - \zeta^2 & \zeta - \zeta^{-1} \end{pmatrix},$$

where we take $\sqrt{5} = \zeta + \zeta^{-1} - \zeta^2 - \zeta^{-2}$. A short computation with the relations reveals that we must select the positive sign in both cases, and that this works (thereby giving a second existence proof that descends to $\mathbf{Q}$ by uniqueness and Galois descent). ■

Put $M_n = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and note that since $(n, 5) = 1$, conjugation by M_n induces an automorphism of G depending only n mod 5. Define the representation

$$\widetilde{\rho}_n : G \hookrightarrow \mathrm{SL}_{2/\mathbf{Q}}$$

on points by the functorial recipe

$$\widetilde{\rho}_n(g) = \widetilde{\rho}(M_n g M_n^{-1}),$$

so in particular we have $\widetilde{\rho}_1 = \widetilde{\rho}$. For an extension $K/\mathbf{Q}$ splitting $X^5 - 1$ and a primitive 5th root of unity $\zeta \in K^\times$, we write $\widetilde{\rho}_{\zeta,n}$ to denote the representation of $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) \simeq G(K)$ into $\mathrm{SL}_2(\mathbf{Q}(\zeta))$ corresponding to $\widetilde{\rho}_{n/K}$.

In §6 we defined the polynomial $F_n(X, Y)$ as the dehomogenization (with respect to (∞, ∞)) of a certain absolutely irreducible bihomogenous polynomial $\widetilde{F}_n(X_0, X_1; Y_0, Y_1)$ whose zero-scheme $Z_{5,n,\mathbf{Q}} \subseteq \mathbf{P}^1_{\mathbf{Q}} \times \mathbf{P}^1_{\mathbf{Q}}$ is the generic fiber of the scheme-theoretic image of the map

$$\overline{\pi}_n \times \overline{\pi}'_n : X(\Gamma_\mu(5), \Gamma_0(n)) \to X_\mu(5) \times_{\mathbf{Z}[1/5]} X_\mu(5)$$

[1] Throughout, Klein works with coordinates ζ_1, ζ_2 satisfying $\zeta_1/\zeta_2 = 1/j_5 = F$ and regards F as a rational parameter on $X(5)$. This convention seems somewhat at odds with the case of $X(1)$, where the classical rational parameter j has a simple pole at the cusp ∞. The function $1/j_5$ in fact has a simple zero at ∞.

[2] We follow the standard conventions; see for example [18, p. 77]. Klein [7] reverses the roles of S and T.

over $\mathbf{Z}[1/5]$. As we noted in the proof of Lemma 6.2, the Kroneckerian model $Z_{5,n}$ over $\mathbf{Z}[1/5]$ as in Definition 6.1 is the scheme-theoretic image of $(\overline{\pi}_n \times \overline{\pi}'_n) \circ \phi$ for any automorphism ϕ of $X(\Gamma_\mu(5), \Gamma_0(N))$.

Lemma C.3. *The action $\rho \times \rho_n$ of G on $X_\mu(5) \times_{\mathbf{Q}} X_\mu(5)$ restricts to an automorphism of $Z_{5,n,\mathbf{Q}}$.*

Proof. It suffices to check this over a field $\mathbf{Q}(\zeta)$ generated by a primitive 5th root of unity ζ, over which we may identify $X_\mu(5)$ with $X_\zeta(5)$ and $X(\Gamma_\mu(5), \Gamma_0(n))$ with $X(\Gamma(5), \Gamma_0(n))_{\mathbf{Q}(\zeta)}$ For any $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, let $\overline{\gamma}$ denote the image of γ under the canonical map $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) = G(\mathbf{Q}(\zeta))$. The diagram

(C.6)
$$\begin{array}{ccc} X(\Gamma(5), \Gamma_0(n))_{\mathbf{Q}(\zeta)} & \xrightarrow{\overline{\pi}_n \times \overline{\pi}'_n} & X_\zeta(5) \times X_\zeta(5) \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle \overline{\gamma} \times M_n \overline{\gamma} M_n^{-1}} \\ X(\Gamma(5), \Gamma_0(n))_{\mathbf{Q}(\zeta)} & \xrightarrow[\overline{\pi}_n \times \overline{\pi}'_n]{} & X_\zeta(5) \times X_\zeta(5) \end{array}$$

is readily seen to commute, where γ and $\overline{\gamma}$ act (away from the cusps) as in (2.2). Thus, the action of $G(\mathbf{Q}(\zeta))$ through $\rho \times \rho_n$ is intertwined with a group action on $X(\Gamma(5), \Gamma_0(n))_{\mathbf{Q}(\zeta)}$ and thus restricts to an action on the scheme-theoretic image $Z_{5,n,\mathbf{Q}}$. ∎

Let $R \subseteq \mathbf{Q}[X_0, X_1] \otimes_{\mathbf{Q}} \mathbf{Q}[Y_0, Y_1]$ be the homogeneous coordinate of $X_\mu(5) \times X_\mu(5)$; that is, it is the $\mathbf{Q}$-subalgebra generated by all bihomogeneous polynomials of bidegree (v, v) for $v \geq 0$. By the preceding lemma, the action of G on R through $\widetilde{\rho} \otimes \widetilde{\rho}_n$ preserves the $\mathbf{Q}$-line spanned by the irreducible generator $\widetilde{F}_n(X_0, X_1; Y_0, Y_1)$ of the ideal of $Z_{5,n,\mathbf{Q}}$. Since G has no 1-dimensional characters, we conclude that $\widetilde{F}_n$ is G-invariant with respect to $\widetilde{\rho} \otimes \widetilde{\rho}_n$.

To ease notation, let $G(n)$ denote G equipped with its action on R through $\widetilde{\rho} \otimes \widetilde{\rho}_n$. Following Klein, we now determine polynomial generators for $R^{G(n)}$ for each $n \in (\mathbf{Z}/5\mathbf{Z})^\times$. Since $\widetilde{F}_n \in R^{G(n)}$, in this way we will be able to *compute* $\widetilde{F}_n$ very efficiently.

Lemma C.4. *There is a map $R^{G(n)} \to R^{G(-n)}$ given by*

(C.7)
$$f(X_0, X_1; Y_0, Y_1) \mapsto f(-X_1, X_0; Y_0, Y_1),$$

and this map is an isomorphism.

By this lemma, it suffices to determine generators for $R^{G(n)}$ when $n \equiv 1, 2 \bmod 5$.

Proof. We may extend scalars to $\mathbf{Q}(\zeta)$ with ζ a primitive 5th root of unity. Let δ_n be the automorphism of $X_\mu(5)$ defined by (6.2). Using the canonical isomorphism $X_\zeta(5)_{\mathbf{Q}(\zeta)} \simeq X_\mu(5)_{\mathbf{Q}(\zeta)}$, a short calculation shows

$$(\delta_2 \times M_n \delta_2^{-1} M_n^{-1}) \circ (g \times M_n g M_n^{-1}) \circ (g \times M_n \delta_2 M_n^{-1}) = g \times M_n \delta_2^{-1} g \delta_2 M_n^{-1} = g \times M_{-n} g M_{-n}^{-1}$$

as automorphisms of $X_\zeta(5) \times X_\zeta(5)$ for any $g \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z}) = G(\mathbf{Q}(\zeta))$, and hence

(C.8)
$$(\widetilde{\rho}_\zeta \otimes \widetilde{\rho}_{\zeta,-n})(g) = (\widetilde{\rho}_\zeta(\delta_2)^{-1} \otimes 1)(\widetilde{\rho}_\zeta \otimes \widetilde{\rho}_{\zeta,n})(g)(\widetilde{\rho}_\zeta(\delta_2) \otimes 1).$$

By Corollary 5.5 we have $\widetilde{\rho}_\zeta(\delta_2) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ up to a sign ambiguity that is easily resolved by the proof of Theorem C.1, so $\widetilde{\rho}_\zeta(\delta_2)$ is self-inverse up to a sign and hence (C.8) provides the desired map. ∎

The case $n \equiv 1 \bmod 5$ is simpler than the case $n \equiv 2 \bmod 5$ because the action $\widetilde{\rho} \times \widetilde{\rho}_n$ is the diagonal action of $\widetilde{\rho} = \widetilde{\rho}_1$ for such n. Thus, we will first work out the case $n \equiv 1 \bmod 5$. Before we can determine the associated ring of invariants $R^{G(1)} = R^G$, we need some terminology and results from clasical invariant theory (*cf.* [12, §7]).

Let $\rho : \Gamma \to \mathrm{GL}(V)$ be an algebraic representation of a finite étale K-group on a finite-dimensional vector space V over a field K of characteristic 0, and let $K[V^*]$ be the symmetric algebra of the dual space V^*. For any positive integer r we let Γ act on $K[V^{*\oplus r}] \simeq K[V^*]^{\otimes r}$ via the action $\rho^{*\otimes r}$, where ρ^* denotes the dual *right* action of Γ on $K[V^*]$. For any $s \geq r$, the linear projection map $\mathrm{pr} : V^{\oplus s} \to V^{\oplus r}$ onto the first r copies of V gives a Γ-equivariant inclusion

$$K[V^{*\oplus r}] \hookrightarrow K[V^{*\oplus s}], \tag{C.9}$$

and in this way we will identify $K[V^{*\oplus r}]$ as a subring of $K[V^{*\oplus s}]$.

Definition C.5. For each i, j with $1 \leq i, j \leq s$, the *polarization* operators $\Delta_{ij} : K[V^{*\oplus s}] \to K[V^{*\oplus s}]$ are the linear maps defined by

$$\Delta_{ij} f(v_1, \dots, v_s) = \left.\frac{f(v_1, \dots, v_j + tv_i \dots, v_s) - f(v_1, \dots, v_s)}{t}\right|_{t=0} \tag{C.10}$$

with $v_j + tv_i$ in the jth component. The K-algebra generated by all Δ_{ij} with $1 \leq i, j \leq s$ will be denoted $\mathcal{U}(s)$.

The importance of the polarization algebra is that it sometimes allows us to construct $K[V^{*\oplus s}]^\Gamma$ from $K[V^{*\oplus r}]^\Gamma$ when $s > r$.

Definition C.6. Let $\dim V = r \leq s$, and for any ordered r-tuple $1 \leq i_1 \leq \ldots \leq i_r \leq s$ of integers let

$$[i_1, \dots, i_r] \in (V^{\oplus s})^* = V^{*\oplus s}$$

be the composition $V^{\oplus s} \to \wedge^r V \xrightarrow{\det} K$, where $V^{\oplus s} \to \wedge^r V$ is given by

$$(v_1, \dots, v_s) \mapsto v_{i_1} \wedge v_{i_2} \wedge \ldots \wedge v_{i_r}.$$

Observe that $[i_1, \dots, i_r]$ is $\mathrm{SL}(V)$ invariant.

Theorem C.7. *Let $r = \dim V$ and suppose that Γ acts on V through $\mathrm{SL}(V)$. Let $S \subset K[V^{*\oplus(r-1)}]^\Gamma$ be a subset that generates $K[V^{*\oplus(r-1)}]^\Gamma$ as a K-algebra. Identify $K[V^{*\oplus(r-1)}]^\Gamma$ as a subring of $K[V^{*\oplus s}]^\Gamma$ as in (C.9).*

For any $s \geq r$, $K[V^{*\oplus s}]^\Gamma$ is generated as a K-algebra by the union of the set of all elements $[i_1, \dots, i_r] \in K[V^{*s}]$ and the set $\mathcal{U}(s)(S)$ obtained by applying all polarization operators in $\mathcal{U}(s)$ to S.

Proof. It suffices to prove the result after extending the ground field K, and so we may suppose that the finite étale K-group Γ is an ordinary finite group. This case is [12, Cor. 1, §7.5]. ∎

Returning to our original situation of interest, we wish to compute $\mathbf{Q}$-algebra generators for the invariants $R^{G(1)} \subseteq \mathbf{Q}[X_0, X_1; Y_0, Y_1]^{G(1)}$ in the $\mathbf{Q}$-subalgebra R generated by bihomogeneous polynomials of bidegree (v, v) for $v \geq 0$. We first use Theorem C.7 with $\Gamma = \widetilde{\rho}(G)$ and $s = r = 2$ to compute $\mathbf{Q}$-algebra generators of $\mathbf{Q}[X_0, X_1; Y_0, Y_1]^{G(1)}$ by computing $\mathbf{Q}$-algebra generators of $\mathbf{Q}[X_0, X_1]^G$.

We will prove the following classical theorem, formulated to work over $\mathbf{Q}$ and not just over $\mathbf{C}$:

Theorem C.8. *Let*

$$\begin{aligned}
\Phi_{12} &= X_0X_1(X_0^{10} + 11X_0^5X_1^5 - X_1^{10})\\
\Phi_{20} &= -(X_0^{20} + X_1^{20}) + 228(X_0^{15}X_1^5 - X_1^{15}X_0^5) - 494X_0^{10}X_1^{10}\\
\Phi_{30} &= (X_0^{30} + X_1^{30}) + 522(X_1^{25}X_0^5 - X_0^{25}X_1^5) - 10005(X_0^{20}X_1^{10} + X_1^{20}X_0^{10}).
\end{aligned}$$

Then $\mathbf{Q}[X_0, X_1]^G$ is generated over $\mathbf{Q}$ by $\Phi_{12}, \Phi_{20}, \Phi_{30}$, which satisfy the relation

$$1728\Phi_{12}^5 - \Phi_{20}^3 - \Phi_{30}^2 = 0. \tag{C.11}$$

Moreover, if T is the graded polynomial ring $\mathbf{Q}[U_{12}, U_{20}, U_{30}]$ where U_i is given degree i then the kernel of the surjective graded $\mathbf{Q}$-algebra homomorphism $\alpha : T \twoheadrightarrow \mathbf{Q}[X_0, X_1]^G$ given by $\alpha : U_i \mapsto \Phi_i$ is a principal ideal, generated by $1728U_{12}^5 - U_{20}^3 - U_{30}^2$.

Proof. Let $f \in \mathbf{Q}[X_0, X_1]^G$ be any nonzero homogeneous polynomial. The closed subscheme $Z = V(f) \subseteq X_\mu(5)$ is G-stable and is therefore topologically a finite union G-orbits. Conversely, any finite union of G-orbits defines a G-stable closed subscheme of $X_\mu(5)$ that is the zero-scheme of a nonzero radical homogeneous polynomial f that is unique up to unit-scaling and hence the line $\mathbf{Q} \cdot f$ supports a 1-dimensional algebraic representation of G; the only such representation is the trivial one, so such f must be G-invariant.

Now the map $j : X_\mu(5) \to \mathbf{P}^1_{\mathbf{Q}}$ is a degree-60 covering branched only over $j = 0$, $j = \infty$ and $j = 1728$, and it is generically a torsor for the generically-free action of the quotient $\rho(G) = G/\mu_2$ of G by its center. In particular, over $\mathbf{Q}(\zeta_5)$ this becomes a Galois covering with Galois group $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})/\{\pm 1\} \simeq A_5$. By identifying $X_\mu(5)$ with $X_\zeta(5)$ over $\mathbf{Q}(\zeta)$ we see that $j^{-1}(0)$ consists of 20 (geometrical) points with ramification index 3, $j^{-1}(\infty)$ consists of the 12 (geometrical) cusps with ramification index 5, and $j^{-1}(1728)$ has 30 (geometrical) points with ramification index 2. For any field K of characteristic 0 and any $t \in \mathbf{P}^1(K)$, $j^{-1}(t)$ is a G-orbit on $X_\mu(5)_{/K}$. We write ϕ_t to denote the associated nonzero radical G-invariant homogeneous polynomial in $K[X_0, X_1]$ (so ϕ_t is well-defined modulo $K^\times$). (Klein [11, p. 50] calls the ϕ_t *ground forms*). We claim that the ring $\mathbf{Q}[X_0, X_1]^G$ is generated by ϕ_0, ϕ_∞, and ϕ_{1728}.

It suffices to work over $K = \overline{\mathbf{Q}}$, and by working over this K we may identify every G-orbit in $X_\mu(5)(K)$ as $j^{-1}(t)$ for a unique $t \in \mathbf{P}^1(K)$. If $\phi \in (K \otimes_{\mathbf{Q}} R)^G$ is nonzero then its K-finite zero-scheme $V(\phi)$ on $X_\mu(5)_{/K}$ is a union of orbits and hence ϕ is a product of factors that are G-stable up to $K^\times$-multiple and hence are G-stable (as G has no non-trivial 1-dimensional characters). Thus, we may suppose that the zero-scheme of ϕ is topologically a G-orbit, so $V(\phi) = j^{-1}(t)$ topologically for some $t \in \mathbf{P}^1(K)$. By G-invariance, it follows that ϕ has zeros of equal order at all points of $V(\phi)$ and hence ϕ is a scalar multiple of a power of the radical ϕ_t whose degree is equal to the size of $j^{-1}(t)$. We therefore may restrict our attention to the ϕ_t's.

Suppose that $t \notin \{0, \infty, 1728\}$, pick $v \in j^{-1}(t)$, and consider the polynomial

$$\phi := \phi_\infty^5(v)\phi_0^3 - \phi_0^3(v)\phi_\infty^5.$$

By construction, ϕ is a G-invariant homogeneous polynomial of degree $60 = |G|/2$ vanishing at v, and hence it vanishes on the G-orbit $j^{-1}(t)$ of v. This orbit has $|G|/2$ distinct geometrical points, so ϕ is a scalar multiple of ϕ_t. This shows that all ϕ_t lie in the subalgebra generated by ϕ_0, ϕ_{1728}, and ϕ_∞.

Since G is finite, $\mathbf{Q}[X_0, X_1]$ is a finite $\mathbf{Q}[X_0, X_1]^G$-module, so both rings have Krull dimension 2. Moreover, $\mathbf{Q}[X_0, X_1]^G$ is a domain and hence $\ker \alpha$ is a prime ideal which (by dimension considerations) must have height 1. But T is a polynomial ring, hence a UFD, so every height-1 prime is principal. Thus, up to $\mathbf{Q}^\times$-multiple there is a unique irreducible algebraic relation among U_{12}, U_{20}, and U_{30} over $\mathbf{Q}$ that is contained in $\ker \alpha$ and it must generate $\ker \alpha$. The same holds when $\mathbf{Q}$ is replaced with any field of characteristic 0. The preceding considerations apply with $t = 1728$ and thereby provide an algebraic relation

$$\phi_{1728}^2 = \phi_\infty^5(v)\phi_0^3 - \phi_0^3(v)\phi_\infty^5 \tag{C.12}$$

over $\overline{\mathbf{Q}}$ for any $v \in j^{-1}(1728)$; the coefficients $\phi_\infty(v), \phi_0(v)$ cannot both vanish (as $\phi_{1728} \neq 0$), so this is an irreducible algebraic relation over $\overline{\mathbf{Q}}$. The monicity in ϕ_{1728}^2 and the uniqueness of the irreducible relation up to $\overline{\mathbf{Q}}^\times$-multiple forces the relation (C.12) to have coefficients in $\mathbf{Q}$.

It remains to compute ϕ_0, ϕ_∞, and ϕ_{1728} explicitly (up to $\mathbf{Q}^\times$-multiple) and to find the explicit coefficients in (C.12) upon making specific choices of ϕ_0, ϕ_∞, and ϕ_{1728}. In Table B.1, we computed the values of j_5 on the geometrical cusps $j^{-1}(\infty)$. As G acts transitively on the geometrical cusps of $X_\mu(5)$ we can immediately write down the degree-12 G-invariant polynomial

$$\Phi_{12} := X_0 X_1 \prod_{c \in j^{-1}(\infty) - \{\infty, 0\}} (X_0 - X_1 j_5(c)) = X_0 X_1 (X_0^{10} + 11 X_0^5 X_1^5 - X_1^{10}),$$

which by construction must be (a $\mathbf{Q}^\times$-multiple of) ϕ_∞. The coordinate-free theory of the Hessian ensures that the *Hessian determinant*

$$H(\Phi_{12}) = \begin{vmatrix} \partial^2\Phi_{12}/\partial X_0^2 & \partial^2\Phi_{12}/\partial X_0\partial X_1 \\ \partial^2\Phi_{12}/\partial X_1\partial X_0 & \partial^2\Phi_{12}/\partial X_1^2 \end{vmatrix}$$

is G-invariant (more specifically, by [11, pp. 56–62] this is a *covariant* of Φ_{12} of degree $2(12-2)=20$), so

$$\Phi_{20} := \frac{1}{121}H(\Phi_{12}) = -(X_0^{20}+X_1^{20}) + 228(X_0^{15}X_1^5 - X_1^{15}X_0^5) - 494X_0^{10}X_1^{10}$$

is a degree-20 invariant polynomial. As there is a unique G-orbit of degree 20 on $X_\mu(5)$, namely $j^{-1}(0)$, we conclude that Φ_{20} is a $\mathbf{Q}^\times$-multiple of ϕ_0. Similarly, the differential determinant

$$\begin{aligned}\Phi_{30} &:= -\frac{1}{20}\begin{vmatrix} \partial\Phi_{12}/\partial X_0 & \partial\Phi_{12}/\partial X_1 \\ \partial\Phi_{20}/\partial X_1 & \partial\Phi_{20}/\partial X_1 \end{vmatrix} \\ &= (X_0^{30}+X_1^{30}) + 522(X_1^{25}X_0^5 - X_0^{25}X_1^5) - 10005(X_0^{20}X_1^{10} + X_1^{20}X_0^{10})\end{aligned}$$

of degree $3(12-2)=30$ must be a G-invariant polynomial, and must therefore coincide with a $\mathbf{Q}^\times$-multiple of ϕ_{1728} because there is a unique G-orbit of degree 30, and 30 cannot be written as a sum of positive integral multiples of 12 and 20.

We may now rephrase (C.12) as an algebraic relation

$$a\Phi_{12}^5 - b\Phi_{20}^3 - \Phi_{30}^2 = 0$$

for some unique $a, b \in \mathbf{Q}$ not both zero. Using (C.4) and the definitions of the Φ's in terms of X_0 and X_1, comparison of a few q-series coefficients allows us to solve for a and b to obtain the relation (C.11). ∎

Before we proceed further with our computation of $R^{G(n)}$, let us use (C.4) to identify $\Phi_{12}, \Phi_{20}, \Phi_{30}$ as modular forms for $\mathrm{SL}_2(\mathbf{Z})$. By (C.4) we may identify the coordinates X_0 and X_1 with weight-5 modular forms for $\Gamma(5)$, so Φ_{12}, Φ_{20}, and Φ_{30} are modular forms for $\Gamma(5)$ with weights $60, 100, 150$ respectively; the $G(\mathbf{C})$-invariance implies that these are in fact modular forms of full level 1. By comparing q-expansions, we thereby easily find

$$\Phi_{12} = -\Delta^5 = -q^5 + 120q^6 - 7020q^7 + \cdots \tag{C.13}$$

$$\Phi_{20} = \Delta^8 E_2 = q^8 + 48q^9 - 25776q^{10} + \cdots \tag{C.14}$$

$$\Phi_{30} = \Delta^{12} E_3 = q^{12} - 792q^{13} + 169560q^{14} + \cdots \tag{C.15}$$

where

$$\Delta = q\prod_{k=1}^\infty (1-q^k)^{24}, \qquad E_2 = 1 + 240\sum_{k=1}^\infty \frac{k^3q^k}{1-q^k}, \qquad E_3 = 1 - 504\sum_{k=1}^\infty \frac{k^5q^k}{1-q^k}.$$

From these identifications, we immediately see that $j = E_2^3/\Delta = \Phi_{20}^3/\Phi_{12}^5$. As we have the identification $j_5 = X_0/X_1$, we use Theorem C.8 to find

$$j = \frac{1}{j_5^5}\cdot\frac{\left(j_5^{20} - 228j_5^{15} + 494j_5^{10} + 228j_5^5 + 1\right)^3}{\left(j_5^{10} - 11j_5^5 - 1\right)^5}. \tag{C.16}$$

This "icosahedral equation" was of course well-known to Klein [11, pp. 60–66].

Returning now to the determination of $R^{G(n)}$ for $n \equiv 1 \bmod 5$, we know from Theorem C.7 that $\mathbf{Q}[X_0, X_1; Y_0, Y_1]^{G(1)}$ is generated by the determinant $[1, 2]$ as in Theorem C.7 and all polarizations of Φ_{12}, Φ_{20}, and Φ_{30}. Define

$$A_1 := \alpha_1[1, 2],$$

and for $i = 6, 10, 15$ put

$$A_i := \alpha_i \Delta_{12}^i \Phi_{2i} \tag{C.17}$$

where $\alpha_i \in \mathbf{Q}^\times$ is chosen so as to make A_i primitive (with an arbitrary choice of sign) for $i \in \{1, 6, 10, 15\}$. After a short calculation with the explicit formula (C.10) (and an arbitrary choice of sign), we find

$$\begin{aligned}
A_1 &= X_0Y_1 - Y_0X_1 \\
A_6 &= 42(X_0Y_1 + Y_0X_1)(X_1^5Y_1^5 - X_0^5Y_0^5) + X_0^6Y_1^6 + Y_0^6X_1^6 + 36X_0Y_0X_1Y_1(X_0^4Y_1^4 + Y_0^4X_1^4) \\
&\quad + 225X_0^2Y_0^2X_1^2Y_1^2(X_0^2Y_1^2 + Y_0^2X_1^2) + 400X_0^3Y_0^3X_1^3Y_1^3 \\
A_{10} &= 374(X_1^{10}Y_1^{10} + X_0^{10}Y_0^{10}) - 66(X_1^5Y_1^5 - X_0^5Y_0^5)(21(X_0^5Y_1^5 + Y_0^5X_1^5) + 175X_0Y_0X_1Y_1(X_0^3Y_1^3 + Y_0^3X_1^3) \\
&\quad + 450X_0^2Y_0^2X_1^2Y_1^2(X_0Y_1 + Y_0X_1)) + (X_0^{10}Y_1^{10} + Y_0^{10}X_1^{10}) + 100X_0Y_0X_1Y_1(X_0^8Y_1^8 + Y_0^8X_1^8) \\
&\quad + 2025X_0^2Y_0^2X_1^2Y_1^2(X_0^6Y_1^6 + Y_0^6X_1^6) + 14400X_0^3Y_0^3X_1^3Y_1^3(X_0^4Y_1^4 + Y_0^4X_1^4) \\
&\quad + 44100X_0^4Y_0^4X_1^4Y_1^4(X_0^2Y_1^2 + Y_0^2X_1^2) + 63504X_0^5Y_0^5X_1^5Y_1^5 \\
A_{15} &= X_0^{15}Y_0^{15} + Y_1^{15}X_1^{15} + (X_1^{10}Y_1^{10} - Y_0^{10}X_0^{10})(11(X_0^5Y_1^5 + Y_0^5X_1^5) + 75X_0Y_0X_1Y_1(X_0^3Y_1^3 + Y_0^3X_1^3) \\
&\quad + 175X_0^2Y_0^2X_1^2Y_1^2(X_0Y_1 + Y_0X_1)) - (X_0^5Y_0^5 + Y_1^5X_1^5)(X_0^{10}Y_1^{10} + Y_0^{10}X_1^{10} \\
&\quad + 25X_0Y_0X_1Y_1(X_0^8Y_1^8 + Y_0^8X_1^8) + 225X_0^2Y_0^2X_1^2Y_1^2(X_0^6Y_1^6 + Y_0^6X_1^6) + 975X_0^3Y_0^3X_1^3Y_1^3(X_0^4Y_1^4 + Y_0^4X_1^4) \\
&\quad + 2275X_0^4Y_0^4X_1^4Y_1^4(X_0^2Y_1^2 + Y_0^2X_1^2) + 3003X_0^5Y_0^5X_1^5Y_1^5).
\end{aligned}$$

Observe that each A_i is bihomogenous and G-invariant. Thus, the ring $S := \mathbf{Q}[A_1, A_6, A_{10}, A_{15}]$ is a subring of R^G. We claim that $S = R^G$. If not, we may choose (a possibly non-unique) $f \in R^G - S$ of minimal positive bihomogeneous degree (d_0, d_0). The $G(1)$-equivariant linear map $V \to V^{\oplus 2}$ given by $v \mapsto (v, v)$ defines a $\mathbf{Q}$-algebra homomorphism $L : \mathbf{Q}[V^{*\oplus 2}]^{G(1)} \to \mathbf{Q}[V^*]^{G(1)}$ and we use Theorem C.8 to write $L(f) = P(\Phi_{12}, \Phi_{20}, \Phi_{30})$ for some polynomial P with $\mathbf{Q}$-coefficients. One checks easily from the definitions of the polarization operators (C.10) and the polynomials A_i for $i \in \{1, 6, 10, 15\}$ (C.17) that

$$L(A_i) = \begin{cases} 0 & \text{if } i = 1 \\ \beta_i \Phi_{2i} & \text{otherwise} \end{cases},$$

for some $\beta_i \in \mathbf{Q}^\times$. Letting

$$g = f - P\left(A_6/\beta_6, A_{10}/\beta_{10}, A_{15}/\beta_{15}\right),$$

it follows that $L(g) = 0$ so the polynomial g vanishes on the zero-set of A_1. As A_1 is absolutely irreducible, we conclude that $A_1|g$ so we have

$$f = A_1 f_1 + P\left(A_6/\beta_6, A_{10}/\beta_{10}, A_{15}/\beta_{15}\right),$$

where f_1 is evidently a bihomogeneous $G(1)$-invariant polynomial of bidegree $(d_0 - 1, d_0 - 1)$, hence a polynomial in the A_i for $i \in \{1, 6, 10, 15\}$ by our minimality assumption on d_0. It follows that $f \in S$ afterall, and that the polynomials A_i for $i \in \{1, 6, 10, 15\}$ generate $R^{G(n)}$ as a $\mathbf{Q}$-algebra for $n \equiv 1 \bmod 5$.

Observe that A_{15}, A_{10}, and A_6 are uniquely determined as homogeneous generators of $R^{G(1)}$ *only modulo* A_1. As Klein [11, p. 242] observes, A_6, A_{10}, and A_{15} do not have particularly nice geometric interpretations, and as a consequence, when $n \equiv 1 \bmod 5$ the formulae for $\widetilde{F}_n$ in terms of A_1, A_6, A_{10}, and A_{15} are somewhat messy and involve rather large coefficients. Following Klein, we choose more convenient generators by defining[3]

$$\begin{aligned} W_2 &= A_1^2 \\ W_6 &= \frac{-A_6 + A_1^6}{42} \\ W_{10} &= \frac{A_{10} - A_1^{10} + 110A_1^4 W_6}{374} \\ W_{15} &= A_{15}. \end{aligned} \tag{C.18}$$

It is immediate from these definitions that $R^{G(1)} = \mathbf{Q}[A_1, W_6, W_{10}, W_{15}]$. By Lemma 6.2(2), we know that for $n \equiv \pm 1 \bmod 5$ the modular polynomial $\widetilde{F}_n$ satisfies $\widetilde{F}_n(X_0, X_1; Y_0, Y_1) = \widetilde{F}_n(Y_0, Y_1; X_0, X_1)$. Observe that this transformation $h(X_0, X_1; Y_0, Y_1) \mapsto h(Y_0, Y_1; X_0, X_1)$ that preserves $\widetilde{F}_n$ also preserves W_6, W_{10}, W_{15} but sends A_1 to $-A_1$. We conclude that $\widetilde{F}_n$ is a polynomial in $W_2 = A_1^2$, W_6, W_{10}, W_{15}. Such an expression for $\widetilde{F}_n$ is not unique, as the relation (C.11) gives rise to a relation among the W_i:

$$16W_{15}^2 = W_2^5 W_{10}^2 - 10W_2^4 W_6^2 W_{10} + 25W_2^3 W_6^4 - 40W_2^2 W_6 W_{10}^2 + 360W_2 W_6^3 W_{10} - 864W_6^5 + 16W_{10}^3. \tag{C.19}$$

However, since $n \equiv 1 \bmod 5$, so in particular $n > 2$, it follows that $\deg \pi_n = n\prod_{p|n}(1 + 1/p)$ is even and hence every homogeneous component of $\widetilde{F}_n$ is bihomogeneous with *even* bidegree. Since W_2, W_6, W_{10} are bihomogeneous of even bidegree and W_{15} is bihomogeneous of *odd* bidegree, $\widetilde{F}_n$ is in fact a polynomial in W_2, W_6, W_{10} and W_{15}^2. Thus, (C.19) shows that $\widetilde{F}_n$ is a polynomial in W_2, W_6, W_{10}. We claim that such a representation is *unique*. Indeed, the ring R is 3-dimensional (as it is the Segre product of $\mathbf{Q}[X_0, X_1]$ and $\mathbf{Q}[Y_0, Y_1]$) and since $G(1)$ is finite, $R^{G(1)}$ also has dimension 3. As $R^{G(1)}$ is generated as a $\mathbf{Q}$-algebra by A_1, W_6, W_{10}, W_{15} and we have the relation (C.19), we conclude that A_1, W_6, W_{10} are algebraically independent, so $W_2 = A_1^2$, W_6, W_{10} must be algebraically independent.

We next compute the ring of invariants $R^{G(n)}$ when $n \equiv 2 \bmod 5$ and use it to analyze the element $\widetilde{F}_n$ for such n. As the action $\widetilde{\rho} \otimes \widetilde{\rho}_n$ of G on $R \subseteq \mathbf{Q}[X_0, X_1, Y_0, Y_1]$ is not the same on each set of variables X_0, X_1 and Y_0, Y_1, the polarization method used to treat the case of $n \equiv 1 \bmod 5$ is not available. Following Klein [7, pp. 139–141], we will explicitly construct generators for $R^{G(n)}$.

We have seen that the modular polynomials $\widetilde{F}_n$ are contained in the $\mathbf{N}_0$-graded subring

$$R \subseteq \mathbf{Q}[X_0, X_1] \otimes \mathbf{Q}[Y_0, Y_1]$$

whose vth graded piece R_v is the $\mathbf{Q}$-vector space of bihomogeneous polynomials of bidegree (v, v). Moreover, it is clear that R is generated as a $\mathbf{Q}$-algebra by R_1. Let V_X and V_Y be the representation spaces underlying $\widetilde{\rho}$ and $\widetilde{\rho}_n$, and identify $\mathbf{Q}[V_X^* \otimes V_Y^*]$ with the polynomial ring $\mathbf{Q}[y_1, y_2, y_3, y_4]$ via

$$y_1 \mapsto X_0 Y_0 \qquad y_2 \mapsto X_1 Y_0 \qquad y_3 \mapsto -X_0 Y_1 \qquad y_4 \mapsto X_1 Y_1. \tag{C.20}$$

Observe that this gives a G-equivariant isomorphism $\mathbf{Q}[y_1, y_2, y_3, y_4]/(y_1 y_4 + y_2 y_3) \simeq R$ as graded rings. Geometrically, this is simply the Segre embedding $\mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^3$.

Since $\mu_2 \subseteq G$ acts trivially on each y_i, the representation $G \to \mathrm{SL}(V_X \otimes V_Y)$ factors through G/μ_2. We claim that the representation $V_X \otimes V_Y$ is geometrically irreducible. We may pass to an algebraically closed ground field K, so G/μ_2 is identified with A_5. Since the irreducible representations of A_5 have dimensions $1, 3, 3, 4, 5$, geometrically $V_X \otimes V_Y$ is either irreducible or it decomposes as the direct sum of the trivial

[3] In Klein's notation [11, p. 242], we have taken $W_6 = B/2$, $W_{10} = C$, and $W_{15} = D$. We have decided to depart from Klein's conventions in order to obtain more compact formulae and to ensure that our generators of $R^{G(1)}$ are polynomials in X_0 and X_1 with integer coefficients.

representation with one of the three-dimensional representations or as the direct sum of four copies of the trivial representation. As $n \equiv 2 \bmod 5$, a simple calculation shows that

$$M_n T M_n^{-1} = T^2,$$

so using the explicit description (C.5) of $\widetilde{\rho}_\zeta$ for a primitive 5th root of unity $\zeta \in K$ and using the definition of $\widetilde{\rho}_{\zeta,n}$ we calculate that $T \in \mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ carries y_i to $\zeta^i y_i$ and hence the character of $V_X \otimes V_Y$ takes the value $\zeta + \zeta^2 + \zeta^{-2} + \zeta^{-1} = -1$ on the conjugacy class of the order-5 element T. The character table for A_5 then rules out the possibility that $V_X \otimes V_Y$ has the trivial representation as a direct summand, and this gives our claim. Thus, $V_X \otimes V_Y$ is a $\mathbf{Q}$-model for the unique (absolutely) irreducible 4-dimensional representation of A_5; that is, just as G/μ_2 is an étale twisted form of A_5, $V_X \otimes V_Y$ is an étale twisted form of the A_5-stable subspace of those vectors of trace 0 inside the standard 5-dimensional permutation representation of A_5.

Consider the transformations

(C.21) $$i_1 : h(X_0, X_1; Y_0, Y_1) \mapsto h(-Y_1, Y_0; X_0, X_1)$$

(C.22) $$i_2 : h(X_0, X_1; Y_0, Y_1) \mapsto h(Y_0, Y_1; -X_1, X_0)$$

on R.

Lemma C.9. *For any $n \equiv 2 \bmod 5$ we have $\widetilde{F}_n \circ i_1 = \widetilde{F}_n$ and $\widetilde{F}_n \circ i_2 = \widetilde{F}_n$ if $n > 2$, while $\widetilde{F}_2 \circ i_2 = -\widetilde{F}_2$.*

The sign for i_2 should be compared with the delicate symmetry for the dehomogenized polynomial F_n in Theorem 6.5.

Proof. We may and do extend scalars to a field K that splits $X^5 - 1$ and we choose a primitive 5th root of unity $\zeta \in K$, so we thereby identify G with $\mathrm{SL}_2(\mathbf{Z}/5\mathbf{Z})$ and G/μ_2 with A_5. As was explained above, we may (non-canonically) identify $V_X \otimes V_Y$ with the hyperplane $\sum z_j = 0$ in the 5-dimensional standard representation W for A_5 that we endow with coordinate functions $z_1, \ldots, z_5$.

We let G act on $K[W^*]$ via the standard A_5-action that permutes the z_j's, so we have a G-equivariant graded ring homomorphism

(C.23) $$\varphi : K[y_1, y_2, y_3, y_4]/(y_1 y_4 + y_2 y_3) \longrightarrow K[z_1, z_2, z_3, z_4, z_5]/(z_1 + z_2 + z_3 + z_4 + z_5)$$

given explicitly as in [7, p. 140] by

(C.24) $$\varphi(y_j) = \frac{1}{5} \sum_{k=1}^{5} \zeta^{-kj} z_k.$$

As this is a graded homomorphism and the y_i's satisfy a nontrivial G-invariant quadratic relation, the z_i's must also satisfy a nontrivial G-invariant quadratic relation. Since the G-invariant quadratic polynomials in the z_i's are precisely the K-span of s_1^2 and s_2 with

(C.25) $$s_j := \sum_{k=1}^{5} z_k^j,$$

we must have that $s_2 = 0$. Letting $B := K[z_1, z_2, z_3, z_4, z_5]/(s_1, s_2)$, it follows that (C.24) descends to a G-equivariant isomorphism

(C.26) $$\varphi : K[y_1, y_2, y_3, y_4]/(y_1 y_4 + y_2 y_3) \xrightarrow{\sim} B$$

and hence an isomorphism $(K \otimes_{\mathbf{Q}} R)^{G(n)} \simeq B^G$.

The K-algebra of invariants B^G is generated by the images of generators of $K[z_1, z_2, z_3, z_4, z_5]^G$; that is, B^G is generated by the images of the power sums (C.25) for $1 \leq j \leq 5$ and the discriminant $\Delta := \prod_{i<j}(z_i - z_j)$. The transformations i_1 and i_2 correspond to the automorphisms $\sigma \circ (1 \times [\delta_3])$ and $\sigma \circ ([\delta_3] \times 1)$ of $X_\zeta(5) \times X_\zeta(5)$ occurring in Lemma 6.2. Since

$$\sigma \circ ([\delta_3] \times 1) = \sigma \circ (1 \times [\delta_3]) \circ \delta_2 \times \delta_2,$$

it follows from Lemma 6.2(2) and the commutative diagram (C.6) with $\gamma = \delta_2$ that

$$\widetilde{F}_n \circ i_j = \pm \widetilde{F}_n$$

for $j = 1, 2$; the sign may depend on j, n. It remains to determine the sign.

Observe that $i_1(y_i) = y_{3i}$, and thus, as one computes, $i_1(z_i) = z_{2i}$ for $1 \le i \le 5$ (where the indices are taken modulo 5). This is an *odd* permutation of the z_j, so $i_1(s) = s$ for any symmetric function s in $z_1, \dots, z_5$, while $i_1(\Delta) = -\Delta$.

Since Δ^2 is a polynomial in the z_j, we may write the image of $\widetilde{F}_n$ in B as $u + v\Delta$ where u, v are symmetric in the z_i. Thus, the image of $\widetilde{F}_n \circ i_1$ in B is then $u - v\Delta$, so $u + v\Delta = \pm(u - v\Delta)$, whence either $u = 0$ or $v = 0$ (depending on whether the sign is -1 or $+1$ respectively). In the former case, $\widetilde{F}_n$ is reducible, which is a contradiction. Thus, $v = 0$ and the image of $\widetilde{F}_n = \widetilde{F}_n \circ i_1$ in B is a polynomial in the symmetric functions s_3, s_4, s_5 of the z_i. For $3 \le j \le 5$ we define $W_j \in K[y_1, y_2, y_3, y_4]$ by

$$W_j := \alpha_j \varphi^{-1}(s_j),$$

with $\alpha_j \in \mathbf{Q}^\times$ chosen (with arbitrary sign) so as to make W_j primitive. Since no nonzero polynomial relation holds between the s_j's, we conclude that $\widetilde{F}_n$ is *uniquely* a $\mathbf{Q}$-polynomial in W_3, W_4, W_5.

The W_j's may be written as polynomials in the X_i, Y_i by using (C.20). Using the explicit description of the isomorphism φ as in (C.24), we compute

$$W_3 = -X_0^3Y_0^2Y_1 + X_0^2X_1Y_1^3 + X_0X_1^2Y_0^3 + X_1^3Y_0Y_1^2$$
$$W_4 = -X_0^4Y_0Y_1^3 + X_0^3X_1Y_0^4 - 3X_0^2X_1^2Y_0^2Y_1^2 - X_0X_1^3Y_1^4 + X_1^4Y_0^3Y_1$$
$$W_5 = X_0^5Y_0^5 - X_0^5Y_1^5 + 10X_0^4X_1Y_0^3Y_1^2 + 10X_0^3X_1^2Y_0Y_1^4 + 10X_0^2X_1^3Y_0^4Y_1 - 10X_0X_1^4Y_0^2Y_1^3 + X_1^5Y_0^5 + X_1^5Y_1^5.$$

Note that $i_2(W_j) = (-1)^j W_j$ for $j = 3, 4, 5$. As $\widetilde{F}_n$ is bihomogeneous of even bidegree for $n > 2$, every monomial term $W_3^a W_4^b W_5^c$ must have $3a + 4b + 5c \equiv a + b \equiv 0 \bmod 2$. This shows that $\widetilde{F}_n \circ i_2 = \widetilde{F}_n$ for $n > 2$, and by degree considerations we evidently must have $\widetilde{F}_2 = W_3$ (up to $\mathbf{Q}^\times$-scaling), so $\widetilde{F}_2 \circ i_2 = -\widetilde{F}_2$. ■

Remark C.10. Observe that the preceding argument would not have worked to compute the ring of invariants $R^{G(1)}$, as in this case the 4-dimensional representation V of G/μ_2 that we obtain is reducible, being the sum of the trivial representation and a 3-dimensional representation, as one easily sees over an algebraically closed field by computing the character values.

Remark C.11. We have taken the power sums $s_3, s_4, s_5 \in B$ in the z_i as generators of the ring of invariants B^G and used the isomorphism (C.24) to define polynomials W_3, W_4, W_5 in X_0, X_1, Y_0, Y_1. One might decide instead to use the *elementary* symmetric functions e_3, e_4, e_5 in the z_i instead of the power sums s_3, s_4, s_5 to generate the ring B^G. However, because of Newton's formula

$$(-1)^{n+1} e_n - s_n = \sum_{j=1}^{n-1} (-1)^j e_j s_{n-j} = 0$$

and the fact that $s_1 = s_2 = e_1 = e_2 = 0$ in B, we see that s_j is a $\mathbf{Q}^\times$-multiple of e_j for $1 \le j \le 5$, so we conclude that the formulae for W_3, W_4, W_5 (up to sign) do not depend on whether one chooses the power sums or the elementary symmetric functions as generators for the algebra B^G.

Recall that we have an isomorphism $R^{G(n)} \simeq R^{G(-n)}$ as in (C.7) given by

$$f(X_0, X_1; Y_0, Y_1) \mapsto f(-X_1, X_0; Y_0, Y_1).$$

For $i = 2, 3, 4, 5, 6, 10, 15$ define

$$Z_i(X_0, X_1; Y_0, Y_1) = W_i(-X_1, X_0; Y_0, Y_1);$$

the W_i's were all defined in the proof of Lemma C.9 and the discussion following the proof of Theorem C.8. We have now proved the following theorem:

Theorem C.12. *Let $n > 1$ be any integer with $(n,5) = 1$ and let W_i and Z_i be as above. Then $\widetilde{F}_n$ is uniquely a* **Q***-polynomial in:*

$$\begin{cases} W_2, W_6, W_{10} & \text{if } n \equiv 1 \bmod 5 \\ W_3, W_4, W_5 & \text{if } n \equiv 2 \bmod 5 \\ Z_3, Z_4, Z_5 & \text{if } n \equiv 3 \bmod 5 \\ Z_2, Z_6, Z_{10} & \text{if } n \equiv 4 \bmod 5 \end{cases} \tag{C.27}$$

The point is that uniqueness is inherited under extension on the ground field and also descends through such extensions, so it suffices to work over an extension of **Q**. Upon introducing a primitive 5th root of unity, we can apply all preceding considerations (including the ones in the proof of Lemma C.9).

Computing F_n for any given n relatively prime to 5 is now a matter of simple linear algebra. We know that $\widetilde{F}_n$ can be written as a **Q**-linear combination of certain monomials in the W_i, Z_j. Knowledge of the common X- and Y-degrees of F_n and the W_i, Z_j enables us to predict exactly which monomials can occur. Using the identification (C.4) of X_0, X_1 with weight-5 modular forms for $\Gamma(5)$ and hence of Y_0, Y_1 with weight-5 modular forms for $\Gamma(5) \cap \Gamma_0(n)$, we may compute the q-expansions of the modular forms W_i, Z_j. By computing enough terms, we are guaranteed to find a unique relation (up to $\mathbf{Q}^\times$-scaling) in the expected degrees, and this must be $\widetilde{F}_n$ (up to $\mathbf{Q}^\times$-scaling). One can even specify how many q-series terms are sufficient: indeed, with the identifications above, $\widetilde{F}_n$ is a modular form for $\mathrm{SL}_2(\mathbf{Z})$ of weight $k := 5n\prod_{p|n}(1+1/p)$, so we need only check the q-expansion to order $\lfloor k/12 \rfloor$.

Let us illustrate this with an example.

Example C.13. Let $n = 8$. From Table C.1, we see that $\widetilde{F}_8$ is an element of $\mathbf{Q}[Z_3, Z_4, Z_5]$. As F_8 has common X- and Y-degree $2^2 \cdot 3 = 12$, the only monomials that can occur are

$$Z_3^4,\ Z_4^3,\ Z_3Z_4Z_5.$$

We have

$$\begin{aligned} Z_3^4(X_0, X_1; Y_0, Y_1) &= q^{44} - 112q^{45} + 6096q^{46} - 214592q^{47} + \cdots, \\ Z_4^3(X_0, X_1; Y_0, Y_1) &= \phantom{q^{44}} - q^{45} + 120q^{46} - 7020q^{47} + \cdots, \\ Z_3Z_4Z_5(X_0, X_1; Y_0, Y_1) &= q^{44} - 114q^{45} + 6336q^{46} - 228632q^{47} + \cdots, \end{aligned}$$

from which we determine that any linear relation among these monomials is contained in the kernel of the matrix

$$\begin{pmatrix} 1 & -112 \\ 0 & -1 \\ 1 & -114 \end{pmatrix}.$$

But the kernel is already one-dimensional, being the **Q**-span of the row vector $(1, 2, -1)$. Thus we conclude that $\widetilde{F}_8$ is a scalar multiple (which can easily be determined by examining the coefficient of the top X_0-degree term) of

$$Z_3^4 + 2Z_4^3 - Z_3Z_4Z_5.$$

We tabulate $\widetilde{F}_n$ (up to a $\mathbf{Q}^\times$-factor, so that equality below is to be interpreted as up to $\mathbf{Q}^\times$-scaling) for $n \le 27$ (Observe the errors in $\widetilde{F}_{13}$ and $\widetilde{F}_8$ in [7, vol. 2, p. 150]). We note that Klein writes $\widetilde{F}_n$ for $n \equiv \pm 1 \bmod 5$ in terms of the A_i and $B_i := A_i(-X_1, X_0; Y_0, Y_0)$, and we use the W_i and Z_i because $\widetilde{F}_n$ is *significantly* simpler in these variables. We do not know why Klein did not use his variables A, B, C, D as in [11, p. 242] to write $\widetilde{F}_n$, as the computations involved are much less arduous for even moderately large n when using the W_i's and Z_i's.

$$F_2 = W_3$$

$$F_3 = Z_4$$

$$F_4 = Z_6$$

$$F_6 = W_2W_{10} - W_6^2$$

$$F_7 = W_3W_5 - W_4^2$$

$$F_8 = -Z_3^4 + Z_3Z_4Z_5 - 2Z_4^3$$

$$F_9 = -4Z_2^3Z_6 + Z_2Z_{10} + 3Z_6^2$$

$$F_{11} = 4W_2^6 - 4W_2^3W_6 + W_2W_{10} - W_6^2$$

$$F_{12} = 2W_3^8 - W_3^5W_4W_5 + W_3W_4^4W_5 - W_4^6$$

$$F_{13} = -Z_3^3Z_5 - Z_3^2Z_4^2 + Z_4Z_5^2$$

$$F_{14} = -16Z_2^9Z_6 + 4Z_2^7Z_{10} - 36Z_2^6Z_6^2 + 4Z_2^4Z_6Z_{10} - 20Z_2^3Z_6^3 + Z_2^2Z_{10}^2 - 2Z_2Z_6^2Z_{10} + Z_6^4$$

$$F_{16} = -8W_2^9W_6 + 4W_2^7W_{10} + 52W_2^6W_6^2 - 18W_2^4W_6W_{10} + 10W_2^3W_6^3 + W_2^2W_{10}^2 - W_6^4$$

$$F_{17} = 8W_3^6 - 10W_3^3W_4W_5 + 9W_3^2W_4^3 + W_3W_5^3 - W_4^2W_5^2$$

$$F_{18} = -8Z_3^{12} + 8Z_3^9Z_4Z_5 - 12Z_3^8Z_4^3 - Z_3^7Z_5^3 + 4Z_3^6Z_4^2Z_5^2 - 2Z_3^5Z_4^4Z_5 - 2Z_3^4Z_4^6 + Z_3^4Z_4Z_5^4 - 5Z_3^3Z_4^3Z_5^3 + 10Z_3^2Z_4^5Z_5^2 - 9Z_3Z_4^7Z_5 + 3Z_4^9$$

$$F_{19} = -4Z_2^7Z_6 + Z_2^5Z_{10} + 31Z_2^4Z_6^2 - 24Z_2^2Z_6Z_{10} - 8Z_2Z_6^3 + 4Z_{10}^2$$

$$F_{21} = -16W_2^7W_6^3 + W_2^6W_{10}^2 + 2W_2^5W_6^2W_{10} + 285W_2^4W_6^4 - 16W_2^3W_6W_{10}^2 - 72W_2^2W_6^3W_{10} + 72W_2W_6^5 + 4W_2W_{10}^3 - 4W_6^2W_{10}^2$$

$$F_{22} = 8W_3^{12} - 36W_3^9W_4W_5 + 60W_3^8W_4^3 + W_3^7W_5^3 + 52W_3^6W_4^2W_5^2 - 172W_3^5W_4^4W_5 + 134W_3^4W_4^6 - 2W_3^4W_4W_5^4 - 22W_3^3W_4^3W_5^3 + 113W_3^2W_4^5W_5^2 - 171W_3W_4^7W_5 + W_3W_4^2W_5^5 + 81W_4^9 - W_4^4W_5^4$$

$$F_{23} = -64Z_3^8 + 120Z_3^5Z_4Z_5 - 144Z_3^4Z_4^3 - Z_3^3Z_5^3 - 57Z_3^2Z_4^2Z_5^2 + 135Z_3Z_4^4Z_5 - 81Z_4^6 + Z_4Z_5^4$$

$$F_{24} = -64Z_2^{16}Z_6Z_{10} + 576Z_2^{15}Z_6^3 + 16Z_2^{14}Z_{10}^2 + 1888Z_2^{13}Z_6^2Z_{10} - 16752Z_2^{12}Z_6^4 - 1264Z_2^{11}Z_6Z_{10}^2 + 7840Z_2^{10}Z_6^3Z_{10} - 9648Z_2^9Z_6^5 + 188Z_2^9Z_{10}^3 - 1028Z_2^8Z_6^2Z_{10}^2 + 2324Z_2^7Z_6^4Z_{10} - 1996Z_2^6Z_6^6 + 12Z_2^6Z_6Z_{10}^3 - 52Z_2^5Z_6^3Z_{10}^2 + 132Z_2^4Z_6^5Z_{10} + Z_2^4Z_{10}^4 - 92Z_2^3Z_6^7 - 4Z_2^3Z_6^2Z_{10}^3 + 6Z_2^2Z_6^4Z_{10}^2 - 4Z_2Z_6^6Z_{10} + Z_6^8$$

$$F_{26} = 16W_2^{15}W_6^2 - 8W_2^{13}W_6W_{10} + 136W_2^{12}W_6^3 + W_2^{11}W_{10}^2 - 134W_2^{10}W_6^2W_{10} + 805W_2^9W_6^4 + 42W_2^8W_6W_{10}^2 - 588W_2^7W_6^3W_{10} + 1554W_2^6W_6^5 - 4W_2^6W_{10}^3 + 240W_2^5W_6^2W_{10}^2 - 1008W_2^4W_6^4W_{10} + 1204W_2^3W_6^6 - 52W_2^3W_6W_{10}^3 + 180W_2^2W_6^3W_{10}^2 - 360W_2W_6^5W_{10} + 4W_2W_{10}^4 + 216W_6^7 - 4W_6^2W_{10}^3$$

$$F_{27} = 192W_3^{12} - 408W_3^9W_4W_5 + 496W_3^8W_4^3 + 3W_3^7W_5^3 + 295W_3^6W_4^2W_5^2 - 837W_3^5W_4^4W_5 + 559W_3^4W_4^6 - 3W_3^4W_4W_5^4 - 80W_3^3W_4^3W_5^3 + 402W_3^2W_4^5W_5^2 - 576W_3W_4^7W_5 + W_3W_4^2W_5^5 + 256W_4^9 - W_4^4W_5^4$$

Appendix D. Evaluation of Certain Arithmetic Sums

In this section, we prove two results that are used in §7.

Lemma D.1. *Let φ denote Euler's function, and let m be a positive integer. Then*

$$\sum_{\substack{k=1 \\ k\equiv 0 \bmod m}}^{N} \frac{\varphi(k)}{k^2} = \frac{6}{\pi^2}\frac{1}{[\Gamma(1):\Gamma_0(m)]}\log N + O(1),$$

where the O-constant is absolute: it is independent of m and N.

Proof. We will study sums of the form $\sum_{k>0, k\equiv a \bmod m} \varphi(dk)\chi(k)/k^s$ as $s \to 1^+$, where χ is a Dirichlet character modulo m and $d = \gcd(a,m) \geq 1$. We may write $a = da'$ and $m = dm'$, so

$$\sum_{\substack{k>0 \\ k\equiv a \bmod m}} \frac{\varphi(k)}{k^s} = \sum_{\substack{k>0 \\ k\equiv a' \bmod m'}} \frac{\varphi(dk)}{(dk)^s}$$

$$= \frac{1}{\varphi(m')d^s} \sum_{\chi \bmod m'} \overline{\chi}(a') \sum_{k>0} \frac{\varphi(dk)\chi(k)}{k^s}. \tag{D.1}$$

We are therefore reduced to understanding sums of the form $\sum_{k>0} \varphi(dk)\chi(k)/k^s$. Since $\varphi(nd)/\varphi(d)$ is a multiplicative function of n, we have an Euler product:

$$\sum_{k>0} \frac{\varphi(dk)\chi(k)}{k^s} = \varphi(d) \sum_{k>0} \frac{\varphi(dk)}{\varphi(d)} \frac{\chi(k)}{k^s}$$
$$= \varphi(d) \prod_p \left(\sum_{r\geq 0} \frac{\varphi(dp^r)}{\varphi(d)} \frac{\chi(p^r)}{p^{rs}} \right).$$

We would like to simplify the inner sum occuring in the product above; in order to do this, we must distinguish two cases.

If $p \nmid d$ then we have

$$\begin{aligned}
\sum_{r\geq 0} \frac{\varphi(dp^r)}{\varphi(d)} \frac{\chi(p^r)}{p^{rs}} &= \sum_{r\geq 0} \frac{\varphi(p^r)\chi(p^r)}{p^{rs}} \\
&= 1 + \sum_{r>0} \frac{p-1}{p} \cdot \frac{p^r\chi(p^r)}{p^{rs}} \\
&= 1 + \frac{p-1}{p} \frac{p\chi(p)/p^s}{1 - p\chi(p)/p^s} \\
&= 1 + (p-1) \frac{\chi(p)}{p^s - p\chi(p)} \\
&= \frac{p^s - \chi(p)}{p^s - p\chi(p)} \\
&= \frac{1 - \chi(p)/p^s}{1 - \chi(p)/p^{s-1}}.
\end{aligned}$$

On the other hand, if $p|d$ then let us write $d = p^e d'$ with $p \nmid d'$ and $e > 0$. Then since

$$\frac{\varphi(dp^r)}{\varphi(d)} = \frac{\varphi(d')\varphi(p^{r+e})}{\varphi(d')\varphi(p^e)} = p^r,$$

we have

$$\begin{aligned}
\sum_{r\geq 0} \frac{\varphi(dp^r)}{\varphi(d)} \frac{\chi(p^r)}{p^{rs}} &= \sum_{r\geq 0} \frac{p^r\chi(p^r)}{p^{rs}} \\
&= \sum_{r\geq 0} \frac{\chi(p)^r}{p^{r(s-1)}} \\
&= \frac{1}{1 - \chi(p)/p^{s-1}}.
\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{k>0}\frac{\varphi(dk)\chi(k)}{k^s} &= \varphi(d)\prod_{p\mid d}\frac{1}{1-\chi(p)/p^{s-1}}\prod_{p\nmid d}\frac{1-\chi(p)/p^s}{1-\chi(p)/p^{s-1}}\\ &= \varphi(d)\frac{L(s-1,\chi)}{L(s,\chi)}\frac{1}{\prod_{p\mid d}(1-\chi(p)/p^s)}.\end{aligned}$$

Together with (D.1), this gives

$$\sum_{\substack{k>0\\ k\equiv a \bmod m}}\frac{\varphi(k)}{k^s} = \frac{\varphi(d)}{d^s\varphi(m')}\sum_{\chi \bmod m'}\overline{\chi}(a')\frac{L(s-1,\chi)}{L(s,\chi)}\prod_{p\mid d}\frac{1}{1-\chi(p)/p^s}.$$

Observe that for nontrivial $\chi \bmod m'$, the term $L(s-1,\chi)/L(s,\chi)$ is holomorphic for $\mathrm{Re}(s)\geq 2$, while $L(s-1,\chi_{\mathrm{triv}})/L(s,\chi_{\mathrm{triv}})$ has a simple pole at $s=2$. Using the fact that

$$L(s,\chi_{\mathrm{triv}}) = \zeta(s)\prod_{p\mid m'}(1-1/p^s)$$

and the expansion $\zeta(s) = 1/(s-1)+h(s)$ where $h(s)$ is holomorphic, we see that

$$\sum_{\substack{k>0\\ k\equiv a \bmod m}}\varphi(k)/k^s$$

has a simple pole at $s=2$ with residue

$$\text{(D.2)}\qquad \frac{\varphi(d)}{\varphi(m')d^2}\frac{\prod_{p\mid m'}(1-1/p)}{\prod_{p\mid m'}(1-1/p^2)\cdot\zeta(2)}\prod_{\substack{p\mid d\\ p\nmid m'}}\frac{1}{1-1/p^2} = \frac{6}{\pi^2 d^2}\frac{\varphi(d)}{\varphi(m')}\prod_{p\mid m'}\left(1-\frac{1}{p}\right)\prod_{p\mid dm'}\frac{1}{1-1/p^2}.$$

We now appeal to the following well-known theorem (make the change of variable $s' = s/2$):

Theorem D.2. *Let $f(s) = \sum_{k>0}a_k/k^s$ converge absolutely for $\mathrm{Re}(s)>2$ with analytic continuation to $\mathrm{Re}(s)=2$ except for a simple pole at $s=2$ with residue R. Then*

$$\sum_{k\leq x}\frac{a_k}{k^2} = R\log x + O(1).$$

Theorem D.1 now follows on setting $a=m$ in (D.2) and using the well-known identity $[\Gamma(1):\Gamma_0(m)] = m\prod_{p\mid m}(1+1/p)$. ■

Lemma D.3. *Let a and k be integers with $k>0$, and let p be a prime that divides k. Assume $p\nmid a$, and let ζ be a primitive kth root of unity in $\mathbf{C}$. Define*

$$c_k(m) = \sum_{\substack{h\in(\mathbf{Z}/k\mathbf{Z})^\times\\ h\equiv a \bmod p}}\zeta^{hm}.$$

Then

$$c_k(m) = \begin{cases}(\mu(k/(m,k))\varphi(k))/((p-1)\varphi(k/(m,k))) & \text{if } \mathrm{ord}_p(k)\leq \mathrm{ord}_p(m),\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Since $\zeta^{k/p}$ is a primitive pth root of unity, we may write

$$\begin{aligned} c_k(m) &= \frac{1}{p} \sum_{\zeta_0^p=1} \sum_{h \in (\mathbf{Z}/k\mathbf{Z})^\times} \zeta_0^{-(a-h)} \zeta^{mh} \\ &= \frac{1}{p} \sum_{j \in \mathbf{Z}/p\mathbf{Z}} \zeta^{-kja/p} \sum_{h \in (\mathbf{Z}/k\mathbf{Z})^\times} \zeta^{(m+jk/p)h}. \end{aligned}$$

We can remove the a in the first exponent since $p \nmid a$. Combining this with the standard evaluation

$$\sum_{h \in (\mathbf{Z}/k\mathbf{Z})^\times} \zeta^{\ell h} = \mu(k/(k,\ell)) \cdot \frac{\varphi(k)}{\varphi(k/(k,\ell))}$$

for $\ell \in \mathbf{Z}$, we get

$$c_k(m) = \frac{1}{p} \sum_{j \in \mathbf{Z}/p\mathbf{Z}} \zeta^{-kj/p} \mu\left(\frac{k}{(k, m+jk/p)}\right) \frac{\varphi(k)}{\varphi(k/(k,m+jk/p))}.$$

Evidently,

$$(k, m+jk/p) = \begin{cases} (m,k/p) & \text{if } j \not\equiv 0 \bmod p \\ (m,k) & \text{otherwise} \end{cases}.$$

Therefore,

$$c_k(m) = \frac{1}{p}\left(-\mu\left(\frac{k}{(m,k/p)}\right)\frac{\varphi(k)}{\varphi(k/(m,k/p))} + \mu\left(\frac{k}{(m,k)}\right)\frac{\varphi(k)}{\varphi(k/(m,k))}\right).$$

If $\mathrm{ord}_p(m) < \mathrm{ord}_p(k)$ then $(m,k) = (m,k/p)$ so $c_k(m) = 0$. On the other hand, if $\mathrm{ord}_p(m) \geq \mathrm{ord}_p(k)$ then $(m,k/p) = (m,k)/p$ and $\mathrm{ord}_p(k/(m,k)) = 0$, so we have

$$\begin{aligned} c_k(m) &= \frac{1}{p}\left(-\mu\left(\frac{pk}{(m,k)}\right)\frac{\varphi(k)}{\varphi(pk/(m,k))} + \mu\left(\frac{k}{(m,k)}\right)\frac{\varphi(k)}{\varphi(k/(m,k))}\right) \\ &= \frac{1}{p}\mu\left(\frac{k}{(m,k)}\right)\left(\frac{\varphi(k)}{\varphi(p)\varphi(k/(m,k))} + \frac{\varphi(k)}{\varphi(k/(m,k))}\right) \\ &= \frac{1}{\varphi(p)}\mu\left(\frac{k}{(m,k)}\right)\frac{\varphi(k)}{\varphi(k/(m,k))} \end{aligned}$$

This completes the proof. ∎

References

[1] B.C. Berndt, H.H. Chan, and L.C. Zhang, Explicit evaluations of the Rogers–Ramanujan continued fraction. J. reine angew. Math. **480** (1996), 141-159.

[2] B.C. Berndt, H.H. Chan, S-S Huang, S-Y Kang, J. Sohn, S.H. Son, The Rogers–Ramanujan continued fraction, J. Computational and Applied Mathematics **105** (1999), 9–24.

[3] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer-Verlag, 1990.

[4] Cohen, P. On the coefficients of the transformation polynomials for the elliptic modular function. Math. Proc. Camb. Phil. Soc. (1984), **95**, 389-402

[5] P. Deligne and M. Rapoport, "Les schémas de modules des courbes elliptiques" in *Modular functions of one variable II*, Lecture notes in mathematics **349**, Springer-Verlag (1973), pp. 143–316.

[6] Elkies, N.D. "The Klein quartic in number theory" in *The eightfold way*, MSRI publications, (1999), **35**, pp. 51–101.

[7] R. Fricke and F. Klein, *Vorlesungen über die Theorie der elliptischen Modulfunktionen*, Vol. II, B.G. Teubner, 1890-2.

[8] A. Gee and M. Honsbeek, Singular values of the Rogers–Ramanujan continued fraction, Ramanujan Journal, to appear.

[9] Kang, S. Ramanujan's formulas for the explicit evaluation of the Rogers–Ramanujan continued fraction and theta-functions. Acta Arith. XC.1 (1999), 49-67.

[10] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of math studies **108**, Princeton University Press, 1985.

[11] Klein, F. *Lectures on the icosahedron*, Dover Publications, Inc. (1956).

[12] H. Kraft and C. Procesi, *Classical invariant theory: a primer*, www.math.unibas.ch/∼kraft/Papers/KP-Primer.pdf, 1996.
[13] Kubert, D.S., Lang, S. *Modular Units.* Springer-Verlag, New York 1981.
[14] Lang, S. *Elliptic Functions.*, 2nd ed. Springer-Verlag, New York, 1987.
[15] Lang, S. *Algebra*, 3rd ed. Addison-Wesley, New York, 1993.
[16] H. Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.
[17] McKean, H., Moll, V. *Elliptic curves.* Cambridge University Press, Cambridge 1997.
[18] Serre, J.P. *A Course in Arithmetic.* Springer-Verlag, New York, 1990.
[19] Shimura, G. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, Princeton NJ. 1994.
[20] Silverman, J.H. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, New York 1994.
[21] Watson, G.N. Theorems Stated by Ramanujan (VII): theorems on continued fractions, J. London Math. Soc. **4** (1929), 39-48.
[22] Whittaker, E.T., Watson, G.N. *A Course of Modern Analysis.* Cambridge University Press, Cambridge 1996.
[23] Yi, J. Modular Equations for the Rogers–Ramanujan Continued Fraction and the Dedekind Eta-Function. Ramanujan J. **5** (2001), 377-384.
[24] Yi, J. Evaluations of the Rogers–Ramanujan continued fraction $R(q)$ by modular equations. Acta Arith. XCVII.2 (2001), 103-127.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: bcais@umich.edu

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: bdconrad@umich.edu