THE ADELIC CLOSURE OF TRIANGLE GROUPS

FRANK CALEGARI

Abstract. We compute the congruence completions of certain triangle groups (n, ∞, ∞) and $(2, n, \infty)$ for n odd, answering some questions raised in [McM24].

1. Introduction

The goal of this note is to answer some questions concerning triangle groups first raised in [McM24]. Fix an integer $n \geq 3$, and let $\zeta = e^{2\pi i/n}$ be an nth root of unity in $\mathbf{C}$. In this paper, we shall be concerned with the family of triangle groups $\Delta = \Delta_n \subset \mathrm{SL}_2(\mathbf{R})$ given explicitly by $\Delta = \langle T, U, R \rangle$, where:

$$T = \begin{pmatrix} 1 & 2 + \zeta + \zeta^{-1} \\ 0 & 1 \end{pmatrix}, \quad U = - \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad R = UT.$$

The element R has order n, and the quotient $\mathbf{H}/\Delta$ is a hyperbolic orbifold of genus zero with signature $(n/2, \infty, \infty)$ when n is even and $(2, n, \infty)$ when n is odd. If $K = \mathbf{Q}(\zeta + \zeta^{-1})$ and $\mathcal{O} = \mathcal{O}_K = \mathbf{Z}[\zeta + \zeta^{-1}]$, then $\Delta \subset \Gamma := \mathrm{SL}_2(\mathcal{O})$. Let $\widehat{\mathcal{O}}$ denote the closure of $\mathcal{O}$ inside the finite adeles $\mathbf{A}^f_K$. There is a natural map

$$\Delta \to \mathrm{SL}_2(\mathcal{O}) \hookrightarrow \mathrm{SL}_2(\widehat{\mathcal{O}}).$$

Let $\widehat{\Delta}$ denote the closure of the image of Δ. (The adelic group $\widehat{\Gamma} := \mathrm{SL}_2(\widehat{\mathcal{O}})$ has a natural topology as a profinite group; we can also view it as the congruence closure of $\mathrm{SL}_2(\mathcal{O})$, that is, the profinite group given by the projective limit of the groups $\mathrm{SL}_2(\mathcal{O}/d)$ over all integers d.) As noted in [McM24, Prop 1.15], the group $\widehat{\Delta}$ has finite index in $\widehat{\Gamma}$. The goal of this note is to describe $\widehat{\Delta}$ as precisely as possible. One application of these results is to answer a number of questions first raised in [McM24]. (The paper [McM24] is itself an offshoot of a number of other papers — including [McM23] and [McM22] — whose goal is to understand billiards in regular polygons.) One of the intentions of [McM24] was to distill a number of purely group theoretical and number theoretical questions in a transparent way, and [McM24] makes no direct reference to billiards. In this paper, we similarly shall not mention these connections, but rather refer the reader (as a starting point) to [McM24, McM23, McM22]. Instead, the questions raised in [McM24] are phrased directly in terms of the arithmetic of the cusps of Δ, and we now recall the basic story of these cusps. The group $\Delta \subset \mathrm{SL}_2(\mathbf{R})$ acts on the usual upper half plane $\mathbf{H}$ with finite covolume. The quotient curve (orbifold) $\mathbf{H}/\Delta$ has either one or two cusps (∞ and 0) depending on the parity of n; in the usual way one can think about these cusps as certain orbits of $\mathbf{P}^1(K) \subset \mathbf{P}^1(\mathbf{R})$ under the action of Δ. Very explicitly, if

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta, \tag{1}$$

then $a/c \in \mathbf{P}^1(K)$ lies in the orbit of ∞ and b/d lies in the orbit of 0. If $[K : \mathbf{Q}] \leq 2$, then every point of $\mathbf{P}^1(K)$ is a cusp. If $[K : \mathbf{Q}] > 2$, this is no longer true, and there is no known explicit characterization of the cusps. Even when $[K : \mathbf{Q}] = 2$ (which occurs for $n = 5$, 8, and 12), there are still many mysteries regarding the cusps. In these cases, given $x \in \mathbf{P}^1(K)$, then there exists a $\gamma \in \Delta$ as in (1) such that either a/c or b/d is equal to x. (For more general n this still holds at least if one assumes that x is a cusp of Δ.) But the column $[a, c]$ of γ turns out to be unique up to sign, whereas (assuming $[K : \mathbf{Q}] > 1$ so the unit group of K is infinite) there are many

The author was supported in part by NSF Grant DMS-2001097.

possible pairs (a, c) for which $a/c = x$. It is precisely the map which sends a cusp $x \in \mathbf{P}^1(K)$ to a representative $[a, c]$ (up to sign) with $a/c = x$ which is poorly understood. In [McM24], certain simple functions δ and κ on the set of cusps are considered. For example, when n is even, the map κ is the function on the set of cusps $x \in \mathbf{P}^1(K)$ which is 0 when x is in the orbit of the cusp ∞ and 1 if x is in the orbit of 0. The definition of δ is slightly more complicated and is recalled in section 6. McMullen raises the problem as to what extent these maps are *congruence*, that is, whether they only depend on the image of $x \in \mathbf{P}^1(\mathcal{O})$ in $\mathbf{P}^1(\mathcal{O}/N)$ for some integer N. It is shown in [McM24] that, when the prime factorization of n has certain explicit forms, these maps are congruence. However, it is also shown [McM24, Thm 1.13] that δ is *not* congruence when $n = 12$. In this paper, we extend this result to show that δ and κ are *never* congruence invariants in all the remaining cases not addressed in [McM24], generalizing the result (and method) for δ addressed in [McM24] when $n = 12$. In particular, we have (see Theorems 6.1 and 6.3):

Theorem 1.1. *The invariant δ congruence if and only if either $4 \nmid n$ or $n = 2^k$. The invariant κ is congruence unless $n = 2m$ where m is odd and has at least two prime factors.*

As suggested by the arguments of [McM24], one can establish this result as a consequence of understanding the adelic closure $\widehat{\Delta}$ of Δ in $\widehat{\Gamma} = \mathrm{SL}_2(\widehat{\mathcal{O}})$. We turn to this now, breaking up the result into two parts depending on whether one is considering the prime $p > 2$ or $p = 2$.

Theorem 1.2. *The congruence closure $\widehat{\Delta}$ of Δ is a direct product of the closures*

$$\widehat{\Delta}_p \subseteq \widehat{\Gamma}_p = \mathrm{SL}_2(\mathcal{O} \otimes \mathbf{Z}_p) = \prod_{\mathfrak{p}|p} \mathrm{SL}_2(\mathcal{O}_{\mathfrak{p}})$$

of Δ for all primes p of $\mathbf{Z}$. Moreover, $\widehat{\Delta}_p$ has index one for all odd primes p outside the following two exceptions, where in both cases there is a unique prime $\mathfrak{p}$ above p in $\mathcal{O}$.

(1) *$n = 2p^k$, $k \geq 1$, and $\widehat{\Delta}_p$ is the preimage of $\mathbf{Z}/p\mathbf{Z} \subset \mathrm{SL}_2(\mathcal{O}/\mathfrak{p}) = \mathrm{SL}_2(\mathbf{F}_p)$ with index $p^2 - 1$.*
(2) *$n = 5p^k$, $k \geq 0$, $p = 3$, and $\widehat{\Delta}_p$ is the preimage of $A_5 \subset A_6 \simeq \mathrm{PSL}_2(\mathbf{F}_9) = \mathrm{PSL}_2(\mathcal{O}/\mathfrak{p})$.*

This follows from Lemmas 4.2, 4.6, and 4.8. We now give a precise description of the 2-adic closure $\widehat{\Delta}_2$. In the introduction, we only give the statement in the case when n is not a power of 2, and leave the statement of the remaining case when $n = 2^k$ to the main body of the text (see Theorem 5.2). For any (commutative) ring A, any ideal I, and any group $G \subset \mathrm{SL}_2(A)$, let $G(J)$ denote the kernel of the homomorphism $G \to \mathrm{SL}_2(A/J)$. Furthermore, we let $M^0(A)$ denote the additive group of 2×2 matrices over A with trace zero. If A is a ring with $2 = 0$, then $M^0(A)$ has a subgroup isomorphic to A consisting of diagonal matrices. The following is proved in Section 3 (note that Theorem 1.3 (3) is [McM24, Thm 1.1]).

Theorem 1.3. *Suppose that n is not a power of 2. Then:*

(1) *There is an equality $\widehat{\Delta}(4)_2 = \widehat{\Gamma}(4)_2 = \mathrm{SL}_2(\mathcal{O} \otimes \mathbf{Z}_2)(4)$.*
(2) *Consider the homomorphism*

$$\widehat{\Delta}(2)/\widehat{\Delta}(4) \simeq \Delta(2)/\Delta(4) \to \Gamma(2)/\Gamma(4) = I + 2M^0(\mathcal{O}/2).$$

The index of the image is $|\mathcal{O}/2|/2$. The intersection of the image with the subgroup $\mathcal{O}/2$ of diagonal matrices of the target consists only of $\{0, I\}$.
(3) *The image of $\Delta/\Delta(2)$ inside $\mathrm{SL}_2(\mathcal{O}/2)$ is isomorphic to $D_{n'}$ where $n' = n/2$ if n is even and $n' = n$ otherwise.*

In particular, the 2-adic index is given by $\dfrac{|\mathrm{SL}_2(\mathcal{O}/2)|}{2n'} \cdot \dfrac{|\mathcal{O}/2|}{2}$.

Combining these two theorems (together with Theorem 5.2 which explains what happens when $n = 2^k$), we obtain the following formula for the full index of $\widehat{\Delta}$ in $\widehat{\Gamma}$, namely:

Theorem 1.4. *The index of $\widehat{\Delta}$ in $\widehat{\Gamma}$ for $n \geq 3$ is given by* $\dfrac{|\mathrm{SL}_2(\mathcal{O}/2)|}{2n'} \cdot \dfrac{|\mathcal{O}/2|}{2}$ *where $n' = n/2$ if n is even and n if n is odd, times the following extra factors in the following exceptional circumstances:*

(1) *A factor of 2 if $n = 2^k$.*

(2) *A factor of* 6 *if* $n = 5 \cdot 3^k$ *and* $k \geq 0$.
(3) *A factor of* $p^2 - 1$ *if* $n = 2 \cdot p^k$ *and* $k \geq 1$.

Note that at most one of these exceptional circumstances can occur for any given n.

Remark 1.5. We can also write out the order of $|\mathrm{SL}_2(\mathcal{O}/2)| \cdot |\mathcal{O}/2|$ more explicitly as follows: Let d be the degree of K, so $d = \varphi(n)/2$. With $n = 2^k \cdot m$ with m odd, and $n \geq 3$.

(1) Let e be the ramification degree of 2 in K, so, if $m > 1$, then $e = \varphi(2^k)$, and if $m = 1$, then $e = \varphi(n)/2 = \varphi(2^k)/2$.
(2) Let f be the order of the decomposition group of 2 in K, so f is the order of 2 in $(\mathbf{Z}/m\mathbf{Z})^{\times}/(\pm 1)$.
(3) Let r be the number of primes above 2 in $\mathcal{O}$, so $d = erf$.

Then $|\mathcal{O}/2| = 2^d$, and

$$\begin{aligned} |\mathrm{SL}_2(\mathcal{O}/2)| &= |\mathbf{F}|^{3r(e-1)} \cdot |\mathrm{SL}_2(\mathbf{F})|^r = |\mathbf{F}|^{3r(e-1)} \cdot (|\mathbf{F}|^3 - |\mathbf{F}|)^r, \\ &= |\mathbf{F}|^{3re} \cdot \left(1 - \frac{1}{|\mathbf{F}|^2}\right)^r \\ &= 2^{3d}\left(1 - \frac{1}{2^{2f}}\right)^r. \end{aligned}$$

An explicit table of the indices for $3 \leq n \leq 16$ is given below:

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$[\widehat{\Gamma} : \widehat{\Delta}]$	1	3	72	8	144	24	112	288	23808	8	322560	6912	6528	3072

1.6. **Acknowledgments.** I would like to thank Curt McMullen both for encouraging me to write this note and also for a number of useful discussions, remarks, and references.

2. Some preliminaries

In this section, we record some preliminary facts and lemmas which will be used in the sequel. In addition to the field $K = \mathbf{Q}(\zeta + \zeta^{-1})$, we shall also consider $L = \mathbf{Q}(\zeta)$. If we write $n = 2^k m$ with m odd, then $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^{\times} = (\mathbf{Z}/m\mathbf{Z})^{\times} \times (\mathbf{Z}/2^k\mathbf{Z})^{\times}$, whereas $\mathrm{Gal}(K/\mathbf{Q})$ is the quotient of this group by the image of complex conjugation, given explicitly by $c = (-1, -1)$. If $m > 1$, it follows from this description and the natural identification of the inertia group at 2 of $\mathrm{Gal}(L/\mathbf{Q})$ with $(\mathbf{Z}/2^k\mathbf{Z})^{\times}$ that L/K is unramified at all primes above 2. The ramification index e of (both) fields at the prime 2 is $e = \varphi(2^k)$ which equals 2^{k-1} if $k \geq 1$ and 1 otherwise, unless $n = 2^k$ in which case $e = 2^{k-2}$ for K. Although Δ is naturally a subgroup of $\mathrm{SL}_2(\mathcal{O}_K)$, it will sometimes be convenient to work in the larger group $\mathrm{SL}_2(\mathcal{O}_L)$ where certain elements are naturally diagonalizable, making a number of explicit computations easier.

2.1. **The adjoint representation.** Let J be an ideal of $\mathcal{O}_K$. The ideal J is principal in the ring $\mathcal{O}/J^2$ and any choice of generator gives an isomorphism $J/J^2 \simeq \mathcal{O}/J$. If $\Gamma = \mathrm{SL}_2(\mathcal{O}_K)$, then there is a corresponding identification

$$\Gamma(J)/\Gamma(J^2) \simeq I + M^0(J/J^2) \simeq M^0(\mathcal{O}/J), \tag{2}$$

where $M^0(A)$ denotes the 2×2 matrices in A with trace zero (the trace zero condition comes from the fact that elements in Γ have determinant one). Not only is (2) an isomorphism of (abelian) groups, but there is also a natural action of $\Gamma/\Gamma(J) \simeq \mathrm{SL}_2(\mathcal{O}/J)$ on $\Gamma(J)/\Gamma(J^2)$ such that the corresponding action on $M^0(\mathcal{O}/J)$ is given by conjugation. More generally, for any non-zero ideal $P \subset \mathcal{O}$, we have

$$\Gamma(JP)/\Gamma(J^2P) \simeq M^0(\mathcal{O}/J)$$

A natural approach to understanding the closure of a subgroup G of $\mathrm{SL}_2(\mathcal{O}_{\mathfrak{p}})$ is to consider the filtration of G by $G(\mathfrak{p}^r)$ and understand the graded pieces $G(\mathfrak{p}^r)/G(\mathfrak{p}^{r+1})$ as modules for the image $G/G(\mathfrak{p})$ of G in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$.

Remark 2.2. A basic principle which we apply repeatedly through the paper (sometimes explicitly but more often implicitly) is the following. Let B be a p-group or a pro-p group and let $A \subset B$ be a closed subgroup. In order to prove that $A = B$, it suffices, by Burnside's basis theorem [Hal59, Thm 12.2.1], to show that A surjects onto the maximal exponent p-abelian quotient $B/\Phi(B)$ of B. In the context of our problem, one should imagine taking A to be $\widehat{\Delta}(\mathfrak{p})$, and $B \subset \widehat{\Gamma}(\mathfrak{p})$ to be the subgroup which we hope to show is equal to A. One measure of the difficulty in applying Burnside's theorem is the size of $B/\Phi(B)$. For the particular problem we are considering, these quotients are quite small when $p > 2$, since in all cases we can take $B = \widehat{\Gamma}(\mathfrak{p})$ with $\Phi(B) = \widehat{\Gamma}(\mathfrak{p}^2)$, However, when $p = 2$, B has large index in $\widehat{\Gamma}(\mathfrak{p})$, and the Frattini quotient $B/\Phi(B)$ is also large; this is reflected by the fact that we need to work harder to pin down the precise image when $p = 2$.

2.3. **The adjoint representation at 2.** It will be of particular importance when studying the 2-adic image of Δ to understand the basic group theory of these modules, which we discuss now. If $n = 2^k m$ with $m > 1$ odd, it is shown in [McM24, Theorem 1.1] that the image of Δ in $\mathrm{SL}_2(\mathcal{O}_K/2)$ is isomorphic to $D_{n/2}$ if $k > 0$ and D_n otherwise. If $\mathfrak{p}$ is a prime of residue characteristic two, then the image of Δ in $\mathrm{SL}_2(\mathcal{O}_K/\mathfrak{p})$ is isomorphic to D_m. (The importance of the image of Δ in $\mathrm{SL}_2(\mathcal{O}_L/\mathfrak{p})$ is why we reserve m for the largest odd divisor of n, in contrast to [McM24] where $n = m$ or $n = 2m$ depending on whether n is odd or not; hopefully this conflict does not cause any confusion.)

Let $n = 2^k m$, Let $\zeta = \zeta_n$, and let

$$T = \begin{pmatrix} 1 & 2+\zeta+\zeta^{-1} \\ 0 & 1 \end{pmatrix}, \quad U = -\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad R = U.T.$$

The matrix R has order n and eigenvalues ζ and ζ^{-1}. Moreover, we can explicitly diagonalize R by the matrix of eigenvectors:

$$E = \begin{pmatrix} -1-\zeta & -1-\zeta^{-1} \\ 1 & 1 \end{pmatrix}. \tag{3}$$

Note that this matrix lies in $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$ for any prime $\mathfrak{p}|2$ only if $m > 1$ (so that $1+\zeta$ is a 2-adic unit). In the new basis, we have

$$\begin{aligned} E^{-1}RE &= \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix}, \\ E^{-1}TE &= \frac{1}{1-\zeta}\begin{pmatrix} 2 & 1+\zeta \\ -1-\zeta & -2\zeta \end{pmatrix}, \\ E^{-1}UE &= \frac{1}{1-\zeta}\begin{pmatrix} -2 & -1-\zeta^{-1} \\ \zeta(1+\zeta) & 2\zeta \end{pmatrix}. \end{aligned} \tag{4}$$

The basis (4) will occasionally be more convenient for some computations. Note that it is only defined over the larger field $L = \mathbf{Q}(\zeta)$ rather than $K = \mathbf{Q}(\zeta+\zeta^{-1})$. We only use this basis when $m > 1$. Let us now assume that $m > 1$. (The case $n = 2^k$ is considered in Section 5.) Let D_m denote the dihedral group of order $2m$. Let $\mathbf{F}$ be the finite field of characteristic 2 given by adjoining $\zeta+\zeta^{-1}$ to $\mathbf{F}_2$ for a primitive mth root of unity ζ. (Note that if ζ is a primitive $2^k m$th root of unity, then the image of ζ in any field of characteristic 2 is a primitive mth root of unity.) The group D_m admits a 2-dimensional representation over $\mathbf{F}$ given by the image of Δ in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ for a prime $\mathfrak{p}|2$. The action of conjugation makes $M^0(\mathbf{F})$ a representation for D_m. There is a splitting

$$M^0(\mathbf{F}) \simeq \mathbf{F} \oplus Q$$

of this representation as a D_m module given explicitly by

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \oplus \begin{pmatrix} b+c & b(\zeta+\zeta^{-1}) \\ c & b+c \end{pmatrix} \tag{5}$$

The representation $Q/\mathbf{F}$ is absolutely irreducible. However, more is true:

Lemma 2.4. *The representation Q considered as a representation of D_m over $\mathbf{F}_2$ is irreducible.*

Proof. Over $\mathbf{F}_2$, the representation $Q/\mathbf{F}_2$ has dimension $2[\mathbf{F} : \mathbf{F}_2]$. The base change $Q/\mathbf{F}_2 \otimes_{\mathbf{F}_2} \mathbf{F}$ decomposes as a product of all the $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_2)$-conjugates of Q which are distinct representations because the trace of an order m element generates $\mathbf{F}$. It follows that the only $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_2)$-invariant subrepresentation is the entire space, and thus $Q/\mathbf{F}_2$ is irreducible. $\square$

Now suppose that $P = \prod_{\mathfrak{p}|2} \mathfrak{p}$. The image of Δ in $\mathrm{SL}_2(\mathcal{O}/P)$ is once again isomorphic to D_m. If r is any integer, there is an isomorphism

$$\Gamma(P^r)/\Gamma(P^{r+1}) \simeq \bigoplus_{\mathfrak{p}|2} \Gamma(P^r)/\Gamma(P^r\mathfrak{p}) \simeq \bigoplus_{\mathfrak{p}|2} M^0(\mathbf{F}) \simeq \bigoplus_{\mathfrak{p}|2} (\mathbf{F} \oplus Q).$$

Our goal will be to study the filtration $\Delta(P^r)/\Delta(P^{r+1})$ by showing that the image in $\Gamma(P^r)/\Gamma(P^{r+1})$ contains the Q-isotypic component of $\Gamma(P^r)/\Gamma(P^{r+1})$ for all $r \geq e$.

It will also be useful to consider $\Gamma(2)/\Gamma(4)$ as a module for the image $D_{n/2}$ (or D_n if n is odd) inside $\mathrm{SL}_2(\mathcal{O}/2)$. There certainly exists a splitting:

$$\Gamma(2)/\Gamma(4) \simeq I + 2M^0(\mathcal{O}/2) \simeq M^0(\mathcal{O}/2) \simeq (\mathcal{O}/2) \oplus \widetilde{Q},$$

where $\mathcal{O}/2$ is the subgroup consisting of scalar matrices, and $\widetilde{Q} \simeq (\mathcal{O}/2)^2$ is the group given by matrices of the form

$$\begin{pmatrix} b+c & b(\zeta+\zeta^{-1}) \\ c & b+c \end{pmatrix} \tag{6}$$

just as in the decomposition (5) above (remember we are assuming that $m > 1$ and so $\zeta + \zeta^{-1}$ is a 2-adic unit). All we shall use about $\widetilde{Q}$ is that it is stable under conjugation by the dihedral group.

2.5. **Roots of unity.** We have the following elementary construction involving roots of unity.

Lemma 2.6. *Let ζ be a root of unity of order $2^k m$ with $m > 1$ odd. Let $r \geq 0$ be an integer such that $2r + 1 < e$, where e is the ramification index of 2 in L. Let $\xi = \zeta^m = \zeta_{2^k}$. Let $\mathcal{O}_L = \mathbf{Z}[\zeta]$, so $(1 - \xi)\mathcal{O}_L = \prod \P_i$, where $\P_i$ are the primes above 2 in $\mathcal{O}$. The $\mathbf{Z}$-span of the elements*

$$\zeta^i - \zeta^j = \zeta^i + \zeta^j \mod 2$$

where i and j are odd contains an element of $\mathcal{O}_L/2$ with valuation exactly $2r$ at $\P$ and valuation greater than $2r$ at all other primes above 2. The $\mathbf{Z}$-span of the elements

$$\zeta^i(\xi^j - 1) \mod 2$$

where i and j are odd contains an element of $\mathcal{O}_L/2$ with valuation $2r+1$ at $\P$ and valuation greater than $2r + 1$ at all other primes above 2.

Proof. Since $\xi - 1$ has valuation 1, the second claim follows from the first (even taking $j = 1$). If $\alpha \in \mathcal{O}_L$ is expressible as a sum of an even number of roots of unity to odd exponent, then so is

$$\alpha(\xi^2 - 1) = \alpha\zeta^{2m} - \alpha,$$

and the valuation of $\alpha(\xi^2 - 1) = \alpha(\xi - 1)^2 \mod 2$ at any $\P$ is exactly 2 plus the valuation of α. Hence, by induction, it suffices to consider the case when $r = 0$. Certainly there exists an $\eta \in \mathcal{O}$ which is divisible by all primes above 2 with the exception of a chosen prime $\P$. Multiplying by the unit $(\zeta - 1)$ (which is a unit since $m > 1$), we can assume that η is expressible as a sum of an even number of roots of unity. Replacing any even odd exponent ζ by ζ^{i+m} keeps η unchanged modulo $(1 - \xi)\mathcal{O}_L$, which preserves the property of being co-prime to $\P$ but not any other prime above 2, and hence we have constructed the desired element. $\square$

3. The 2-adic image

We now consider the 2-adic image of Δ when $n = 2^k m$ and $m > 1$ is odd, deferring the case of $n = 2^k$ to Section 5. To prove Theorem 1.3, we both need to show that $\widehat{\Delta}_2$ is both contained and equal to what is described there. We begin by proving the desired containment. We already know the image of Δ in $\mathrm{SL}_2(\mathcal{O}/2)$ from [McM24, Thm 1.1], so we only need consider the image of $\Delta(2)$ in $\Gamma(2)/\Gamma(4)$. The statement to be proved is that the image of $\Gamma(2)$ is contained within the subgroup

$$\mathbf{F}_2 \oplus \widetilde{Q} \subset \mathcal{O}/2 \oplus \widetilde{Q} \simeq \Gamma(2)/\Gamma(4),$$

where the first $\mathbf{F}_2$ is generated by the image of the matrices $\pm I$. (As noted in [McM24, §1.V], the choice of signs in the definition of Δ ensures that $-I \in \Delta$.) Because $\Delta(2)$ is normal in Δ, and since this subspace is invariant under conjugation by $\Delta/\Delta(2)$, it suffices to show that a set of *normal* generators for $\Delta(2)$ maps to this space. But we know that, with $d = n/2$ if n is even and n otherwise, that

$$\Delta/\Delta(2) \simeq \langle T, U | T^2, U^2, R^d, R = (UT)\rangle.$$

So it suffices to check the claim for T^2, U^2, and R^d. The image of the latter is given by $-I$. On the other hand, we find that (modulo 4):

$$U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \equiv 1 + 2\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + 2\begin{pmatrix} b+c & b(\zeta+\zeta^{-1}) \\ c & b+c \end{pmatrix} \bmod 4$$

with $(a, b, c) = (1, 0, 1)$, whereas

$$T^2 = \begin{pmatrix} 1 & 4+2(\zeta+\zeta^{-1}) \\ 0 & 1 \end{pmatrix} \equiv 1 + 2\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + 2\begin{pmatrix} b+c & b(\zeta+\zeta^{-1}) \\ c & b+c \end{pmatrix} \bmod 4$$

with $(a, b, c) = (1, 1, 0)$.

We now turn to showing that $\widehat{\Delta}_2$ is as big as possible. We reduce it to the following:

Lemma 3.1. *Let e be the ramification degree of 2 in K, and let $P = \prod_{\mathfrak{p}|2} \mathfrak{p}$. Suppose there are d primes dividing 2 in $\mathcal{O}_K$. Suppose that the image of $\Delta(P^r)/\Delta(P^{r+1})$ inside*

$$\Gamma(P^r)/\Gamma(P^{r+1}) \simeq \bigoplus_{\mathfrak{p}|2} \Gamma(P^r)/\Gamma(P^r\mathfrak{p}) \simeq \bigoplus_{\mathfrak{p}|2} M^0(\mathbf{F}) \simeq \bigoplus_{\mathfrak{p}|2} (\mathbf{F} \oplus Q)$$

contains all d copies of Q for every $r = e, e+1, \ldots, 2e-1$. Then Theorem 1.3 holds.

Proof. Since we have already seen that the image of $\Delta(2)/\Delta(4)$ in $\mathcal{O}/2 \oplus \widetilde{Q}$ lands in $\mathbf{F}_2 \oplus \widetilde{Q}$ and contains the copy of $\mathbf{F}_2$ generated by $-I$, this certainly shows that the image is the entire space $\mathbf{F}_2 \oplus \widetilde{Q}$. Thus it suffices to prove that $\widehat{\Delta}_2(4) = \widehat{\Gamma}_2(4)$, or that the image of $\Delta(2^r)$ surjects onto $\Gamma(2^r)/\Gamma(2^{r+1})$ for every $r \geq 2$. We prove this by induction. Note that

$$\Delta(2^r)/\Delta(2^{r+1}) \simeq \mathcal{O}/2 \oplus \widetilde{Q}.$$

Suppose either that $r \geq 2$ and that the image is surjective, or that $r = 1$ and (by assumption) the image contains $\widetilde{Q}$. In both cases, the image certainly contains $\widetilde{Q}$. Hence, any pair of elements in $M_0(\mathcal{O}/2)$, there exist elements

$$I + 2^r A \bmod 2^{r+1}, \quad 1 + 2B \bmod 2^2$$

in the image of Δ where A and B realize the given elements up to a scalar matrix. Hence the image of Δ contains the commutator

$$[I + 2^r A \bmod 2^{r+1}, I + 2B \bmod 4] = I + 2^{r+1}(AB - BA) \bmod 2^{r+2}$$

Now replacing A and B by $A + \lambda I$ and $B + \mu I$ does't change $AB - BA$. On the other hand, the image of the map

$$M^0(\mathcal{O}/2)^2 \to M^0(\mathcal{O}/2)$$

given by $(A, B) \to AB - BA$ is the full space $\mathcal{O}/2$ of scalar matrices. Hence the image of $\Delta(2^r)/\Delta(2^{r+1})$ certainly contains this subgroup $\mathcal{O}/2$ for $r \geq 2$. With A as above, we deduce that $\Delta(2^r)/\Delta(2^{r+1})$ also contains the image of

$$(I + 2^r A)^2 = I + 2^{r+1} A + 2^{2r} A^2 \mod 2^{r+2}.$$

If $r > 1$, this is $I + 2^{r+1} A \bmod 2^{r+2}$, and since we can choose A to be any element in $M^0(\mathcal{O}/2)$ up to scalars, and we have also showed that the image contains all the scalars, we are done by induction. In the case when $r = 1$, this is $I + 4(A + A^2) \bmod 8$. But now since $A \in M^0(\mathcal{O}/2)$ has trace zero it follows that A^2 is scalar, so just as above we can realize $I + 4A \mod 8$ in the image of $\Delta(4)/\Delta(8)$ for any $A \in M^0(\mathcal{O}/2)$, and we are done. $\square$

Proof of Theorem 1.3. To prove Theorem 1.3, it suffices to show that the conditions of Lemma 3.1 are satisfied. For that, we simply write down some explicit elements first in $\Delta(2) = \Delta(P^e)$ and then in $\Delta(P^r)$ for $r \in [e, \dots, 2e-1]$ and compute their images in $\Delta(P^r)/\Delta(P^{r+1})$. We have, for example, the elements

$$X_{i,j} := (R^i T)^2 (R^j T)^{-2} = I + \frac{2}{\zeta - 1} E \begin{pmatrix} 0 & \zeta(\zeta^{-2i-1} - \zeta^{-2j-1}) \\ \zeta^{2i+1} - \zeta^{2j+1} & 0 \end{pmatrix} E^{-1} \mod 4.$$

where E is the matrix (3) which we remind the reader is 2-adically invertible since the determinant $\zeta - \zeta^{-1}$ is a unit when $m > 1$.

Let us define

$$V_i := R^{mi/2+1/2} T^2 R^{-mi/2-1/2} U^{-2} \in \Delta \tag{7}$$

for any odd integer i (since m is odd, this guarantees that the exponent of R is an integer) and then we find:

$$W_{i,j} := R^{(j-1)/2} V_i R^{-(j-1)/2} \equiv I + 2E \begin{pmatrix} 0 & \zeta^{-j}(\xi^{-i} - 1) \\ \zeta^j(\xi^i - 1) & 0 \end{pmatrix} E^{-1} \mod 4 \tag{8}$$

now with i and j both odd. For both $X_{i,j}$ and $W_{i,j}$, note that the off-diagonal matrices are swapped by the automorphism c sending ζ to ζ^{-1}. If $M_i \in M_2(\mathcal{O}_L)$ is any finite set of matrices, there is the elementary congruence:

$$\prod (I + 2M_i) = I + 2\sum M_i \mod 4. \tag{9}$$

It follows that, by either taking products of $X_{i,j}$ or $W_{i,j}$, we can find elements in Δ of the form

$$A = I + EBE^{-1} \mod 4$$

where B is zero on the diagonal and on the lower left hand corner is given (up to a unit scalar) either by a sum of

$$\zeta^i - \zeta^j$$

where i and j are both odd, or

$$\zeta^j(\xi^i - 1)$$

with i and j both odd. Now let $\mathfrak{p}|2$ in $\mathcal{O}_K$, and let ¶ be a prime in $\mathcal{O}_L$ above $\mathfrak{p}$. Note that there are at most two primes above $\mathfrak{p}$ in $\mathcal{O}_L$, and the other has the form c¶ where c is given by complex conjugation. By Lemma 2.6, we may, depending on the parity of r, find an B such that the lower left corner has any given valuation at ¶ and higher valuation at all other primes. Moreover, since the upper right corner is obtained by acting by complex conjugation, it has the same valuation at c¶ and higher valuation at all other primes. Reverting back to the basis over $\mathcal{O}_K$ and to the matrix A, the fact that E is 2-adically invertible means that since all the entries in the original matrix were trivial modulo $P^r\mathfrak{p}'$ for every prime $\mathfrak{p}'$ except $\mathfrak{p}$ means that $A \in \Gamma(P^r \cdot P/\mathfrak{p})$ and moreover the image of A in $\Gamma(P^r)/\Gamma(P^{r+1})$ is non-zero. Moreover, it is non-scalar as well, since otherwise (conjugating again by E) it would still be scalar, and by construction it is not of this form. It follows that its image in this quotient lies in precisely one copy of Q associated to the factor $\Gamma(P^r)/\Gamma(P^r\mathfrak{p})$. Hence, because Q is irreducible over $\mathbf{F}_2$, we deduce that the image of $\Gamma(P^r)$ contains all d copies of Q, as desired. □

4. The adelic Image

We now turn to computing the adelic image away from the prime $p = 2$. In this section, we now allow $n = 2^k$. The groups $\mathrm{SL}_2(\mathbf{F})$ have no normal subgroups except for the center when $|\mathbf{F}| \geq 5$. Moreover $\mathrm{SL}_2(\mathbf{F})$ and $\mathrm{SL}_2(\mathbf{F}')$ have no isomorphic non-trivial quotients when they are distinct fields of non-equal characteristic.

Lemma 4.1. *Let p be odd. Suppose that $\mathbf{F}_p[\zeta + \zeta^{-1}] = \mathbf{F}$. Then U and T generate $\mathrm{SL}_2(\mathbf{F})$ when $\mathbf{F}$ has odd characteristic with the following exceptions:*

1. *$n = 5 \cdot 3^k$ for some $k \geq 0$ and $p = 3$, in which case the image inside $\mathrm{SL}_2(\mathbf{F}_9)$ for a prime above 3 is isomorphic to the degree 2 central extension of $A_5 \subset A_6 \simeq \mathrm{PSL}_2(\mathbf{F}_9)$.*

(2) $n = 2p^k$ *for some* $k \geq 1$*, in which case the image is cyclic of order* p *generated by the image of* U*.*

Moreover, $\mathrm{PSL}_2(\mathbf{F})$ *is simple unless* $n \in \{3^k, 2 \cdot 3^k, 4 \cdot 3^k\}$*, in which case the image is cyclic of order* 3 *or* $\mathrm{SL}_2(\mathbf{F}_3)$ *depending on whether* n *is twice a prime power or not.*

Proof. Note that the image of U and T are both unipotent and non-trivial unless $2 + \zeta + \zeta^{-1} \equiv 0 \bmod \mathfrak{p}$. The latter implies that $\zeta \equiv -1 \bmod \mathfrak{p}$, and thus that ζ has order exactly 2 in $\mathbf{F}$. But if $n = m \cdot p^k$ where $(m, p) = 1$, then ζ has exact order m, so $m = 2$. Hence we may assume that $2 + \zeta + \zeta^{-1}$ is non-zero and generates $\mathbf{F}$.

Any two such unipotent elements generate $\mathrm{SL}_2(\mathbf{F})$ by a theorem of Dickson [Gor80, Thm 8.4, p.44] unless $|\mathbf{F}| = 9$, in which case one can compute directly that the same claim holds unless $\eta = 2 + \zeta + \zeta^{-1}$ satisfies $\eta^2 + 1 = 0$, in which case the image has order 120 and maps to $A_5 \subset A_6 = \mathrm{PSL}_2(\mathbf{F}_9)$. The condition that $\eta^2 + 1 = 0$ is equivalent to

$$0 = \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2},$$

or equivalently $\zeta^5 - 1 = 0$. This happens if and only if ζ has exact order 5 in characteristic 3, which implies the first result.

The order of the residue field at 3 is, writing $n = m \cdot 3^k$ with $(3, m) = 1$, the order of 3 in $(\mathbf{Z}/m\mathbf{Z})^{\times}/\pm 1$. This has trivial order if and only if $3 \equiv \pm 1 \bmod m$, or when $m \in \{1, 2, 4\}$. □

We now prove the following:

Lemma 4.2. *The closure of the adelic image of* Δ *is the product of the closures of the images in* $\mathrm{SL}_2(\mathcal{O} \otimes \mathbf{Z}_p)$ *for all* p*. Moreover, if* $n \neq 2p^k$ *for some* $k \geq 1$*, then the image in* $\mathrm{SL}_2(\mathcal{O} \otimes \mathbf{Z}_p)$ *for* p *odd is the direct product of the images inside* $\mathrm{SL}_2(\mathcal{O}_{\mathfrak{p}})$ *for all* $\mathfrak{p}|p$*.*

Proof. By Goursat's Lemma, this is automatically true unless the different images have common isomorphic finite quotients. For primes above 2, the image is of dihedral type. For primes above 3, the image is either pro-3 or a quotient of $\mathrm{SL}_2(\mathbf{F})$ for some $\mathbf{F}$ of residue characteristic 3, and any quotient of $\mathrm{SL}_2(\mathbf{F}_3)$ surjects onto $\mathbf{Z}/3\mathbf{Z}$ whereas no quotient of the dihedral group has this property. Other than that, there are no coincidences between $\mathrm{SL}_2(\mathbf{F})$ (or $2.A_5$) between fields of different characteristic. This proves the first claim. For the second, our assumption implies that the image in $\mathrm{SL}_2(\mathbf{F})$ is either $\mathrm{SL}_2(\mathbf{F})$ or the one possible exception inside $\mathrm{SL}_2(\mathbf{F}_9)$. If the image is $\mathrm{SL}_2(\mathbf{F}_3)$, then $n = 3^k$, $2 \cdot 3^k$, or $4 \cdot 3^k$; in each case there is a unique prime above 3 so there is nothing to prove. This also happens when $n = 5 \cdot 3^k$ for primes in $\mathbf{Z}[\zeta + \zeta^{-1}]$ since 3 is inert in $\mathbf{Q}(\sqrt{5})$. Thus we may assume that the residual images of all the p-adic representations is equal to $\mathrm{SL}_2(\mathbf{F})$.

By Goursat's lemma, it suffices to prove that the map to

$$\prod_{\mathfrak{p}} \mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$$

is also surjective. Assume first that $n = mp^k$. Since there is only something to prove when there are at least two primes above p in K, we may also assume that $m \geq 3$. Write $\eta = \zeta^{p^k}$ and let $F \subset K$ be the field $F = \mathbf{Q}(\eta + \eta^{-1})$. Then K/F is totally ramified at all primes above p, we have $\mathcal{O}_F = \mathbf{Z}[\eta + \eta^{-1}]$. For each prime $\mathfrak{p}$ in $\mathcal{O}$ above p, if $\mathfrak{p}_F = \mathfrak{p} \cap \mathcal{O}_F$ then $\mathcal{O}_F/\mathfrak{p}_F = \mathcal{O}/\mathfrak{p}$. In particular, there is a canonical isomorphism of target groups

$$\prod_{\mathfrak{p}|p} \mathrm{SL}_2(\mathcal{O}/\mathfrak{p}) \simeq \prod_{\mathfrak{p}_F|p} \mathrm{SL}_2(\mathcal{O}_F/\mathfrak{p}_F). \tag{10}$$

Since $\zeta^{p^n} \equiv \eta \bmod \mathfrak{p}$, the images of Δ_n and Δ_m coincide (up to conjugation in $\mathrm{Gal}(K/\mathbf{Q})$ by the inverse of $[p^k] \in (\mathbf{Z}/m\mathbf{Z})^{\times}/\pm 1$) after the targets are identified by equation (10). This reduces the claim for Δ_n to the for Δ_m, and thus we may assume that $(n, p) = 1$.

By [Rib75, Lemma 3.3], it suffices to prove the image surjects onto any pair of factors (note that we are in the situation where we may assume that $|\mathbf{F}| \geq 5$ so $\mathrm{SL}_2(\mathbf{F})$ is perfect.) By Goursat's lemma, the result follows unless the image is a graph $(x, \phi(x))$ for some isomorphism $\phi : \mathrm{SL}_2(\mathbf{F}) \to \mathrm{SL}_2(\mathbf{F})$. It follows by considering the image of U and T that ϕ fixes

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Let us examine the image of T in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ and $\mathrm{SL}_2(\mathcal{O}/\sigma\mathfrak{p})$ respectively for a pair of primes $\sigma\mathfrak{p} \ne \mathfrak{p}$. We fix an isomorphism $\mathbf{F} = \mathcal{O}/\mathfrak{p}$, so that the image of $\zeta + \zeta^{-1}$ in $\mathcal{O}/\mathfrak{p}$ is $\zeta + \zeta^{-1}$. The image of $\zeta + \zeta^{-1}$ in $\mathbf{F} = \mathcal{O}/\sigma\mathfrak{p}$ has the form $\sigma^{-1}(\zeta + \zeta^{-1})$ in $\mathcal{O}/\mathfrak{p}$. The assumption that $\mathfrak{p} \ne \sigma\mathfrak{p}$ is the assumption that σ is not in the subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ generated by the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbf{Q})$ (which would mean that $\mathfrak{p} = \sigma\mathfrak{p}$). All automorphisms of $\mathrm{SL}_2(\mathbf{F})$ come from diagonal automorphisms (conjugation by $\mathrm{GL}_2(\mathbf{F})$) and the action of $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$, which is generated by Frobenius. The latter fixes U and preserves the subspace of upper triangular unipotent matrices. The centralizer of U in $\mathrm{GL}_2(\mathbf{F})$ meanwhile consists of the group generated by scalar matrices and lower triangular unipotent matrices. The only such automorphisms which send an upper triangular unipotent matrix to another upper triangular unipotent matrix are trivial. Thus ϕ has to be a Galois automorphism, and thus it must be the case that:

$$\mathrm{Frob}_p^i(\zeta + \zeta^{-1}) \equiv \sigma^{-1}(\zeta + \zeta^{-1}) \mod \mathfrak{p},$$

for some i where $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ is not in the group generated by Frob_p. This is impossible if the minimal polynomial of $\zeta + \zeta^{-1}$ is separated modulo p. But the ring of integers in $\mathbf{Q}(\zeta + \zeta^{-1})$ is $\mathbf{Z}[\zeta + \zeta^{-1}]$, and since we are assuming that ζ has order $(m, p) = 1$, this field is unramified at p, and thus we are done. □

We now have:

Lemma 4.3. *Suppose that p is odd and $(n, p) = 1$. Then the map $\Delta \to \mathrm{SL}_2(\mathcal{O}_\mathfrak{p})$ is surjective.*

Proof. We have seen that the image to $\mathrm{SL}_2(\mathbf{F})$ is surjective. Since p is unramified, the image of T^{p^r} is non-trivial in $\Delta(\mathfrak{p}^r)/\Delta(\mathfrak{p}^{r+1})$ for every $r \ge 1$. If the adjoint representation is irreducible as a representation of $\mathrm{SL}_2(\mathbf{F})$, then the image must be all of $\Delta(\mathfrak{p}^r)/\Delta(\mathfrak{p}^{r+1})$, and then the result follows by induction. To see that the adjoint representation $Q := \Delta(\mathfrak{p})/\Delta(\mathfrak{p}^2)$ is irreducible as an $\mathbf{F}_p[\mathrm{SL}_2(\mathbf{F})]$-module, we may argue as in Lemma 2.4. Namely, $Q \otimes_{\mathbf{F}_p} \mathbf{F}$ decomposes as a direct sum of the $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$-conjugates of the adjoint representation over $\mathbf{F}$, and as long as the traces of elements of $\mathrm{SL}_2(\mathbf{F})$ on this module generate $\mathbf{F}$, the conjugates are all distinct. Any element $\gamma \in \mathbf{F}$ is the trace of a matrix in $\mathrm{SL}_2(\mathbf{F})$, and the trace of the same element on the adjoint representation is $\gamma^2 - 1$. So it suffices to observe that the elements γ^2 for $\gamma \in \mathbf{F}$ generate $\mathbf{F}$ over $\mathbf{F}_p$. □

4.4. **Ramified Primes.** We now deal with (odd) ramified primes. As we have seen, if $n = 2p^k$ and $k \ge 1$, then the mod-$\mathfrak{p}$ representations themselves only have cyclic image, so we defer this case until Section 4.7. We begin with some preliminaries. or any integer $d \ge 2$, we certainly have an exact sequence of groups:

$$0 \to M \to \mathrm{SL}_2(\mathcal{O}/\mathfrak{p}^d) \to \mathrm{SL}_2(\mathbf{F}) \to 0, \tag{11}$$

Letting π be a generator of $\mathfrak{p}/\mathfrak{p}^2$, we may think of elements of M as matrices of the form $1 + \pi A$ with $A \in M(\mathcal{O}/\mathfrak{p}^{d-1})$ (but note that this does not respect the group structure). The group $M = M(\mathfrak{p})$ has an obvious filtration $M(\mathfrak{p}^i)$ and $M^0(\mathbf{F}) \simeq M(\mathfrak{p}^i)/M(\mathfrak{p}^{i+1})$ sending A to $1 + \pi^i A$ which is an isomorphism both of abelian groups and as modules for $\mathbf{F}_p[\mathrm{SL}_2(\mathbf{F})]$.

We first need to understand the structure of the p-group M. Let $\Phi(M) \subset M$ denote the Frattini subgroup (the intersection of all maximal subgroups of M). Since M is a p-group, it has the form $\Phi(M) = [M, M]M^p$, and $M/\Phi(M)$ is elementary p-abelian.

Lemma 4.5. *The Frattini subgroup $\Phi(M)$ is isomorphic to $M(\mathfrak{p}^2)$, so the Frattini quotient $M/\Phi(M)$ is isomorphic to the image of M in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p}^2)$.*

Proof. For $i, j \in 1$, we have:

$$[I + \pi^i A, 1 + \pi^j B] = 1 + \pi^{i+j}(AB - BA) \bmod \pi^{i+j+1}.$$

But since $AB - BA$ generates $M^0(\mathbf{F})$ (assuming as we are that $p > 2$), we see that $[M, M]$ inductively contains $M(\mathfrak{p}^i)$ starting with $i = d$ and descending down to $i = 2$. Hence $\Phi(M) \supseteq [M, M]$ contains this subgroup as well. But $M/M(\mathfrak{p}^2)$ is elementary p-abelian, so $\Phi(M) \subseteq M(\mathfrak{p}^2)$ and thus $\Phi(M) = M(\mathfrak{p}^2)$. $\square$

An alternative way to phrase this is that the Frattini quotient of the pro-p group M which is the kernel of $\mathrm{SL}_2(\mathcal{O}_{\mathfrak{p}}) \to \mathrm{SL}_2(\mathbf{F})$ has $\Phi(M) \simeq M(\mathfrak{p}^2)$, which corresponds to the limit case case $d = \infty$. We now have:

Lemma 4.6. *Let p be an odd prime dividing n. Suppose that n is not of the form $n = 2p^k$ for $k \geq 1$. Then the map $\Delta \to \mathrm{SL}_2(\mathcal{O}_{\mathfrak{p}})$ is surjective, unless $n = 5 \cdot 3^k$ for some $k \geq 0$, in which case the image has index 6.*

Proof. Let us consider the image G of Δ in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p}^d)$ for some integer $d \geq 2$, and let $G(\mathfrak{p})$ be the kernel of the map $G \to \mathrm{SL}_2(\mathbf{F})$. We know, by assumption, that the image of G in $\mathrm{SL}_2(\mathbf{F})$ is either everything or has index 6 in the one exceptional case. But in either case, the adjoint representation is irreducible as an $\mathbf{F}_p[\mathrm{SL}_2(\mathbf{F})]$-module. From Lemma 4.5, there is a map:

$$G(\mathfrak{p}) \hookrightarrow M \to M/\Phi(M) \subset \mathrm{SL}_2(\mathcal{O}/\mathfrak{p}^2).$$

If $G(\mathfrak{p})$ surjects onto $M/\Phi(M)$ then $G \simeq M$ by Burnside's basis theorem [Hal59, Thm 12.2.1]. Since $d \geq 2$ was arbitrary, the result follows. Hence it suffices to show that $G(\mathfrak{p})/G(\mathfrak{p}^2) \subseteq \Gamma(\mathfrak{p})/\Gamma(\mathfrak{p}^2)$ is non-zero, since the adjoint representation is irreducible. In particular, it suffices to write down a single element with non-zero image. Write $n = mp^k$ with $(m, p) = 1$ and $m \neq 2$. Let v denote the valuation on $K_{\mathfrak{p}}$ so that $v(\mathfrak{p} \setminus \mathfrak{p}^2) = 1$. Note that v extends to any finite extension of $K_{\mathfrak{p}}$. If $\gamma \in G(\mathfrak{p}^2)$, then any eigenvalue $\lambda \in \overline{K}$ of γ satisfies

$$v(\lambda - 1) \geq 2. \tag{12}$$

Thus it suffices to write down an element γ which is trivial modulo $\mathfrak{p}$ (so $\gamma \in G(\mathfrak{p})$) and has eigenvalues which do not satisfy (12) so $\gamma \notin G(\mathfrak{p}^2)$. The element R has eigenvalues ζ and ζ^{-1}. If $n = p^k m$ with $m > 2$, then ζ and ζ^{-1} are distinct modulo $\mathfrak{p}$, and thus the reduction of R in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})$ is semisimple. It follows that $\gamma = R^m$ is trivial modulo $\mathfrak{p}$ and has eigenvalues $\zeta^m = \zeta_{p^k}$ and $\zeta_{p^k}^{-1}$. If $m > 2$, then $\mathbf{Q}(\zeta)/\mathbf{Q}(\zeta+\zeta^{-1})$ is unramified at p, and thus $v(\zeta_{p^k} - 1) = 1$. Thus γ gives the desired element, and so we are done unless $m \leq 2$. We are assuming that $m \neq 2$. If $m = 1$, then the reduction of R mod $\mathfrak{p}$ is not semisimple, and hence some alternate argument is required. We now assume that $n = p^k$. There is now a unique prime $\pi = \zeta + \zeta^{-1} - 2$ above p in K with residue field $\mathbf{F}_p$. We use the following *ad hoc* construction. Let $V = RU = UTU$; we will now show that $\gamma = V^{p^2-1}$ lies in $G(\mathfrak{p})$ and is non-trivial in $G(\mathfrak{p})/G(\mathfrak{p}^2)$. We first note that the mod $\mathfrak{p}$ reduction of V is as follows:

$$\overline{V} = \begin{pmatrix} -3 & 4 \\ 2 & -3 \end{pmatrix} \bmod \mathfrak{p}.$$

The element $\overline{V}$ is semisimple because the characteristic polynomial $x^2+6x+1 \in \mathcal{O}/\mathfrak{p}[x]$ is separable (the discriminant is 32 and $p > 2$). Hence the order of $\overline{V} \in \mathrm{SL}_2(\mathbf{F}_p)$ divides p^2-1, and so $\gamma = V^{p^2-1}$ lies in $G(\mathfrak{p})$. Let $\varepsilon = -3 - 2\sqrt{2}$ be a root of $x^2 + 6x + 1 \in K[x]$. We note that $\varepsilon^{p^2-1} \equiv 1 \bmod p$, so $v(\varepsilon^{p^2-1} - 1) \geq e > 1$. The eigenvalues of $\overline{V}$ may be identified with the mod-p reductions of ε and ε^{-1}. Let η be the eigenvalue of V which is congruent to ε modulo $\mathfrak{p}$, and let $\lambda = \eta^{p^2-1}$ be the corresponding eigenvalue of γ, so certainly $v(\lambda - 1) \geq 1$. We claim that if $v(\eta/\varepsilon - 1) = 1$, then $v(\lambda - 1) = 1$. Assume otherwise, so $v(\lambda - 1) > 1$. If $v(\xi - 1) = 1$, then $v(\xi^i - 1) = 1$

for $(i,p)=1$, since $(\xi^i-1)/(\xi-1)=1+\xi+\ldots\xi^{i-1}\equiv i \bmod \mathfrak{p}$. Thus $v(\eta/\varepsilon-1)=1$ implies that

$$\begin{aligned}1 &= v((\eta/\varepsilon)^{p^2-1}-1)=v(\lambda/\varepsilon^{p^2-1}-1)\\ &= v(\lambda-\varepsilon^{p^2-1})-v(\varepsilon^{p^2-1})=v(\lambda-\varepsilon^{p^2-1})\\ &= v\left((\lambda-1)+(1-\varepsilon^{p^2-1})\right)\\ &\geq \min(v(\lambda-1),v(1-\varepsilon^{p^2-1}))\\ &> 1,\end{aligned}$$

since $v(\varepsilon^{p^2-1}-1)>1$ and we are assuming that $v(\lambda-1)>1$. This is a contradiction. Hence if $v(\eta/\varepsilon-1)=1$, then $v(\lambda-1)=1$, and then $\gamma\in\Delta(\mathfrak{p})/\Delta(\mathfrak{p}^2)$ is non-trivial, and we are done. The characteristic polynomial of V, with $\pi=\zeta+\zeta^{-1}-2$, is given by

$$T^2+(6+2\pi)T+1.$$

We now compute that $\eta/\varepsilon-1$ is a root of the polynomial

$$T^2+(6\varepsilon^{-1}+2\varepsilon^{-1}\pi+2)T+2\varepsilon^{-1}\pi=0.$$

The Newton polygon of this polynomial has slopes 0 and 1, from which we deduce that $v(\eta/\epsilon-1)=1$, as desired. □

4.7. **The p-adic image when $n=2p^k$.** We prove the following:

Lemma 4.8. *If $n=2p^k$ with $p>2$ and $k\geq 1$, the closure of Δ in $\mathrm{SL}_2(\mathcal{O}\otimes\mathbf{Z}_p)$ is a p-Sylow subgroup, and the index coincides with the index of p in $\mathrm{SL}_2(\mathbf{F}_p)$, namely p^2-1.*

Proof. When $n=2p^k$ there is a unique prime above p and the residue field is $\mathbf{F}_p$. Our assumptions imply that $\pi=2+\zeta+\zeta^{-1}$ is a uniformizer, and so the image of T in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p})=\mathrm{SL}_2(\mathbf{F}_p)$ is trivial. For any $d\geq 2$, we consider again the exact sequence (11):

$$0\to M\to\mathrm{SL}_2(\mathcal{O}/\mathfrak{p}^d)\to\mathrm{SL}_2(\mathbf{F}_p)\to 0.$$

By Lemma 4.5, the Frattini quotient of M has rank 3 over $\mathbf{F}_p$ and is identified with the image of M in $\mathrm{SL}_2(\mathbf{F}_p[x]/x^2)$. Let N be the preimage of $\langle U\rangle$, so N contains M with index p. When $n=2p^k$, the image G of Δ in $\mathrm{SL}_2(\mathcal{O}/\mathfrak{p}^d)$ is a subgroup of N, since U maps to N by construction and T maps to M. We have the following elements in $G\subset N$ and which are non-trivial in $N/M(\mathfrak{p}^2)$:

$$\begin{aligned}V:=U^{(p+1)}&\equiv\begin{pmatrix}1&0\\1&1\end{pmatrix}\bmod \pi^2,\\ T&=I+\pi\begin{pmatrix}0&1\\0&0\end{pmatrix},\\ VTV^{-1}&\equiv I+\pi\begin{pmatrix}-1&1\\-1&1\end{pmatrix}\bmod\pi^2,\\ V^2TV^{-2}&\equiv I+\pi\begin{pmatrix}-2&1\\-4&2\end{pmatrix}\bmod\pi^2,\end{aligned}\tag{13}$$

but now assuming that $p\neq 2$, as we may, we see that the map $G\cap M\to M/\Phi(M)$ is surjective, and thus (once more) by Burnside's basis theorem, we deduce that $G\cap M=M$, and $G=N$. Since $d\geq 2$ was arbitrary, the result follows. □

5. The 2-adic image when $n=2^k$

To complete our analysis of the image, we need to understand the 2-adic closure Δ_2 of Δ when $n=2^k$ is a power of 2. The arguments will be quite similar to those in Section 3 but sufficiently different to warrant separate consideration. Note that in this case $\mathcal{O}=\mathbf{Z}[\zeta+\zeta^{-1}]$ is totally ramified of degree $e=2^{k-1}$ and in particular there is a single prime $\mathfrak{p}=(\zeta+\zeta^{-1})$ above 2. The matrix E of equation (3) is no longer invertible locally at 2, so we have to work in the original basis. Certainly the image of Δ modulo $\mathfrak{p}$ has order 2, since T is trivial modulo $\mathfrak{p}$. We already know that the image of Δ in $\mathrm{SL}_2(\mathcal{O}/2)$ is isomorphic to $D_{n/2}$. If $J \subset \mathcal{O}$ is a proper ideal, let us define the following congruence subgroup:

$$\Gamma^0(J) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod J.$$

Now if I and J are ideals, let us define

$$\Gamma^0(I, J) = \Gamma(I) \cap \Gamma^0(IJ),$$

in words, matrices which are trivial modulo I but with an additional congruence in the upper right hand corner by a further ideal J. The image of Δ lands inside $\Gamma^0(\mathfrak{p}) = \Gamma^0(1, \mathfrak{p})$. But we observe that the group $\Gamma^0(2, \mathfrak{p})$ is normal in $\Gamma^0(1, \mathfrak{p})$, and $\Gamma^0(2^{r+1}, \mathfrak{p})$ is normal in $\Gamma^0(2^r, \mathfrak{p})$. Moreover, for $r \ge 1$ there is an isomorphism of groups $\Gamma^0(2^r, \mathfrak{p})/\Gamma^0(2^{r+1}, \mathfrak{p}) \simeq M^0(\mathcal{O}/2)$ given explicitly by considering matrices of the form

$$I + 2^r \begin{pmatrix} a+b+c & b(\zeta + \zeta^{-1}) \\ c & a+b+c \end{pmatrix} \tag{14}$$

for $a, b, c \in \mathcal{O}/2$. Let $\widetilde{Q}$ inside this denote the subgroup $(\mathcal{O}/2)^2$ consisting of matrices of the form

$$\begin{pmatrix} b+c & b(\zeta + \zeta^{-1}) \\ c & b+c \end{pmatrix} \tag{15}$$

Then $\widetilde{Q} \simeq (\mathcal{O}/2)^2$ as an abelian group, but is is also preserved by the action of $D_{n/2}$ by conjugation. Moreover, we also have an isomorphism

$$\Gamma^0(2^r, \mathfrak{p})/\Gamma^0(2^{r+1}, \mathfrak{p}) \simeq \mathcal{O}/2 \oplus \widetilde{Q}$$

of $\mathbf{F}_2[D_{n/2}]$-modules. The explicit action on this basis is given as follows: R, T, and U act trivially on $(a, 0, 0)$ and their action on $(0, b, c)$ (by conjugation) satisfies:

$$\begin{aligned} R.(0,b,c) - (0,b,c) &= b(0,0,\zeta+\zeta^{-1}) + c(0,\zeta+\zeta^{-1},(\zeta+\zeta^{-1})^2), \\ U.(0,b,c) - (0,b,c) &= b(0,0,\zeta+\zeta^{-1}), \\ T.(0,b,c) - (0,b,c) &= c(0,\zeta+\zeta^{-1},0) \end{aligned} \tag{16}$$

Lemma 5.1. *$\widetilde{Q}$ is generated as an $\mathbf{F}_2[D_{n/2}]$-module by $(0,1,0)$, and $(0,0,1)$.*

Proof. Note that $\mathcal{O}/2$ is generated as an $\mathbf{F}_2$ module by the powers of $\pi = \zeta + \zeta^{-1}$. But then the result is apparent by applying both U and T to get elements of the form $(0, \pi^i, 0)$ and $(0, 0, \pi^j)$ for any i and j which generate $\widetilde{Q}$. $\square$

Theorem 5.2. *Assume $n = 2^k \ge 4$. The group Δ is a subgroup of $\Gamma^0(\mathfrak{p}) = \Gamma^0(1, \mathfrak{p})$. Moreover:*

1. *The image of Δ in $\Gamma^0(1, \mathfrak{p})/\Gamma^0(2, \mathfrak{p})$ is isomorphic to $D_{n/2}$.*
2. *The image of $\Delta^0(2, \mathfrak{p})$ in $\Gamma^0(2, \mathfrak{p})/\Gamma^0(4, \mathfrak{p})$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus (\mathcal{O}/2)^2$ given by $\widetilde{Q}$ in (15) together with $\pm I$.*
3. *The image of $\Delta^0(4, \mathfrak{p})$ in $\Gamma^0(4, \mathfrak{p})$ is dense.*

In particular, if $n = 2^k$, so K has degree 2^{k-2} and $e = 2^{k-2}$, the index is

$$\begin{aligned} \frac{[\Gamma : \Gamma^0(2, \mathfrak{p})]}{|D_{n/2}|} \cdot \frac{|\mathcal{O}/2|}{2} = \frac{2|\mathrm{SL}_2(\mathcal{O}/2)|}{n} \cdot \frac{|\mathcal{O}/2|}{2} &= \frac{|\mathrm{SL}_2(\mathcal{O}/2)| \cdot |\mathcal{O}/2|}{n} \\ &= \frac{6 \cdot 2^{3e-3} \cdot 2}{n} \cdot 2^{e-1} = \frac{3 \cdot 2^{4e-2}}{n} = 3 \cdot 2^{2^k - k - 2}. \end{aligned}$$

Proof. let us assume that $n \ge 8$. The image of Δ in $\mathrm{SL}_2(\mathcal{O}/2)$ is isomorphic to $D_{n/2}$. As follows from the computation of Section 3, the images of T^2, U^2, and R^d with $d = n/2$ all lie in $\Gamma^0(2, \mathfrak{p})$, and all have the form (15). This proves that the image of Δ in $\Gamma^0(1, \mathfrak{p})/\Gamma^0(2, \mathfrak{p})$ is $D_{n/2}$, and (since matrices of the form (15) together with $-I$ are invariant under conjugation) that the image of $\Delta^0(2, \mathfrak{p})$ in $\Gamma^0(2, \mathfrak{p})/\Gamma^0(4, \mathfrak{p})$ is satisfies the required containment. Hence it suffices to show that the image contains all of this group. On the other hand, the images of $-I$, U^2 and T^2 in this group in the basis of $\mathcal{O}/2 \oplus \widetilde{Q} \simeq (\mathcal{O}/2)^3$ given by (a, b, c) as in equation 14 have the form:

$$(1, 0, 0), (1, 0, 1), (1, 1, 0),$$

and these generate the desired space by Lemma 5.1.

We now turn to showing that the image of $\Delta^0(4, \mathfrak{p})$ in $\Gamma^0(4, \mathfrak{p})$ is dense. The argument will be quite similar to the proof of Lemma 3.1. Consider $I + 2A$ and $I + 2B$ in $\Gamma^0(2, \mathfrak{p})/\Gamma^0(4, \mathfrak{p})$. Then the commutator

$$[I + 2A, I + 2B] = I + 4(AB - BA)$$

is well-defined as an element of $\Gamma^0(4, \mathfrak{p})/\Gamma^0(8, \mathfrak{p})$, and is a scalar matrix. However, this does not generate the entire subspace $\mathcal{O}/2$ of scalar matrices, since the condition that A and B have upper right entry divisible by π implies that the image is the index two subspace $\pi\mathcal{O}/2$. Thus we need to find some more diagonal matrices. To this end, recalling that $R^{n/2} = -I$ and $4|n$, we note that

$$R^{n/4} = \begin{pmatrix} i \cdot \dfrac{1+\zeta}{1-\zeta} & 2i \cdot \dfrac{1+\zeta}{1-\zeta}. \\ 2i \cdot \dfrac{\zeta}{-1+\zeta^2} & -i \cdot \dfrac{1+\zeta}{1-\zeta} \end{pmatrix},$$

where $i = \zeta^{2^{k-2}}$. Note that the entries here still lie in K though this is not transparent from how it is written. From this, we compute further that

$$V = U^2 R^{n/4} U^2 R^{-n/4} = I + 4 \cdot \frac{(1+\zeta)^2}{(1-\zeta)^2} \begin{pmatrix} -1 & -2 \\ 2 + \dfrac{2\zeta}{(1+\zeta)^2} & 5 \end{pmatrix}$$

Certainly the valuation of $1+\zeta$ and $1-\zeta$ are equal. Moreover, the valuation of 2 is greater than the valuation of $(1+\zeta)^2$ since $n = 2^k \geq 8$. Hence the image of V in $\Gamma^0(4, \mathfrak{p})/\Gamma^0(4\mathfrak{p}, \mathfrak{p})$ is a non-trivial scalar.

Now we are ready to prove that $\Delta^0(4, \mathfrak{p})/\Delta^0(8, \mathfrak{p})$ is isomorphic to $\Gamma^0(4, \mathfrak{p})/\Gamma^0(8, \mathfrak{p})$. Take A to be any element in $\widetilde{Q}$, so that we know $I + 2A \in \Delta^0(2, \mathfrak{p})/\Delta^0(4, \mathfrak{p})$. Then we find that

$$(I + 2A)^2 = I + 4A + 4A^2 = 1 + 4B, \quad B \in \mathcal{O}/2 \oplus \widetilde{Q} \tag{17}$$

is a well-defined element of $\Delta^0(4, \mathfrak{p})/\Delta^0(8, \mathfrak{p})$. Moreover, we find that A^2 is scalar. If we take A to be divisible by π, then certainly A^2 is divisible by π, and thus since we have seen above using commutators that everything in $\pi\mathcal{O}/2$ lies in the image of $\Delta^0(4, \mathfrak{p})$ we see that everything in $\pi\mathcal{O}/2 \oplus \pi\widetilde{Q}$ lies in the image. In particular, we are reduced to showing that $\Delta^0(4, \mathfrak{p})$ surjects onto $\Gamma^0(4, \mathfrak{p})/\Gamma^0(4\mathfrak{p}, \mathfrak{p})$. The image of V gives a non-trivial scalar matrix. But now by (17) we see that anything in $\widetilde{Q} \bmod \pi$ lies in the image up to this scalar, and hence everything is in the image. Thus we are done. Now the required identification

$$\Delta^0(2^r, \mathfrak{p})/\Delta(2^{r+1}, \mathfrak{p}) \simeq \Gamma^0(2^r, \mathfrak{p})/\Gamma^0(2^{r+1}, \mathfrak{p})$$

follows from the case $r = 2$ by induction and the fact that for $I + 2^r A \in \Delta^0(2^r, \mathfrak{p})$ we have (now using that $r \geq 2$) that $(I + 2^r A)^2 = I + 2^{r+1} A \in \Delta^0(2^{r+1}, \mathfrak{p})$. Finally it remains to consider the case $n = 4$. In this case, the group Δ_4 is just the group $\Gamma^0(2)$ of finite index 3 inside $\mathrm{SL}_2(\mathbf{Z})$, and the results hold (alternatively one can use the same proof as above after computing any suitable V). ◻

6. The invariants δ and κ

Let us now consider the invariants δ and κ introduced in [McM24]. As previously mentioned, for any cusp $x \in \mathbf{P}^1(K)$, the invariant $\kappa(x)$ is defined to be 0 if x is in the orbit of ∞ under Δ and 1 otherwise. (In particular, if n is odd and there is only one class of cusp, then $\kappa(x)$ always equals zero.) To prove that κ is not a congruence invariant for some even n, it suffices to construct cusps x adelically close to ∞ such that $\kappa(\infty) = 1$. We phrase this more explicitly as follows. Suppose that

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta.$$

Then $\gamma(0) = b/d$ is a cusp equivalent to 0, so to show that κ is non-congruence it suffices to find, for any integer N, an element with $d \equiv 0 \bmod N$, so $[b/d] = [\infty]$ in $\mathbf{P}^1(\mathcal{O}/N)$ but $\kappa(b/d) = 1$.

The second invariant δ is defined as follows. Let $n' = n$ if n is odd and $n/2$ otherwise. (The integer n' was denoted by m in [McM24] but that conflicts with our notation.) The image of Δ in $\mathrm{SL}_2(\mathcal{O}/2)$ is identified with $D_{n'} = \langle r, t\rangle \subset \mathrm{Sym}(\mathbf{Z}/m)$, where $r(x) = x + 1$ and $t(x) = -x$. The cusps of Δ are given by the coset $\Delta/\langle T\rangle$, and the map $\Delta \to \mathrm{SL}_2(\mathcal{O}/2)$ sending T to $t \in D_{n'}$ maps $\Delta/\langle T\rangle$ to $D_{n'}/\langle t\rangle$, and then the latter is identified with $\mathbf{Z}/n'\mathbf{Z}$ by sending g to $g(0)$. In [McM24], one can further extend δ to the cusps equivalent to 0, but we have no need to discuss this here. Note that δ extends to a map on Δ itself by

$$\delta(\gamma) = \delta(\gamma(\infty)).$$

As noted in [McM24], the map $\delta \mod 2$ is a homomorphism but δ is not a homomorphism in general. The map δ on Δ clearly only depends on the congruence class of $\gamma \in \Delta$. However, as a map on cusps, this is no longer necessarily true. To show (for a particular even integer n) that δ is not a congruence invariant of the cusps, it suffices to find, for any integer N, a $\gamma \in \Delta$ such that:

(1) $\gamma \equiv R^i \bmod 2$ where $i \not\equiv 0 \bmod n' = n/2$.
(2) The cusp $\gamma(\infty) = [a : c]$ is equal to $[1 : 0] \in \mathbf{P}^1(\mathcal{O}/N)$, equivalently, that $c \equiv 0 \bmod N$.

The point is that the first condition implies that $\delta(\gamma(\infty)) = i \bmod n/2$. Since (by [McM24, Cor 1.]) the invariant 2δ *is* congruence, this should only be possible if $4|n$ and $i = n/4 \bmod n/2$. Note that by the proof of [McM24, Theorem 1.13], it indeed suffices to find such a γ for N any power of 2, although we don't need to use this fact.

Theorem 6.1. *The map $\delta \mod 2^{k-1}$ is a not a congruence invariant if $n = 2^k m$ where $k \geq 2$ and $m > 1$ is odd.*

Proof. We begin by considering the element

$$\gamma_1 := R^{2^{k-2}m} \equiv I + \begin{pmatrix} i-1 & 0 \\ 0 & i-1 \end{pmatrix} \mod 2.$$

Note that $n/4 = 2^{k-2}m$. By construction, we therefore have

$$\delta(R^{2^{k-2}m}) \equiv n/4 \bmod n/2.$$

Since δ on Δ depends only on the image in $\Delta/\Delta(2) \subset \mathrm{SL}_2(\mathcal{O}/2)$, it follows that any lift of this element has this property. We now consider $\gamma_1 = R^{n/4} \mod 4$. By Theorem 1.3 (we are assuming n is not a power of 2), we can inductively find η_r in $\Delta(2^r)/\Delta(2^{r+1})$ so that $\gamma_{r+1} := \eta_r\gamma_r \bmod 2^{r+1}$ also has zero in the lower left corner. Inductively, we construct a limit point $\gamma_\infty \in \widehat{\Delta}_2$ with a zero in the lower left hand corner. Similarly, we deduce from Theorem 1.2 that we may find $\gamma_\infty \in \widehat{\Delta}$ with the same property. (The condition that $4|n$ implies that the closure of the image away from 2 is everything.) Now take any $\gamma \in \Delta$ which is congruent to γ_∞ modulo N for any integer N, we deduce that $\gamma(\infty) = [a : c]$ reduces to ∞ in $\mathbf{P}^1(\mathcal{O}/N)$, but $\delta(a/c) = \delta(\gamma) = n/4 \bmod n/2$, and hence δ is not a congruence invariant modulo N for any integer N. $\square$

We now turn to κ. We begin with a preliminary lemma.

Lemma 6.2. *Assume that $n = 2m$ where m is odd. There exists an element γ_∞ in the closure of Δ in $\mathrm{SL}_2(\mathcal{O} \otimes \mathbf{Z}_2)$ of the form*

$$\begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \bmod 2^k.$$

Proof. We proceed by induction. Since $n \equiv 2 \mod 4$, we may take $i = (n+2)/4$ and then

$$\gamma_1 = R^i = \frac{1}{\zeta^i(1-\zeta^2)} \begin{pmatrix} (1+\zeta)(\zeta^{2i}-\zeta) & (1+\zeta)^2(1-\zeta^i)^2 \\ \zeta(\zeta^i-1)^2 & \zeta(1+\zeta)(\zeta^{2i}-\zeta^{-1}) \end{pmatrix}.$$

Since $m > 1$, the leading factor is a unit. But $\zeta^{2i-1} = \zeta^{n/2} = -1$, so $\zeta^{2i} - \zeta \equiv 0 \bmod 2$. Hence γ_1 is such an element modulo 2. We now consider $\gamma_1 \bmod 4$. By Theorem 1.3 (we are assuming n is not a power of 2), we can adjust $\gamma_1 \bmod 4$ by any element η_1 in $\widetilde{Q}$, which have the form:

$$\begin{pmatrix} b+c & b(\zeta+\zeta^{-1}) \\ c & b+c \end{pmatrix}$$

In particular, since we can choose $b + c \in \mathcal{O}/2$ to be anything. we can ensure that $\gamma_2 = \eta_1\gamma_1$ has a 0 in the first entry. Just as in the proof of Theorem 6.1, we proceed by induction to find the required element γ_∞. □

Theorem 6.3. *The function κ is not a congruence invariant if $n = 2m$ where m is odd and divisible by at least two prime factors.*

Proof. We claim that for any integer N, there exists a $\gamma \in \Delta$ such that

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \bmod N.$$

By Theorem 1.2, it suffices to show that this can be achieved when N is any prime power. By Theorem 1.2 and the assumption that n has at least three prime factors, it follows that $\widehat{\Delta}_p = \widehat{\Gamma}_p$, and hence contains the image of Δ contains the element

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

modulo any power of an odd prime p. On the other hand, by Lemma 6.2, there exists an element of the required form modulo any power of 2, which proves the claim. But that means that the cusp $\gamma(\infty) = (a, c) \in \mathbf{P}^1(\mathcal{O}/N)$ maps to the image of 0 in $\mathbf{P}^1(\mathcal{O}/N)$, and so κ is not a congruence invariant modulo N. Since this holds for any integer N, we are done. □

References

[Gor80] Daniel Gorenstein, *Finite groups*, second ed., Chelsea Publishing Co., New York, 1980. MR 569209

[Hal59] Marshall Hall, Jr., *The theory of groups*, The Macmillan Company, New York, 1959. MR 103215

[McM22] Curtis T. McMullen, *Billiards, heights, and the arithmetic of non-arithmetic groups*, Invent. Math. **228** (2022), no. 3, 1309–1351. MR 4419633

[McM23] ———, *Billiards in regular polygons*, 2023.

[McM24] ———, *Triangle groups: cusps, congruence and chaos*, 2024.

[Rib75] Kenneth A. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275. MR 419358

Email address: fcale@math.uchicago.edu

The University of Chicago, 5734 S University Ave, Chicago, IL 60637, USA