hexagon:2611.01028v2

ORBIT CLOSURES OF SCALENE RATIONAL TRIANGLES: EVERY DENOMINATOR

MANVIR JASWAL

Abstract. Delecroix and Rüth conjectured that, apart from an explicit list, the unfoldings of rational triangles and quadrilaterals without a reflection symmetry have dense $\mathrm{GL}(2,\mathbb{R})$-orbits in their ambient strata, and proved this for the triangles with angles $p_i\pi/N$ and $N \leq 58$. We prove the conjecture for triangles. If a scalene rational triangle is not on their list of three infinite families and nine triangles, the orbit closure of its unfolding is the connected component of its stratum when N is odd, and the locus of holonomy double covers of a connected component of a stratum of quadratic differentials when N is even. With the first paper of this series, it follows that the orbit is not dense in that locus for the triangles on the list, except possibly for the triangle with angles $(3\pi/20, \pi/5, 13\pi/20)$. Most of the proof concerns subgroups of the units modulo N; parts of it, including all of $N \leq 58$, are computer-assisted.

Contents

1. Introduction 1
2. The setting 7
3. Closed sets and witnesses 17
4. Triangles without a witness 22
5. Smaller conductors 27
6. Families without a witness and an angle $2\pi/3$ 33
7. An angle $\pi/3$ 43
8. Small denominators and the proof of the main theorem 60
9. Billiards in the triangle 62
Declarations 64
References 64

1. Introduction

A rational triangle $\Delta = (p_1, p_2, p_3)/N$ has angles $p_i\pi/N$, where p_1, p_2, p_3 are positive integers with $\gcd(p_1, p_2, p_3) = 1$ and $N = p_1 + p_2 + p_3$; it is *scalene* if the p_i are distinct. The billiard in Δ unfolds to a translation surface (X, ω) [36], which we take with the points of cone angle 2π unmarked, as in Part I [19, §2.1]. By Eskin, Mirzakhani and Mohammadi [12, 13] the closure $\mathcal{M}$ of its $\mathrm{GL}(2,\mathbb{R})$-orbit is an affine invariant submanifold: near (X, ω) it is, in period coordinates, an open subset of a complex linear subspace V of $H^1(X, \Sigma; \mathbb{C})$,

Date: November 24, 2026.
2020 *Mathematics Subject Classification.* Primary 37C83; Secondary 32G15, 30F30, 11A07.
Key words and phrases. Rational billiards, translation surfaces, orbit closures, affine invariant submanifolds.

This paper is Part II of a series on orbit closures of unfoldings of rational polygons: Parts I [19] and II treat triangles, Part III [18] quadrilaterals and Part IV [17] polygons with at least five sides.

where Σ is the set of zeros of ω, and its rank is half the dimension of the image $p(V)$ of V in $H^1(X;\mathbb{C})$. The surface X is the normalization of the curve

$$y^N = x^{p_1}(x-1)^{p_2}, \qquad \omega = \frac{y\,dx}{x(x-1)},$$

and $T(x,y) = (x,\zeta y)$, $\zeta = e^{2\pi i/N}$, has $T^*\omega = \zeta\omega$ [28, §6]. For scalene $\Delta \neq (1,2,3)/6$ the powers of T are the only automorphisms of X that multiply ω by a constant [19, Theorem 6.2]. For even N, $\iota = T^{N/2}$ has $\iota^*\omega = -\omega$, so that ω^2 is the pull-back of a quadratic differential q on the quotient X/ι.

Let Δ be scalene. We call the following locus $\mathcal{L}$ the *ambient locus* of Δ. For odd N it is the connected component of the stratum of (X,ω) that contains (X,ω). For even N it is the locus of holonomy double covers of the surfaces in the connected component of the stratum of quadratic differentials that contains $(X/\iota, q)$. In both cases $\mathcal{M} \subset \mathcal{L}$, and $\mathcal{L}$ is the component through (X,ω) of what Delecroix and Rüth call the ambient stratum of Δ [10, §§1 and 4].

Delecroix and Rüth proved with the flatsurf software that for every scalene triangle with $N \leq 58$ the orbit of the unfolding is dense in its ambient stratum, except for the triangles

$$\begin{gathered}(1,2,2k+1)/(2k+4)\ (k\geq 2), \quad (1,k,k+1)/(2k+2)\ (k\geq 3),\\ (2,2k+1,2k+3)/(4k+6)\ (k\geq 1), \quad (1,4,7)/12, \quad (2,3,4)/9, \quad (3,4,5)/12, \quad (3,5,7)/15,\\ (1,3,6)/10, \quad (1,3,8)/12, \quad (1,4,11)/16, \quad (1,4,15)/20, \quad (3,4,13)/20\end{gathered} \tag{1.1}$$

[10, Theorem 4.1], and they conjecture that the list of exceptions in their Theorems 4.1 and 4.2, for triangles and quadrilaterals, is complete [10, §4]. With $k-2$ for k, the first family is $(1,2,2k-3)/2k$, $k \geq 4$, as [19, Theorem 1.1] writes it; there $(1,k,k+1)/(2k+2)$ starts at $k=2$, since $(1,2,3)/6$, whose unfolding is a torus, has rank one. The three families and the next four triangles of (1.1) are lattice triangles, found by Veech, Vorobets, Ward, Kenyon and Smillie, and Hooper [30, 31, 32, 33, 23, 15]; $(1,3,6)/10$ and $(1,3,8)/12$, found in Delecroix and Rüth's search and listed by them as of rank one, have rank one [19, Theorem 1.1]; and $(1,4,11)/16$ and $(1,4,15)/20$ have rank two, their orbit closures being loci found by Eskin, McMullen, Mukamel and Wright [11, Theorem 1.1], [19, Proposition 8.10]. Delecroix and Rüth name as partial results [10, §4] Mirzakhani and Wright's infinite family of triangles with dense orbits in components of strata [28, Theorem 1.4], Larsen, Norton and Zykoski's proof that, outside six families, the triangles with an obtuse angle above $2\pi/3$ are not lattice triangles [26], and Apisa's determination of the orbit closures of all rational right and isosceles triangles [2, Theorems 7.6 and 7.7]. Part I determined the scalene triangles of rank one [19, Theorem 1.1] and proved the conjecture for prime N [19, Theorem 1.2]. We prove it for triangles; quadrilaterals are not treated here.

Theorem 1.1. *Let Δ be a scalene rational triangle that is not in* (1.1)*. Then the* $\mathrm{GL}(2,\mathbb{R})$*-orbit closure of its unfolding is its ambient locus.*

For $N \leq 58$ it is Delecroix and Rüth's theorem, and for right triangles it is Apisa's [2, Theorem 7.6].

The proof reads the rank of the orbit closure off a set S of characters of T, which the rules of Part I make closed under three operations; Theorem 1.1 asks that S be as large as the ambient locus allows. The new step is a translation: if the triangle has a witness, a unit x with $2x \not\equiv 2 \pmod N$ for which T^* has holomorphic eigenforms of characters x and $2-x$, one rule gives $H + (x-1) = xH$ when S is a group H of units and every $h + x - 1$,

$h \in H$, lies in the set F of characters that the ambient locus allows; summing this identity modulo the primes of N shows that H then contains a nontrivial group of units congruent to 1 modulo a divisor of N, at every N. The rules alone can stop short on some triangles with an angle $\pi/3$ or $2\pi/3$ and on three families without a witness; there we use the geometry of the unfolding: relative periods at the vertex of an angle $2\pi/3$, and cylinders in explicit models otherwise. Many of the cases are proved in a supplement of 148 pages, a separate document accompanying this paper, whose sections are numbered S1–S8; Table 1 lists what it proves.

The proof is about characters of T. For $a \in \mathbb{Z}/N$ let H^1_a be the ζ^a-eigenspace of T^* on $H^1(X;\mathbb{C})$, let $[m] \in \{0,\dots,N-1\}$ be the residue of an integer m, and

$$\Phi = \{a \in \mathbb{Z}/N : \ ap_1, ap_2, ap_3 \not\equiv 0 \text{ and } [ap_1]+[ap_2]+[ap_3] = N\}.$$

By the dimension formula for cyclic covers [28, Corollary 6.2], H^1_a is a line if $ap_i \not\equiv 0$ for $i = 1,2,3$, spanned by a holomorphic form ω_a when $a \in \Phi$, and is zero otherwise [19, Lemma 2.1]. As $T^*V = V$,

$$p(V) = \bigoplus_{a\in S} H^1_a, \qquad \operatorname{rank}\mathcal{M} = \tfrac{1}{2}|S|, \tag{1.2}$$

for a set S of characters with $\pm 1 \in S$ [19, Lemma 2.4]. Let F be the set of $a \in \mathbb{Z}/N$ with $ap_1, ap_2, ap_3 \not\equiv 0$, and odd if N is even. Then $S \subset F$; for even N this holds because V lies in the (-1)-eigenspace of ι^* [19, Corollary 6.3]. The ambient locus has rank $|F|/2$, so the next theorem says that $\mathcal{M}$ has the rank of $\mathcal{L}$.

Theorem 1.2. *Let $N > 58$ and let Δ be a scalene rational triangle that is not in (1.1). Then $S = F$.*

For odd N this says $p(V) = H^1(X;\mathbb{C})$, so $\mathcal{M}$ is a connected component of a stratum or the hyperelliptic locus in one, by Mirzakhani and Wright [28, Theorem 1.1]; their Lemma 6.7 excludes the second, as N is odd and the angles are distinct. For even N, Theorem 1.7 below gives $\mathcal{M} = \mathcal{L}$. So Theorem 1.2 proves Theorem 1.1 for $N > 58$. With Part I it decides, for all but one scalene triangle, whether the orbit is dense in its ambient locus.

Corollary 1.3. *Let Δ be a scalene rational triangle other than $(3,4,13)/20$. The orbit closure of its unfolding is its ambient locus if and only if Δ is not in (1.1).*

Indeed, for the triangles of (1.1) other than $(3,4,13)/20$, $|S|$ is 2 or 4 by the results of Part I quoted above, while $|F| \geq \varphi(N) \geq 4$, and $|F| = 8$ for $(1,4,11)/16$ and $(1,4,15)/20$. For $(3,4,13)/20$ the ambient locus is $\widetilde{\mathcal{Q}}_4(11,1)$, of dimension 8; Delecroix and Rüth prove that $\mathcal{M}$ has dimension at least 4 and conjecture that it has dimension 4 and field of definition $\mathbb{Q}(\sqrt{5})$ [10, Theorem 1.2 and Conjecture 1.1], and Delecroix announces a positive answer to this conjecture, from joint work with Kai Fu [6, pp. 48–49]; his slides of June 2025, on joint work with K. Fu and B. Zykoski, list this orbit closure with dimension 4, rank 2 and field of definition $\mathbb{Q}(\sqrt{5})$ [7, slide 12]. With Apisa's Theorems 7.6 and 7.7 [2], this leaves $(3,4,13)/20$ as the only rational triangle whose orbit closure is not known.

For the finite blocking problem, Theorem 1.1 gives that two finitely blocked points of a scalene triangle not in (1.1), other than $(1,2,3)/6$, are the same vertex (Corollary 9.1).

1.1. **Closed sets and witnesses.** Part I proves three rules for S [19, Lemma 3.4 and Theorem 1.5]. We call a set $C \subset F$ *closed* if

(i) $C = -C$;

(ii) for every unit u modulo N, if $C \cap uC \neq \emptyset$, then $uC = C$;
(iii) for every unit u, every $a \in uC \cap \Phi$ and every $a' \in C$, if $b = 1 - a - a'$ lies in Φ, then $b \in uC$.

So S is a closed set containing 1. Rule (iii) with $u = a = x$ and $a' = -1$ puts $2 - x$ in xS for every unit x with $x, 2 - x \in \Phi$. Such an x with $2x \not\equiv 2$ is a *witness* [19, §1.1], and for a witness this is Mirzakhani and Wright's criterion for rank at least two [28, Theorem 7.5].

Let $G = (\mathbb{Z}/N)^\times$ and, for $m \mid N$, $K_m = \{u \in G : \ u \equiv 1 \pmod m\}$ and $H_m = \{u \in G : \ u \equiv \pm 1 \pmod m\}$. For a closed set $C \ni 1$, rule (ii) makes the *unit part* $H = C \cap G$ a subgroup of G containing -1, and the elements a of C with $\gcd(a, N) = d$, if there are any, form one orbit Ha, which forces $K_{N/d} \subset H$. We call the least $m \mid N$ with $K_m \subset H$ the *conductor* of H. It divides N', where $N' = N/2$ if $N \equiv 2 \pmod 4$ and $N' = N$ otherwise, and if it equals N', then $C = H$ (Lemma 2.7). The subgroup containing -1, the groups $K_{N/d}$ and the pairs $x, 2 - x$ go back to Mirzakhani and Wright [28, Lemmas 7.6, 7.12 and 7.13]. Their criterion for full rank [28, Theorem 7.14] asks for every unit in S and for every class of non-units to be linked to the units by such pairs; with rule (iii), the first alone gives $S = F$ once $N > 30$ (Theorem 1.5 below).

For $N > 58$ off (1.1), $\mathcal{M}$ has rank at least two [19, Theorem 1.1], so $|S| \geq 4$, and then the unit part of S is not $\{\pm 1\}$ (Lemma 2.7). If it has conductor 1, it is G, and $S = F$ by Theorem 1.5. So Theorem 1.2 asks to show that the conductor is 1, and the main step is to exclude N'. A witness does this, at every N.

Theorem 1.4. *Let Δ be a scalene rational triangle that has a witness. Then the unit part of every closed set containing 1 contains K_f for some $f \mid N$ with $K_f \neq \{1\}$; equivalently, its conductor is a proper divisor of N'.*

The idea is a translation. Let $C \ni 1$ be closed with unit part H of conductor N', so that $C = H$, and let x be a witness and $d = x - 1$. Rule (iii) with $u = a = x$ and $a' = -1$ puts $2 - x$ in xH; so $2 - x$ is a unit, and $\rho = (2 - x)/x$ lies in H, with $\rho \neq 1$ as $2x \not\equiv 2$. Let $h \in H$ with $h + d \in F$. One of $\pm(h + d)$ lies in Φ, and rule (iii) with $(u, a, a') = (x, x, h)$, where $b = -(h + d)$, or with $(u, a, a') = (2 - x, 2 - x, -h)$, where $b = h + d$, puts b in xH or in $(2 - x)H = xH$, so $h + d \in xH$ as $-1 \in H$. If $h + d \in F$ for every $h \in H$, the injective map $h \mapsto (h + d)/x$ of H to itself therefore gives

$$H + (x - 1) = xH. \tag{1.3}$$

Reduce (1.3) modulo an odd prime $\ell \mid N$ and sum over the image $\bar{H}$ of H in $(\mathbb{Z}/\ell)^\times$. The elements of $\bar{H}$ cancel in pairs $\pm h$, so $|\bar{H}|(x - 1) \equiv 0$, and $\ell \mid x - 1$. Hence $\rho \equiv 1$ modulo every odd prime of N, and modulo 4 when $4 \mid N$, as x is then odd. Every subgroup of the group of units $\equiv 1$ modulo these numbers is some K_f, since that group is a product of cyclic groups of coprime prime-power orders, one for each prime of N. So $\langle \rho \rangle = K_f \neq \{1\}$ lies in H, and the conductor N' of H divides f; but $K_f = \{1\}$ for $f = N'$ and $f = N$, a contradiction. If $(h + d)p_i \equiv 0$ for some $h \in H$ and some i, the map $h \mapsto (h + d)/x$ still sends the other elements of H into H. The exceptional h then form one coset of a subgroup of H when N is even, and at most three cosets when N is odd; sums of powers of degree at most three modulo the primes involved, and the translations of the groups $H \cap K_m$ that the map induces, still give a non-trivial K_f in H (Section 3.2).

Triangles without a witness have been classified: the acute and right ones in Part I [19, Theorem 1.7 and Proposition 10.1], the obtuse ones with obtuse angle at most $2\pi/3$ in [16, Theorem 4.1(a)], and those with a larger obtuse angle by Larsen, Norton and Zykoski [26,

Theorem 4.1]. For $N > 58$ and off (1.1), the scalene ones without an angle $2\pi/3$ lie in ten families (Section 4), such as $(1, (N-d)/2-1, (N+d)/2)/N$ with $d \mid N$ and $N/d \geq 5$ odd. On most of them rule (iii) with $a' \neq -1$ excludes the conductor N'; on the others we show $S = F$ directly (Section 6).

A conductor c with $1 < c < N'$ is excluded by counting holomorphic units in the classes modulo c and by explicit pairs on which rule (iii) acts (Section 5), except that when $12 \mid c$ the unit part may contain $H_{12} = \{u \in G : \ u \equiv \pm 1 \pmod{12}\}$; for $N > 58$, a closed set whose unit part contains H_{12} is F unless Δ has an angle $\pi/3$ or $2\pi/3$ (Section 4).

The rules alone do not always suffice. If $12 \mid N$ and Δ has an angle $\pi/3$ or $2\pi/3$, the set of $a \in F$ with $a \equiv \pm 1 \pmod{12}$ is closed and is not F (Section 2), and on the three families $(1, N/2-2, N/2+1)/N$ with $4 \mid N$, $(2, N/4-1, 3N/4-1)/N$ with $8 \mid N$ and $(4, N/4-2, 3N/4-2)/N$ with $N \equiv 4 \pmod 8$ the group $\{\pm 1, \pm(1+N/2)\}$ is closed. There we use the geometry of the unfolding. For an angle $2\pi/3$ we use relative periods (Theorem 1.6) at the vertex of that angle. For an angle $\pi/3$ we use cylinders: if the units in S were exactly those $\equiv \pm 1 \pmod{12}$, the ratios of the circumferences of $\mathcal{M}$-parallel cylinders would lie in $\mathbb{Q}(\sqrt{3})$, and Wright's cylinder deformation theorem [35] would give some of them a negative conjugate; we find cylinders that admit no such partner (Section 7). The triangles of these three families have explicit cylinder decompositions that give $\mathcal{M}$ the rank of $\mathcal{L}$ (Section 6).

1.2. **Two tools.** Two tools hold well beyond the range of Theorem 1.2, and we state them in that generality. The first completes a closed set once it has all units.

Theorem 1.5. *Let Δ be a rational triangle, isosceles or not, with $N > 30$, and let C be a set with $G \subset C \subset F$ that satisfies rules (ii) and (iii). Then $C = F$.*

For $N \leq 30$ the conclusion fails on exactly eleven triangles, at $N = 12$, 18, 24 and 30, where the characters a with $\gcd(a, N) = 3$ can be missing (Section 2). Once $C \supset G$, rule (iii) is needed only with $u = 1$, and the theorem is a statement about the divisors of N and the holomorphic characters in each class.

The second is a rule for relative periods. Let $Z = \ker p$ and Z_c its ζ^c-eigenspace. For $c \not\equiv 0$, Z_c is a line if c is a multiple of $N/\gcd(p_i, N)$ for a vertex i whose preimages are zeros of ω, and zero otherwise [19, Lemma 2.2].

Theorem 1.6. *Let Δ be scalene, $\Delta \neq (1,2,3)/6$, let u be a unit, $x \in uS \cap \Phi$ and $a \in S$, and suppose that $c = a + x - 1$ is not 0 and that $Z_c \neq 0$. Then $Z_{u^{-1}c} \subset V$.*

The proof follows that of the rule of Part I [19, Theorem 1.5], with relative classes in place of absolute ones. The form ω_x extends to a family of holomorphic forms on the surfaces of $\mathcal{M}$ near (X, ω) whose absolute classes stay in the Galois conjugate $\sigma_u(p(V))$, and by Filip's splitting theorem [14, Theorem 4.2] their relative classes then stay in $\sigma_u(V)$. If $Z_{u^{-1}c} \not\subset V$, a form of character $-c$ with simple poles at the zeros above vertex i is orthogonal to $\sigma_u(V)$, and differentiating its pairing with the family along V contradicts Kahn and Wright's derivative formula [22, Theorem 1.1], in the form [19, Lemma 3.1]. Applied with $u = 1$, once $S = F$, to every odd c with $Z_c \neq 0$, it gives:

Theorem 1.7. *Let N be even and Δ scalene, $\Delta \neq (1,2,3)/6$. If $\operatorname{rank} \mathcal{M} = \operatorname{rank} \mathcal{L}$, then $\mathcal{M} = \mathcal{L}$.*

Remark 1.8. Mirzakhani and Wright asked whether every affine invariant submanifold of such a locus of double covers that has the rank of the locus is the whole locus [28, §1, Question (A)]. As they note, the answer is negative in general, by the work of Eskin, McMullen, Mukamel

and Wright [11]; Theorem 1.7 answers it for the orbit closures of unfoldings of scalene triangles. When $\operatorname{rank}\mathcal{L} \geq g/2+1$, with g the genus of X, Theorem 1.7 also follows from Apisa and Wright's classification [4, Theorem 1.1]: $\mathcal{M}$ is then a connected component of a stratum, and $\mathcal{M} \subset \mathcal{L}$ gives $\mathcal{M} = \mathcal{L}$, or the locus of all holonomy double covers of the surfaces in a stratum of quadratic differentials, which is that of $(X/\iota, q)$ because the covering involution is ι [19, Theorem 6.2].

1.3. **The proof.** Let $N > 58$ and let Δ be scalene and not in (1.1). We prove Theorem 1.2 in the first of the following cases that applies.

(1) *N is prime.* This is [19, Theorem 1.2].
(2) *An angle $2\pi/3$.* Then $\Delta = (p, N/3-p, 2N/3)/N$. The lines Z_c above the vertex $2N/3$ are those with c a non-zero multiple of 3. Theorem 1.6 puts some of them in V, the derivative formula turns each of these into a further rule for S, and with (i)–(iii) these rules force $S = F$ (Section 6).
(3) *$12 \mid N$ and an angle $\pi/3$.* Cylinders put every unit in S (Section 7), and $S = F$ by Theorem 1.5.
(4) *The three families above.* Cylinder decompositions give $S = F$ (Section 6).
(5) *$N = 2^j$, $2P$ or $3P$ with P prime.* Every closed set containing 1 with at least four elements is F (Section 5).
(6) $N \leq 400$. We find that every closed set containing 1 with at least four elements is F (Section 8).
(7) $N > 400$. Let H be the unit part of S and c its conductor; $H \neq \{\pm 1\}$, as $|S| \geq 4$. If Δ has a witness, $c \neq N'$ by Theorem 1.4. If not, Δ is in one of the families of Section 4; on each, $c \neq N'$ or $S = F$ (Section 6), apart from sixteen triangles with $N \leq 2{,}000$, on which we find that no subgroup $H \neq \{\pm 1\}$ of conductor N' is closed (Section 8). If $1 < c < N'$, then $12 \mid c$ and $H \supset H_{12}$ (Section 5), and then $S = F$ (Section 4). Otherwise $c = 1$, $H = G$, and $S = F$ by Theorem 1.5.

For $N \leq 58$, Section 8 proves Theorem 1.1 again, to show what the rules reach on their own: with the classification of rank one in Part I they settle 3,896 of the 4,019 scalene triangles off (1.1), cylinder deformations 120 more and families of cyclic covers two; the one left, $(1, 2, 3)/6$, unfolds to a flat torus.

Section 2 sets up the characters and the ambient locus, proves Theorems 1.5, 1.6 and 1.7 and describes closed sets. Section 3 proves Theorem 1.4, Section 4 lists the triangles without a witness, and Section 5 treats the smaller conductors and the denominators 2^j, $2P$ and $3P$. Sections 6 and 7 use the geometry of the unfolding, and Section 8 treats the small denominators and completes the proofs. Section 9 draws the consequence for billiards. The remaining cases of Sections 5, 6 and 7 and the denominators $N \leq 58$ are proved in the supplement, at the places listed in Table 1.

1.4. **Computations.** Finite computations enter the proofs: the closed sets for $58 < N \leq 400$, the sixteen triangles of case (7), the finite part of Theorem 1.5, finite ranges inside some arguments of Sections 5, 6 and 7, and the triangles with $N \leq 58$. Each fact is stated where it is used. The programs are in C, Python and Sage. They compute with integers, rationals and exact arithmetic in cyclotomic fields; where a decision depends on the sign of a real number, it is made in ball arithmetic [21] or in fixed-point arithmetic with a proved error bound, and the linear programs are solved exactly over $\mathbb{Q}$. For the cylinders we follow Delecroix and Rüth's procedure for bounding orbit closures from below [10, §3], with the flatsurf software

statement	section
Proposition 4.7(a), the list of $B^\sharp$	§S8
Theorems 5.3 and 5.6	§S7
Propositions 5.8, 5.9 and 5.10	§S1
Theorem 6.1	§S2
Theorems 6.12 and 6.13	§S3
Theorems 6.17, 6.18, 6.19, 6.20 and 6.21	§S4
Propositions 7.9, 7.23, 7.24, 7.25, 7.26 and 7.27, and two steps of Section 7.5	§S5
Theorem 8.1	§S6

TABLE 1. The statements proved in the supplement, with its sections.

[8, 9] in Sage, and compute in the number field of each surface. The programs, their output and instructions for rerunning them are deposited [20].

2. The setting

This section proves Theorems 1.5, 1.6 and 1.7 and collects what the later sections use: the elementary structure of closed sets, a rule for relative characters, and two lemmas, one on cylinders and one on residues, that the arguments by cases apply many times. We keep the notation of Part I [19, §2].

2.1. **Notation.** Let $\Delta = (p_1, p_2, p_3)/N$, with vertex i of angle $p_i\pi/N$, and $g_i = \gcd(p_i, N)$; the g_i are pairwise coprime. For a real t, $\{t\}$ is its fractional part. Above vertex i the unfolding has g_i points, of cone angle $2\pi p_i/g_i$, which form one orbit of T; I is the set of vertices with $p_i \nmid N$, Σ_i the set of points above $i \in I$, and $\Sigma = \bigcup_{i\in I} \Sigma_i$ the zero set of ω [19, §2.1]. For $\ell \in \mathbb{Z}/N$, $H^1(X,\Sigma)_\ell$ is the ζ^ℓ-eigenspace of T^* on $H^1(X,\Sigma;\mathbb{C})$. By Lemmas 2.1 and 2.2 of Part I:

- if $ap_i \not\equiv 0$ for $i = 1, 2, 3$, then H^1_a is a line, exactly one of a and $-a$ lies in Φ, $\Phi \cup -\Phi$ is the set of such a, and every unit lies in it; for $a \in \Phi$ the line is spanned by a holomorphic form $\omega_a = y^a x^{-i_a}(x-1)^{-j_a}\,dx$, with integers i_a, j_a, that vanishes to order $[ap_i]/g_i - 1$ at each point above vertex i, and $\omega_1 = \omega$;
- if $a \not\equiv 0$ and $ap_i \equiv 0$ for some i, then this i is unique and $H^1_a = 0$; also $H^1_0 = 0$;
- for $c \not\equiv 0$, Z_c is a line if $(N/g_i) \mid c$ for some $i \in I$, the *vertex* of c, which is then unique, and $Z_c = 0$ otherwise; Z_c is spanned by $\delta e_{i,c}$, where $e_{i,c}$ is the function on Σ equal to ζ^{ck} at $T^k z_i$ for a fixed $z_i \in \Sigma_i$ and to 0 off Σ_i; and $H^1(X,\Sigma)_a$ maps isomorphically onto H^1_a for $a \in \Phi \cup -\Phi$.

So at odd N, $F = \Phi \cup -\Phi$; at even N, F is the set of odd elements of $\Phi \cup -\Phi$. We call a character a *generic* if $a \in \Phi \cup -\Phi$ (then H^1_a is a line) and *holomorphic* if $a \in \Phi$. Let R be the set of $c \not\equiv 0$ with $Z_c \neq 0$. For $c \in R$ with vertex i we have $cp_i \equiv 0$, so $c \notin \Phi \cup -\Phi$, and $H^1(X,\Sigma)_c = Z_c$.

Near (X,ω), in period coordinates, $\mathcal{M}$ is a single linear subspace: there are a ball U about $[\omega]$ and $V = T_{(X,\omega)}\mathcal{M}$ with $\mathcal{M} \cap U = V \cap U$ [19, §2.3]. By Lemma 2.4 of Part I, $V = \bigoplus_\ell V_\ell$ with $V_\ell = V \cap H^1(X,\Sigma)_\ell$, and $V_a = H^1(X,\Sigma)_a$ for $a \in S$. We write $\langle\cdot,\cdot\rangle$ for the perfect pairing between $H^1(X,\Sigma;\mathbb{C})$ and $H^1(X\setminus\Sigma;\mathbb{C})$ given by $\langle[\nu],[\theta]\rangle = \int_X \nu\wedge\theta$;

it is T-invariant, so it pairs $H^1(X,\Sigma)_\ell$ with the $\zeta^{\ell'}$-eigenspace $H^1(X\setminus\Sigma)_{\ell'}$ to zero unless $\ell+\ell'\equiv 0$, and $\langle \delta f,[\theta]\rangle = -2\pi i\sum_{z\in\Sigma} f(z)\operatorname{Res}_z\theta$ for a meromorphic form θ holomorphic on $X\setminus\Sigma$ [19, §3.1].

The rules do not leave F: in rule (iii), $b\in\Phi$, and at even N the characters a and a' are odd, so b is odd. So F is closed, an intersection of closed sets is closed, and every subset of F lies in a smallest closed set, its *closure*. For scalene $\Delta\neq(1,2,3)/6$, whose unfolding has genus at least two [19, §2], Lemma 3.4 and Theorem 1.5 of Part I, and its Corollary 6.3 at even N, show that S is closed and contains the closure of $\{1\}$.

Lemma 2.1. *The set $\{\pm1\}$ is closed if and only if Δ has no witness.*

Proof. Rules (i) and (ii) hold for $\{\pm1\}$. In rule (iii), $a\in u\{\pm1\}$ means $a=\pm u$, so $u\{\pm1\}=\{\pm a\}$; for $a'=1$, $b=-a$ lies in it, and for $a'=-1$, $b=2-a$ lies in it if and only if $2a\equiv 2$, as $2-a\equiv -a$ would give $N\mid 2$. So the rule fails exactly when some unit a has $a,2-a\in\Phi$ and $2a\not\equiv 2$. □

2.2. **The ambient locus.** Let N be even and Δ scalene, $\Delta\neq(1,2,3)/6$. By Theorem 6.2 of Part I, ι is the only automorphism of X with $\iota^*\omega=-\omega$, and by its Corollary 6.3, $V\subset E^-$, where

$$E^- = \{v\in H^1(X,\Sigma;\mathbb{C}):\ \iota^*v=-v\} = \bigoplus_{\ell\text{ odd}} H^1(X,\Sigma)_\ell,$$

as ι^* acts on $H^1(X,\Sigma)_\ell$ by $\zeta^{\ell N/2}=(-1)^\ell$. For odd ℓ, $H^1(X,\Sigma)_\ell$ is the line over H^1_ℓ if $\ell\in F$ and is Z_ℓ otherwise, so

$$E^- = \bigoplus_{a\in F} H^1(X,\Sigma)_a \ \oplus \bigoplus_{c\in R\text{ odd}} Z_c, \qquad p(E^-)=\bigoplus_{a\in F} H^1_a. \tag{2.1}$$

Let $\mathcal{Q}$ be the component of the stratum of quadratic differentials that contains $(X/\iota,q)$, so that $\mathcal{L}=\widetilde{\mathcal{Q}}$ is the locus of holonomy double covers of its surfaces, an affine invariant submanifold [3, §1]. The fixed points of ι off Σ lie over the poles of q and are regular points of ω, unmarked on X. The double cover of the image of $(X/\iota,q)$ under $g\in\mathrm{GL}(2,\mathbb{R})$ is $g(X,\omega)$, so $\mathcal{M}\subset\mathcal{L}$. Lanneau's chart [25, §1.1.1] identifies a neighborhood of $(X/\iota,q)$ in $\mathcal{Q}$, by the double-cover map, with an open subset of the (-1)-eigenspace of ι^* in the cohomology of X relative to the preimages of all zeros and poles of q. The preimage of a pole is one point z fixed by ι, and forgetting it removes the class $\delta 1_z$, which is ι-invariant; so the (-1)-eigenspaces agree, and the chart is a linear isomorphism onto an open subset of E^-. As ι is the only involution of its kind, $\mathcal{L}$ is this one sheet near (X,ω), and by (2.1) $\operatorname{rank}\mathcal{L}=\frac12\dim p(E^-)=|F|/2$.

Lemma 2.2. *Let N be even and Δ scalene, $\Delta\neq(1,2,3)/6$. If $V=E^-$, then $\mathcal{M}=\mathcal{L}$.*

Proof. Let $f\colon\mathcal{Q}\to\mathcal{L}$ be the double-cover map and B the set of $y\in\mathcal{Q}$ such that f maps a neighborhood of y into $\mathcal{M}$. It is open, and it contains $(X/\iota,q)$, since near (X,ω) both $\mathcal{M}$ and the image of Lanneau's chart are $E^-\cap U$. It is closed: let $y_n\in B$ tend to y. As $\mathcal{M}$ is closed, $f(y)\in\mathcal{M}$, and near $f(y)$ the set $\mathcal{M}$ is a finite union of linear subspaces through $f(y)$ in period coordinates [12, 13] (read at a lift if $f(y)$ is an orbifold point, as in [19, §2.3]). Take a connected neighborhood W of y on which f is a linear chart and whose image lies in the domain of that description. For large n, $f(W)\cap\mathcal{M}$ contains a non-empty open subset of $f(W)$; by Baire one of the subspaces contains a non-empty open subset of the affine image $f(W)$, hence all of $f(W)$, and $y\in B$. As $\mathcal{Q}$ is connected, $B=\mathcal{Q}$, so $\mathcal{L}=f(\mathcal{Q})\subset\mathcal{M}\subset\mathcal{L}$. □

2.3. **Relative periods.** We use Filip's splitting theorem [14, Theorem 4.2] in the following form. Wright's decomposition [34, Theorem 1.5] of the flat bundle H^1 over $\mathcal{M}$ has, for each embedding ρ of the field of definition $k(\mathcal{M})$, a summand $V_\rho = \sigma(V_{\mathrm{Id}})$, where σ is any automorphism of $\mathbb{C}$ extending ρ, acting on cohomology through the coefficients, and V_{Id} has fiber $p(V)$ at (X,ω) [19, §2.4]. Filip's theorem, stated for every embedding, says that the relative class of a holomorphic form whose absolute class lies in the fiber of V_ρ lies in the fiber of the conjugate $\sigma(T\mathcal{M})$ of the tangent bundle. On $\mathcal{M}\cap U = V\cap U$ the tangent space is the constant subspace V, so there the fiber of $\sigma(T\mathcal{M})$ is $\sigma(V)$. For a unit u, Lemma 2.5 of Part I gives $\sigma_u(p(V)) = \bigoplus_{a\in uS} H^1_a$, the fiber of the summand with $\rho = \sigma_u|_{k(\mathcal{M})}$, where $\sigma_u(\zeta) = \zeta^u$.

Proof of Theorem 1.6. The proof of the rule of Part I [19, Theorem 1.5] differentiates the absolute class of a holomorphic form that stays in $\sigma_u(p(V))$; we differentiate its relative class, which by Filip's theorem stays in $\sigma_u(V)$, against a form with simple poles.

As T^* and p are defined over $\mathbb{Q}$, σ_u maps $H^1(X,\Sigma)_\ell$ onto $H^1(X,\Sigma)_{u\ell}$ and Z_ℓ onto $Z_{u\ell}$. Let $V^u = \sigma_u(V)$; then $V^u_c = \sigma_u(V_{u^{-1}c})$. Here $c\in R$, and $u^{-1}c\in R$ with the same vertex i_0, so $H^1(X,\Sigma)_{u^{-1}c} = Z_{u^{-1}c}$ is a line, and $V^u_c = 0$ unless $Z_{u^{-1}c}\subset V$. Suppose that $Z_{u^{-1}c}\not\subset V$. Then $V^u_c = 0$, and every class of $H^1(X\setminus\Sigma)_{-c}$ vanishes on $V^u = \bigoplus_\ell V^u_\ell$.

For $j = 1,2,3$ let $t_j = 0$ if $j = i_0$ and $t_j = \{-cp_j/N\}$ otherwise. Since $cp_{i_0}\equiv 0$ and $cp_j\not\equiv 0$ for $j\neq i_0$, the two non-zero t_j have sum 1, so $t_1+t_2+t_3 = 1$, and we may choose integers k,l with $k - cp_1/N + 1 = t_1$ and $l - cp_2/N + 1 = t_2$. Let

$$\eta = y^{-c}x^k(x-1)^l\,dx.$$

At a point above vertex j it vanishes to order $(N/g_j)t_j - 1$ (above ∞ the exponent is fixed by the sum $t_1+t_2+t_3 = 1$), which is -1 for $j = i_0$ and $[-cp_j]/g_j - 1\geq 0$ otherwise. So η is holomorphic on $X\setminus\Sigma$, has simple poles at the points of Σ_{i_0}, and $[\eta]\in H^1(X\setminus\Sigma)_{-c}$.

As $x\in uS\cap\Phi$, the fiber of $V_\rho\cap H^{1,0}$ at $[\omega]$ contains ω_x; let α_ϖ, $\varpi\in V\cap U$, be a holomorphic section through ω_x of the bundle $V_\rho\cap H^{1,0}(X_\varpi)$, which is C^1 along every path $[\omega]+tv$, $v\in V$, as forms on the fixed surface [19, proof of Lemma 3.5]. By Filip's theorem $[\alpha_\varpi]_{\mathrm{rel}}\in V^u$, so $\langle[\alpha_\varpi]_{\mathrm{rel}},[\eta]\rangle = 0$ on $V\cap U$. Let $v\neq 0$ in V_a, a line as $a\in S$. Differentiating along v and applying the derivative formula [19, Lemma 3.1], which allows simple poles,

$$0 = \langle\partial_v[\alpha_\varpi]_{\mathrm{rel}},[\eta]\rangle = \langle v,[\Theta]\rangle,\qquad \Theta = \omega_x\eta/\omega = y^{x-1-c}x^{k'}(x-1)^{l'}\,dx$$

for some integers k',l'. The form Θ is holomorphic off Σ, and $x-1-c\equiv -a$ with $a\in\Phi\cup-\Phi$, so its class in $H^1(X\setminus\Sigma)_{-a}$ is not zero [19, Lemma 3.2]. This eigenspace is a line [19, proof of Lemma 3.3], as is $V_a = H^1(X,\Sigma)_a$, and the pairing between them is perfect; so $\langle v,[\Theta]\rangle\neq 0$, a contradiction. □

With $u = 1$ and c odd the hypotheses of Theorem 1.6 can be met whenever $S = F$:

Lemma 2.3. *Let N be even, $c\in R$ odd with vertex i_0, and $m = N/g_{i_0}$. Then $m\geq 3$ is odd, an odd a lies in $\Phi\cup-\Phi$ if and only if $m\nmid a$, and there is an odd $b\in\Phi$ with $m\nmid b$ and $m\nmid c+1-b$.*

Proof. For odd a and any j, $ap_j\equiv 0$ if and only if $(N/g_j)\mid a$, which needs N/g_j odd, that is, g_j divisible by the 2-part of N; this holds for at most one j, as the g_j are coprime, and holds for i_0, as $(N/g_{i_0})\mid c$. So m is odd, $m\neq 1$ as $g_{i_0}\leq p_{i_0} < N$, and an odd a lies in $\Phi\cup-\Phi$ if and only if $m\nmid a$. For odd b, $m\mid c+1-b$ if and only if $b\equiv 1 \pmod{2m}$.

If $m\geq 5$, one of ± 3 lies in Φ, and neither is divisible by m or $\equiv 1 \pmod{2m}$. Let $m = 3$. The points above i_0 are zeros, so $p_{i_0}\geq 2g_{i_0} = 2N/3$, and $p_{i_0} = 2N/3$; let $p+q = N/3$ be

the other two numerators. Every $b \equiv 5 \pmod 6$ is odd and prime to 3, has $[bp_{i_0}] = N/3$ and $b \not\equiv 1 \pmod 6$, and lies in Φ if and only if $[bp] + [bq] = 2N/3$ rather than $5N/3$, which holds if $[bp] < 2N/3$. As b runs over the class of 5 modulo 6, bp runs over a coset of the subgroup generated by $D = \gcd(6p, N)$, which has an element in $(0, D]$. As $\gcd(p, N)$ is prime to $g_{i_0} = N/3$, it divides 3, so $D \le 18 < 2N/3$ once $N \ge 30$. For $N < 30$ the scalene triangles with even N and a numerator $2N/3$ are $(1,3,8)/12$, $(1,5,12)/18$, $(1,7,16)/24$ and $(3,5,16)/24$, and $b = 5$ lies in Φ on each. □

Proof of Theorem 1.7. By (1.2) and (2.1), $\operatorname{rank} \mathcal{M} = \operatorname{rank} \mathcal{L}$ and $S \subset F$ give $S = F$, so $V \supset \bigoplus_{a \in F} H^1(X, \Sigma)_a$. Let $c \in R$ be odd, and take b as in Lemma 2.3. Then $b \in F \cap \Phi$ and $a = c + 1 - b \in F$, so Theorem 1.6 with $u = 1$ and $x = b$ gives $Z_c \subset V$. By (2.1), $V \supset E^-$; as $V \subset E^-$, $V = E^-$, and Lemma 2.2 gives $\mathcal{M} = \mathcal{L}$. □

Corollary 2.4. *Let Δ be scalene, $\Delta \ne (1,2,3)/6$. If $S = F$, then $\mathcal{M} = \mathcal{L}$.*

Proof. For odd N this is the deduction after Theorem 1.2. For even N, $\operatorname{rank} \mathcal{M} = |F|/2 = \operatorname{rank} \mathcal{L}$, and Theorem 1.7 applies. □

Theorem 1.6 puts relative directions into V. The derivative formula turns such a direction into a rule for S, with residues in place of the pairing of absolute classes. Let $\mathcal{C} = \{c \in R : Z_c \subset V\}$.

Proposition 2.5. *Let Δ be scalene, $\Delta \ne (1,2,3)/6$, let u be a unit and $c \in \mathcal{C}$ with vertex i, and let $x \in uS \cap \Phi$ with $[xp_i] < p_i$. If $b = 1 - x - c$ lies in Φ, then $b \in uS$.*

Proof. Suppose $b \notin uS$. Lemma 3.5 of Part I gives a holomorphic family α_ϖ on $\mathcal{M} \cap U$ with $\alpha_{[\omega]} = \omega_x$ and $\langle \partial_v [\alpha_\varpi]_{\mathrm{rel}}, [\omega_b] \rangle = 0$ for every $v \in V$. Take $v = \delta e_{i,c} \in Z_c \subset V$. By the derivative formula with $\theta = \omega_b$ and the residue form of the pairing,

$$0 = \langle \delta e_{i,c}, [\Psi] \rangle = -2\pi i \sum_{z \in \Sigma_i} e_{i,c}(z) \operatorname{Res}_z \Psi, \qquad \Psi = \omega_x \omega_b / \omega.$$

As $T^*\Psi = \zeta^{x+b-1}\Psi = \zeta^{-c}\Psi$, $\operatorname{Res}_{T^k z_i} \Psi = \zeta^{-ck} \operatorname{Res}_{z_i} \Psi$, and the sum is $g_i \operatorname{Res}_{z_i} \Psi$. At z_i the forms ω_x, ω_b and ω vanish to orders $[xp_i]/g_i - 1$, $[bp_i]/g_i - 1$ and $p_i/g_i - 1$, so Ψ has order $([xp_i] + [bp_i] - p_i)/g_i - 1$, and a non-zero residue if $[xp_i] + [bp_i] = p_i$. This holds: $cp_i \equiv 0$ gives $bp_i \equiv p_i - xp_i$, and $p_i - [xp_i]$ lies in $[1, p_i - 1]$. So the residue is not zero, a contradiction. □

So, besides rules (i)–(iii) for S, the pair $(S, \mathcal{C})$ satisfies two rules on scalene triangles other than $(1,2,3)/6$:

(iv) if u is a unit, $x \in uS \cap \Phi$, $a \in S$ and $c = a + x - 1 \in R$, then $u^{-1}c \in \mathcal{C}$;

(v) if u is a unit, $c \in \mathcal{C}$ has vertex i, $x \in uS \cap \Phi$ has $[xp_i] < p_i$ and $b = 1 - x - c \in \Phi$, then $b \in uS$.

2.4. **Closed sets.** For $d \mid N$, $d < N$, let $O_d = \{a \in \mathbb{Z}/N : \gcd(a, N) = d\}$, so that $O_1 = G$. The group G acts transitively on O_d with stabilizer $K_{N/d}$. Whether $a \in O_d$ lies in $\Phi \cup -\Phi$ depends only on d, as $ap_i \equiv 0$ if and only if $(N/d) \mid p_i$; so $O_d \subset F$ or $O_d \cap F = \emptyset$, and at even N, $O_d \subset F$ needs d odd.

Lemma 2.6. *Let $C \subset F$ satisfy rules (i) and (ii), with $1 \in C$, and let $H = C \cap G$. Then H is a subgroup of G containing -1, and $H = \{u \in G : uC = C\}$. For $d \mid N$, $d < N$, the set $C \cap O_d$ is empty or one orbit Ha_d, and then $K_{N/d} \subset H$. Conversely, for every subgroup $H \ni -1$ of G, every set D of divisors $d > 1$ of N with $O_d \subset F$ and $K_{N/d} \subset H$, and every choice of $a_d \in O_d$, the set $H \cup \bigcup_{d \in D} Ha_d$ satisfies rules (i) and (ii) and has unit part H.*

Proof. For $s \in H$, $s = s \cdot 1 \in C \cap sC$, so $sC = C$; hence H is closed under products, so a subgroup, and $-1 \in H$ by rule (i). If $uC = C$, then $u = u \cdot 1 \in C \cap G$. For $a, b \in C \cap O_d$ choose a unit u with $b = ua$; then $b \in C \cap uC$, so $u \in H$. For $u \in K_{N/d}$ and $a \in C \cap O_d$, $ua = a \in C \cap uC$, so $u \in H$. Conversely, the set is stable under $-1 \in H$; if it meets its image under a unit u, then, as u preserves each O_d and $d > 1$ keeps the orbits Ha_d off G, either $u \in H$ directly or $hua_d = h'a_d$ for some $h, h' \in H$, and then $h'^{-1}hu \in K_{N/d} \subset H$. □

By the Chinese remainder theorem $K_m K_{m'} = K_{\gcd(m,m')}$, since a unit modulo $\operatorname{lcm}(m, m')$ lifts to a unit modulo N; so the conductor of a subgroup is well defined, and $K_m \subset H$ if and only if the conductor divides m. Also $K_m = \{1\}$ if and only if $m = N$ or $m = N'$: at each prime ℓ of N the kernel of reduction from $(\mathbb{Z}/\ell^e)^\times$ to $(\mathbb{Z}/\ell^f)^\times$, $e = v_\ell(N)$, $f = v_\ell(m)$, is trivial only for $f = e$, or for $\ell = 2$, $e = 1$.

Lemma 2.7. *Let $C \ni 1$ be closed, with unit part H of conductor f. Then $f \mid N'$; if C meets O_d, then $f \mid N/d$; and if $f = N'$, then $C = H$. If $H = \{\pm 1\}$ and $N \notin \{3, 4, 6\}$, then $f = N'$ and $C = \{\pm 1\}$.*

Proof. $K_{N'} = \{1\} \subset H$, so $f \mid N'$. If C meets O_d, then $K_{N/d} \subset H$ by Lemma 2.6. If $f = N'$ and $d > 1$, then $N' \mid N/d$, which forces $N' = N/2$ and $d = 2$, and no element of F is even. If $H = \{\pm 1\}$, then $K_f \subset \{\pm 1\}$. Here $-1 \in K_f$ only for $f \in \{1, 2\}$, where $K_f = G \neq \{\pm 1\}$ as $N \notin \{3, 4, 6\}$; so $K_f = \{1\}$, and $f = N'$. □

The next proposition is why the triangles with an angle $\pi/3$ or $2\pi/3$ need the geometry of the unfolding.

Proposition 2.8. *Let $12 \mid N$ and let Δ have a numerator $N/3$ or $2N/3$. Then $S_+ = \{a \in F : \ a \equiv \pm 1 \pmod{12}\}$ is closed and differs from F.*

Proof. Every $a \in F$ is prime to 6: it is odd, and at the vertex with numerator $\kappa N/3$, $\kappa \in \{1, 2\}$, $3 \mid a$ would give $ap_i \equiv 0$. Let χ be the character of $(\mathbb{Z}/12)^\times$ with kernel $\{\pm 1\}$; then $\chi(ua) = \chi(u)\chi(a)$, and $uS_+ = \{a \in F : \ \chi(a) = \chi(u)\}$. Rules (i) and (ii) follow. For rule (iii), let $a \in uS_+ \cap \Phi$, $a' \in S_+$ and $b = 1 - a - a' \in \Phi$; we need $\chi(b) = \chi(a)$. If $a' \equiv 1 \pmod{12}$, then $b \equiv -a$. If $a' \equiv -1$, then $b \equiv 2 - a$, which is divisible by 3 if $a \equiv 5, 11 \pmod{12}$, impossible for $b \in F$, and is $\equiv a$ if $a \equiv 1, 7$. Some unit is $\equiv 5 \pmod{12}$, and it is not in S_+. □

2.5. **Proof of Theorem 1.5.** Let Δ be any rational triangle and C as in Theorem 1.5, but with any $N \geq 3$. Every unit u lies in $C \cap uC$, so $uC = C$: C is a union of orbits O_d, and rule (iii) is needed only for $u = 1$: if $x, a' \in C$ and $x, 1 - x - a' \in \Phi$, then $1 - x - a' \in C$. Let $\mathcal{D}$ be the set of $d \mid N$ with $1 < d < N$ and $O_d \subset F$, so that $F = G \sqcup \bigsqcup_{d \in \mathcal{D}} O_d$.

Lemma 2.9. *Let $d \in \mathcal{D}$. If there are $x \in G \cap \Phi$ and $b \in O_d \cap \Phi$ with $1 - x - b \in G$, then $O_d \subset C$. This holds if there are $x \in G$ and $b \in O_d$ such that the four numbers $1 \pm x \pm b$ are units.*

Proof. The rule with $a' = 1 - x - b \in G \subset C$ puts b in C, and $O_d = Gb$. For the second statement replace x and b by $\pm x$ and $\pm b$ in Φ. □

The case $3 \nmid N$. Let $d \in \mathcal{D}$. By the Chinese remainder theorem it suffices to choose, for each prime $\ell \mid N$, residues $\bar{x} \neq 0$ and $\bar{b}$ modulo ℓ, with $\bar{b} = 0$ if and only if $\ell \mid d$, such that $1 \pm \bar{x} \pm \bar{b} \neq 0$; then $x \in G$ and $b \in O_d$ with these residues exist. For $\ell = 2$ there is nothing to choose, as x and b are odd. For $\ell \geq 5$ and $\ell \mid d$ we need $\bar{x} \notin \{0, \pm 1\}$, which leaves $\ell - 3$ choices. For $\ell \geq 5$ and $\ell \nmid d$, each of the four lines $\bar{x} \pm \bar{b} = \pm 1$ contains $\ell - 2$ points with

both coordinates non-zero, so at least $(\ell-1)^2-4(\ell-2)=(\ell-3)^2$ pairs remain. Lemma 2.9 gives $C=F$.

The case $3 \mid N$. Here the sign that puts a unit into Φ can decide its class modulo 3. For $d \in \mathcal{D}$ let L_d be the set of primes $\ell \geq 5$ dividing d, $r_d = 2$ if $3 \mid d$ and $r_d = 1$ otherwise, and C_d the set of units $x \equiv r_d \pmod 3$ with $x \not\equiv 1 \pmod \ell$ for $\ell \in L_d$; it is not empty.

Lemma 2.10. *If $C_d \cap \Phi \neq \emptyset$, then $O_d \subset C$.*

Proof. Let $x \in C_d \cap \Phi$. Choose $b \in O_d$ with $b \not\equiv \pm(1-x) \pmod \ell$ for every prime $\ell \geq 5$ with $\ell \nmid d$, and replace b by $\pm b \in \Phi$. Then $1-x-b$ is a unit: it is odd if N is even; modulo 3 it is $1-2-0 \equiv -1$ if $3 \mid d$ and $-b \not\equiv 0$ if $3 \nmid d$; modulo $\ell \in L_d$ it is $1-x \not\equiv 0$; and modulo the other $\ell \geq 5$, $b \not\equiv 1-x$. Lemma 2.9 applies. □

For $j = 1, 2, 3$ let $N_j = N/g_j$ and $q_j = p_j/g_j$, a unit modulo N_j. As g_i and g_j are coprime, $\operatorname{lcm}(N_i, N_j) = N$ for $i \neq j$.

Lemma 2.11. *Let $C' \subset G$ be non-empty and defined by conditions on x modulo some primes dividing N, and let $C'_j \subset (\mathbb{Z}/N_j)^\times$ be defined by the conditions at the primes dividing N_j. Then*

$$|\Phi \cap C'| = \tfrac{1}{2}|C'|\,(1 + a_1 + a_2 + a_3), \qquad a_j = \frac{1}{|C'_j|}\sum_{w \in C'_j}\Big(1 - 2\Big\{\frac{wq_j}{N_j}\Big\}\Big).$$

Proof. For a unit x, $\sum_j \{xp_j/N\}$ is 1 or 2, and is 1 exactly when $x \in \Phi$; so $s(x) = 3 - 2\sum_j \{xq_j/N_j\}$ is 1 on Φ and -1 off it, and $|\Phi \cap C'| = \sum_{x \in C'}(1+s(x))/2$. The j-th term of s depends on x modulo N_j, and reduction modulo N_j maps the uniform measure on C' to the uniform measure on C'_j, prime by prime. □

Lemma 2.12. *Write $((t)) = \{t\} - \frac{1}{2}$ for real t, and let μ be the Möbius function and $\omega(m)$ the number of primes dividing m.*

(a) *For integers $M \geq 1$ and a and a real θ, $\sum_{k=0}^{M-1}((\theta + ak/M)) = g\,((M\theta/g))$, where $g = \gcd(a, M)$.*

(b) *Let $q \mid n$, let γ be a unit modulo q and a an integer, and for each divisor d of n prime to q let y_d be an integer with $y_d \equiv \gamma d^{-1} \pmod q$, and $g_d = \gcd(a, n/(qd))$. Then*

$$\sum_{\substack{y \in (\mathbb{Z}/n)^\times \\ y \equiv \gamma \pmod q}} \Big(\Big(\frac{ay}{n}\Big)\Big) = \sum_{\substack{d \mid n \\ \gcd(d,q)=1}} \mu(d)\, g_d\Big(\Big(\frac{ay_d}{qg_d}\Big)\Big).$$

For $a = 1$ the right-hand side is $\sum_d \mu(d)((y_d/q))$, which depends on n only through its set of primes.

Proof. (a) Write $a = ga'$ and $M = gM'$. As k runs over $[0, M)$, $a'k$ runs g times over the residues modulo M', so the sum is $g\sum_{j=0}^{M'-1}((\theta + j/M'))$, and Hermite's identity $\sum_{j=0}^{M'-1}\{\theta + j/M'\} = \{M'\theta\} + (M'-1)/2$ makes this $g((M'\theta))$.

(b) A residue $y \equiv \gamma \pmod q$ is prime to the primes of q, so it is a unit if and only if no prime of n outside q divides it. By Möbius inversion the left-hand side is $\sum_d \mu(d)\Sigma_d$ over the divisors d of n prime to q, where Σ_d is the sum of $((ay/n))$ over the residues $y \equiv \gamma \pmod q$ with $d \mid y$. These are $y = d(y_d + qk)$, $0 \leq k < M = n/(qd)$, and $ay/n = ay_d/(qM) + ak/M$; by (a), $\Sigma_d = g_d((ay_d/(qg_d)))$. For $a = 1$, $g_d = 1$, and the d with $\mu(d) \neq 0$ are the products of distinct primes of n not dividing q. □

With $C' = C_d$ and $y = wq_j$, a_j is the average of $1 - 2y/n$ over a set

$$Y = \{y \in (\mathbb{Z}/n)^\times : \ y \equiv \gamma \pmod 3 \text{ if } 3 \mid n, \ y \not\equiv e_\ell \pmod \ell \text{ for } \ell \in E\},$$

with $n = N_j$, y read in $[0, n)$, $\gamma \equiv r_d q_j$, E the set of primes of L_d dividing N_j, and $e_\ell \equiv q_j$. For $n \geq 2$, a set E of primes ≥ 5 dividing n and non-zero residues γ, e_ℓ, write $\alpha(n; \gamma, E, e)$ for this average and $A^*(n)$ for the largest value of $-\alpha$ over all such data; so $a_j \geq -A^*(N_j)$.

Lemma 2.13. *With $((t))$ as in Lemma 2.12,*

$$\sum_{y \in Y} \Big(\Big(\frac{y}{n}\Big)\Big) = \sum_{\delta \mid \prod E} (-1)^{\omega(\delta)} \sum_{e' \mid R_\delta} \mu(e') \Big(\Big(\frac{t_{\delta,e'}}{q_\delta}\Big)\Big),$$

where $[3 \mid n]$ is 1 if $3 \mid n$ and 0 otherwise, $q_\delta = 3^{[3|n]}\delta$, $R_\delta = \operatorname{rad}(n)/q_\delta$, γ_δ is the residue modulo q_δ that is $\equiv \gamma \pmod 3$ if $3 \mid n$ and $\equiv e_\ell \pmod \ell$ for $\ell \mid \delta$, and $t_{\delta,e'} \equiv \gamma_\delta e'^{-1} \pmod{q_\delta}$. Also $|Y| = \varphi(n)\, 2^{-[3|n]} \prod_{\ell \in E} (\ell - 2)/(\ell - 1)$. In particular $A^*(n) = (\operatorname{rad}(n)/n)\, A^*(\operatorname{rad}(n))$.

Proof. Inclusion and exclusion over the excluded classes gives the outer sum, each of whose terms is the sum of $((y/n))$ over the units y in the class γ_δ modulo q_δ; Lemma 2.12(b) with $a = 1$ and $q = q_\delta$ gives this sum, the d with $\mu(d) \neq 0$ there being the divisors e' of R_δ. The size of Y is the count of the Chinese remainder theorem. The sum depends on n only through $\operatorname{rad}(n)$, and $|Y|$ is proportional to $\varphi(n) = (n/\operatorname{rad} n)\varphi(\operatorname{rad} n)$. □

Lemma 2.14. *For squarefree $\rho \geq 2$ and all data,*

$$|\alpha(\rho; \gamma, E, e)| \leq \beta(\rho) = 2^{[2|\rho]} \prod_{\ell \mid \rho, \ \ell \geq 5} \frac{3}{\ell - 2}.$$

Proof. As α is -2 times the average of $((y/\rho))$, Lemma 2.13 bounds $|\alpha|$ by the number of terms, $2^{\omega(\rho) - [3|\rho]}(3/2)^{|E|}$, divided by $|Y|$. Prime by prime the quotient is 2 for $\ell = 2$, 1 for $\ell = 3$, $2/(\ell - 1) \leq 3/(\ell - 2)$ for $\ell \geq 5$ outside E and $3/(\ell - 2)$ for $\ell \in E$. □

Let $B^* = \{n \geq 2 : \ A^*(n) \geq 1/6\}$. By Lemmas 2.13 and 2.14 it is finite and computable: $\beta(\rho) \geq 1/6$ for finitely many squarefree ρ, and $n = \rho k$ with $\operatorname{rad}(n) = \rho$ lies in B^* only if $k \leq 6A^*(\rho)$. We find that $\max_n A^*(n) = 2/3$, attained only at $n = 6$, and that

$$B^* = \{3, 5, 6, 10, 12, 14, 15, 18, 21, 24, 30, 33, 42, 60, 66, 90\}. \tag{2.2}$$

Lemma 2.15. *Let $3 \mid N$. If $C_d \cap \Phi = \emptyset$ for some $d \in \mathcal{D}$, then $N = \operatorname{lcm}(n, n')$ for some $n, n' \in B^*$ with $A^*(n) \geq A^*(n')$ and $A^*(n) + 2A^*(n') \geq 1$, and N is one of* 3, 6, 12, 15, 18, 24, 30, 42, 60, 66, 90 *and* 330.

Proof. By Lemma 2.11 with $C' = C_d$, $a_1 + a_2 + a_3 = -1$, so $A^*(N_1) + A^*(N_2) + A^*(N_3) \geq 1$. Order these values as $A_1 \geq A_2 \geq A_3$. Then $A_1 + 2A_2 \geq 1$ and $A_2 \geq (1 - A_1)/2 \geq 1/6$, so the two N_j with the largest values lie in B^*, and their least common multiple is N. The list is read off from (2.2) and the values of A^*. □

Proof of Theorem 1.5. If $3 \nmid N$, $C = F$ by the first case. If $3 \mid N$ and N is not in the list of Lemma 2.15, every C_d meets Φ, and $C = F$ by Lemma 2.10. The smallest set containing G that satisfies rules (ii) and (iii) is the closure of G under the rule with $u = 1$ and under multiplication by units, since each b the rule adds brings its orbit $O_{\gcd(b,N)}$. For the N of the list we find that this closure is F for every triangle except the eleven triangles

$$(1,2,9)/12, \quad (2,3,7)/12, \quad (1,3,14)/18, \quad (2,3,13)/18, \quad (3,7,8)/18, \quad (1,4,19)/24,$$
$$(4,7,13)/24, \quad (1,5,24)/30, \quad (5,6,19)/30, \quad (5,7,18)/30, \quad (5,12,13)/30,$$

where it is $G \cup \bigcup_{d \neq 3}(O_d \cap F)$. All of them have $N \leq 30$. □

2.6. **Cylinders.** The cylinder arguments of Sections 6 and 7 rest on one lemma. It says how the periods of a closed curve at the units are Galois conjugates of its period for ω, what Wright's cylinder deformations put into V, and what this forces on S.

In the plane the unfolding is the union of the $2N$ triangles $g(\Delta)$, g in the group $\mathfrak{D}$ of the maps $w \mapsto \zeta^k w$ and $w \mapsto \zeta^k \bar{w}$: the copy $g(\Delta)$ is glued by a translation to $(gr_s)(\Delta)$ along their common side $g(s)$, where $r_s \in \mathfrak{D}$ is the linear part of the reflection in the side s of Δ, the form ω is dw on each copy, and T maps the copy $g(\Delta)$ to $(\zeta g)(\Delta)$ by $w \mapsto \zeta w$ [36]. For a direction θ, a *cylinder of direction* θ is a maximal cylinder whose leaves have direction θ; for such a D let c_D and h_D be its circumference and height and α_D its core curve, oriented so that $\int_{\alpha_D} \omega = c_D e^{i\theta}$. On the rotated surface $(X, e^{-i\theta}\omega)$, D is horizontal, and Wright's class $I_D \in H^1(X, \Sigma; \mathbb{Z})$ vanishes on the relative cycles that can be realized disjointly from the interior of D and is one on a relative cycle crossing D from a zero on its bottom to a zero on its top [35, Lemma 2.4]. It is Poincaré dual to α_D [35, Remark 2.5], so there is a sign $\epsilon = \pm 1$, the same for all cylinders, with

$$\int_X p(I_D) \wedge \eta = \epsilon \int_{\alpha_D} \eta \qquad \text{for every } \eta \in H^1(X; \mathbb{C}). \tag{2.3}$$

We use three statements of Wright. For a collection J of horizontal cylinders on a translation surface, the shear of the cylinders of J by t moves the period coordinates by $t \sum_{D \in J} h_D I_D$ for small t [35, Lemmas 2.3 and 2.4]. For an equivalence class J of $\mathcal{M}$-parallel horizontal cylinders on a surface of $\mathcal{M}$, these shears stay in $\mathcal{M}$ [35, Theorem 5.1]. And two cylinders are $\mathcal{M}$-parallel if and only if their core curves have proportional images in the dual of the tangent space [35, Definition 4.4 and Lemma 4.7].

For $A_0 \subset S$, two cylinders D, D' of direction θ are *A_0-equivalent* if $c_{D'} \int_{\alpha_D} \eta = c_D \int_{\alpha_{D'}} \eta$ for every $\eta \in \bigoplus_{a \in A_0} H^1_a$. Fix a vertex v_0 of Δ, with numerator p_0, let P_0 be the set of points of X above it, e the side of Δ opposite v_0, and $\delta \in H_1(X, P_0; \mathbb{Z})$ the class of a path that runs inside the copy Δ from its vertex v_0 to an interior point of e and on inside the copy $r_e(\Delta)$ to its vertex above v_0. For $\ell \in \mathbb{Z}/N$ let $\Pi_\ell = \frac{1}{N} \sum_k \zeta^{-\ell k} T_*^k$, the projection onto the ζ^ℓ-eigenspace of T_*, and for $v \in G$ let σ_v also denote the automorphism $\zeta \mapsto \zeta^v$ of $\mathbb{Q}(\zeta)$.

Lemma 2.16. *Let Δ be a rational triangle.*

(a) *The sides opposite v_0 of the $2N$ copies are the N edges $T^k(e)$, $k \in \mathbb{Z}/N$, where $T^k(e)$ is the common side of $\zeta^k\Delta$ and $\zeta^k r_e(\Delta)$. Let γ be a closed curve, or a path with ends in P_0, that misses the points above the other two vertices and crosses the edges $T^k(e)$ finitely often and transversally, n_k^+ times from $\zeta^k\Delta$ into $\zeta^k r_e(\Delta)$ and n_k^- times back. Then*

$$[\gamma] = P_\gamma(T)\,\delta \quad \text{in } H_1(X, P_0; \mathbb{Z}), \qquad P_\gamma(T) = \sum_{k \in \mathbb{Z}/N} (n_k^+ - n_k^-) T^k.$$

(b) *Let $\ell \in \mathbb{Z}/N$ with $\ell p_0 \not\equiv 0$. Then $H_1(X; \mathbb{C}) \to H_1(X, P_0; \mathbb{C})$ is an isomorphism on ζ^ℓ-eigenspaces, and for every closed γ as in (a) and every $\eta \in H^1(X; \mathbb{C})$ with $T^*\eta = \zeta^\ell \eta$,*

$$\int_\gamma \eta = P_\gamma(\zeta^\ell)\,\kappa_\eta, \qquad \kappa_\eta = \langle \Pi_\ell \delta, \eta \rangle.$$

If $\ell \in \Phi \cup -\Phi$ and $\eta \neq 0$, then $\kappa_\eta \neq 0$.

(c) *$\kappa_\omega = \int_\delta \omega \neq 0$, and $\int_\gamma \omega \in \kappa_\omega \mathbb{Z}[\zeta]$ for every $\gamma \in H_1(X; \mathbb{Z})$. For a unit v and $0 \neq \eta \in H^1_v$, $\int_\gamma \eta = \kappa_\eta\, \sigma_v(\kappa_\omega^{-1} \int_\gamma \omega)$ for every $\gamma \in H_1(X; \mathbb{Z})$. Hence for cylinders C, D of one direction, $t = c_D/c_C \in \mathbb{Q}(\zeta)$, and $\int_{\alpha_D} \eta = \sigma_v(t) \int_{\alpha_C} \eta$ with $\int_{\alpha_C} \eta \neq 0$.*

Let Δ moreover be scalene, $\Delta \neq (1,2,3)/6$, and θ a direction.

(d) *Two $\mathcal{M}$-parallel cylinders of direction θ are S-equivalent, hence A_0-equivalent for every $A_0 \subset S$. If J is a union of classes of $\mathcal{M}$-parallel cylinders of direction θ, for instance a union of A_0-equivalence classes, then $\sum_{D\in J} h_D I_D \in V$.*

(e) *Let $\xi = \sum_D w_D I_D \in V$, the sum over finitely many cylinders of direction θ with real w_D, and let $b \in \Phi \cup -\Phi$ and $0 \neq \eta \in H^1_b$. If $\sum_D w_D \int_{\alpha_D} \eta \neq 0$, then $b, -b \in S$.*

(f) *Let $A_0 \subset S$, C a cylinder of direction θ, and E a union of classes of $\mathcal{M}$-parallel cylinders of direction θ that contains C and consists of cylinders A_0-equivalent to C, for instance the $\mathcal{M}$-parallel class of C. For $D \in E$ let $t_D = c_D/c_C$, a positive element of $\mathbb{Q}(\zeta)$. Then*

(f1) *$\sigma_v(t_D) = t_D$ for every $D \in E$ and every unit $v \in A_0$;*

(f2) *$\sum_{D\in E} h_D\, \sigma_v(t_D) = 0$ for every unit $v \notin S$;*

(f3) *if N is even, $\iota(D)$ is A_0-equivalent to D for every cylinder D of direction θ.*

(g) *Suppose that $V \cap Z = 0$. If (X,ω) has k cylinders of one direction, no two of them $\mathcal{M}$-parallel, then $\operatorname{rank}\mathcal{M} \geq k$. This holds in particular if their moduli are pairwise not rational multiples of each other.*

For an $\mathcal{M}$-parallel class E and $A_0 = S$, (f1) is close to Wright's theorem that the ratios of circumferences of $\mathcal{M}$-parallel cylinders generate the field of definition of $\mathcal{M}$ [35, Theorem 7.1], which is fixed by the σ_v with $vS = S$ [19, Lemma 2.5 and its proof]; we need it for the coarser A_0-equivalence, where the proof is two lines. Part (g) is a form of Wright's bound on parallel cylinders [35, Theorem 1.10], and its proof is his argument for that bound [35, Lemma 8.10 and Corollary 8.11].

Proof. (a) The copies with the side $g(e)$ are $g(\Delta)$ and $(gr_e)(\Delta)$; as r_e is a reflection, exactly one of g, gr_e is a rotation ζ^k, and T^k maps Δ onto $\zeta^k\Delta$. Retracting each copy minus its vertex above v_0 radially onto its opposite side retracts $X \setminus P_0$ onto the graph Γ of the N edges $T^k(e)$; the retractions agree on the shared sides through points of P_0. By Lefschetz duality a class of $H_1(X,P_0;\mathbb{Z})$ is determined by its intersection numbers with the cycles of Γ, that is, by its intersection numbers with the edges, read modulo coboundaries of Γ, and every assignment of numbers to the edges arises. The class $T^k\delta$ crosses $T^k(e)$ once, from $\zeta^k\Delta$ into $\zeta^k r_e(\Delta)$, and no other edge. This gives the formula and $H_1(X,P_0;\mathbb{Z}) = \mathbb{Z}[T]\,\delta$.

(b) The sequence $0 \to H_1(X;\mathbb{C}) \to H_1(X,P_0;\mathbb{C}) \to \tilde{H}_0(P_0;\mathbb{C}) \to 0$ is exact and T-equivariant, and T permutes P_0 cyclically with stabilizer generated by T^{g_0}, $g_0 = \gcd(p_0,N)$, so ζ^ℓ is an eigenvalue on $H_0(P_0;\mathbb{C})$ only if $(N/g_0) \mid \ell$, that is, $\ell p_0 \equiv 0$. As Π_ℓ commutes with the maps of the sequence and $\Pi_\ell T_*^k = \zeta^{\ell k}\Pi_\ell$, (a) gives $\Pi_\ell[\gamma] = P_\gamma(\zeta^\ell)\,\Pi_\ell\delta$, with $\Pi_\ell\delta$ read as an absolute class; and $\langle\gamma,\eta\rangle = \langle\Pi_\ell\gamma,\eta\rangle$, as η vanishes on the other eigenspaces. If $\ell \in \Phi \cup -\Phi$, H^1_ℓ is a line, so the ζ^ℓ-eigenspace of $H_1(X;\mathbb{C})$, which pairs perfectly with it, is a line, spanned by the classes $\Pi_\ell[\gamma]$ and hence by $\Pi_\ell\delta$; so $\kappa_\eta \neq 0$ for $\eta \neq 0$.

(c) Apply (b) with $\ell = 1$ and $\eta = [\omega]$; as $\int_{T^k\delta}\omega = \zeta^k \int_\delta \omega$, $\kappa_\omega = \int_\delta \omega$. As P_γ has integer coefficients, $P_\gamma(\zeta^v) = \sigma_v(P_\gamma(\zeta)) = \sigma_v(\kappa_\omega^{-1}\int_\gamma\omega)$, and (b) with $\ell = v$ gives the formula. For cylinders, $t = P_{\alpha_D}(\zeta)/P_{\alpha_C}(\zeta)$, and $\int_{\alpha_C}\eta = \kappa_\eta\sigma_v(P_{\alpha_C}(\zeta)) \neq 0$, as $P_{\alpha_C}(\zeta) = \kappa_\omega^{-1}c_C e^{i\theta} \neq 0$.

(d) Let $Y = (X, e^{-i\theta}\omega)$. Rotation multiplies period coordinates by a scalar, so near Y the orbit closure is V in the period coordinates of Y with the marking of (X,ω), and $T_Y\mathcal{M} = V$. If D, D' are $\mathcal{M}$-parallel, there is $\lambda \in \mathbb{C}$ with $\int_{\alpha_D} v = \lambda \int_{\alpha_{D'}} v$ for all $v \in V$; $v = e^{-i\theta}[\omega]$ gives $\lambda = c_D/c_{D'}$, and as these integrals depend only on $p(v)$ and $p(V) = \bigoplus_{a\in S} H^1_a$, D and D'

are S-equivalent. So J is a union of $\mathcal{M}$-parallel classes $J_1, \dots, J_s$; by Wright's theorem the shear of the cylinders of J_r keeps Y in $\mathcal{M}$, so $\sum_{D\in J_r} h_D I_D \in V$, and we sum over r.

(e) By (1.2), $p(\xi) = \sum_{a\in S} \xi_a$ with $\xi_a \in H^1_a$. As T^* preserves the cup product, H^1_a and $H^1_{a'}$ pair to zero unless $a + a' \equiv 0$. By (2.3), $\int_X \xi_{-b} \wedge \eta = \int_X p(\xi) \wedge \eta = \epsilon \sum_D w_D \int_{\alpha_D} \eta \neq 0$, with $\xi_{-b} = 0$ if $-b \notin S$. So $-b \in S$, and $b \in S$ by rule (i).

(f) By (c), $t_D \in \mathbb{Q}(\zeta)$, and $\int_{\alpha_D} \eta = \sigma_v(t_D) \int_{\alpha_C} \eta$ for a unit v and $0 \neq \eta \in H^1_v$, with $\int_{\alpha_C} \eta \neq 0$. For $v \in A_0$, A_0-equivalence gives $\int_{\alpha_D} \eta = t_D \int_{\alpha_C} \eta$, which is (f1). For a unit $v \notin S$, (d) puts $\sum_{D\in E} h_D I_D$ in V, and (e) gives $\sum_D h_D \int_{\alpha_D} \eta = 0$, which is (f2). For (f3), $\iota^*\omega = -\omega$, so ι maps D onto a cylinder of direction θ with $c_{\iota(D)} = c_D$ and $\alpha_{\iota(D)} = -\iota_*\alpha_D$; for $a \in A_0$, odd as $S \subset F$, and $\eta \in H^1_a$, $\iota^*\eta = -\eta$, so $\int_{\alpha_{\iota(D)}} \eta = \int_{\alpha_D} \eta$.

(g) Let $C_1, \dots, C_k$ be the cylinders and P_j the $\mathcal{M}$-parallel class of C_j; the P_j are distinct. In the second case they are not $\mathcal{M}$-parallel by Mirzakhani and Wright's theorem that, when $V \cap Z = 0$, the moduli of $\mathcal{M}$-parallel cylinders are rational multiples of each other [27, Corollary 1.6]. By (d), $\eta_j = \sum_{D\in P_j} h_D I_D \in V$. A segment σ_j in the closure of C_j, transverse to the leaves, from a zero on one boundary component to a zero on the other, has $I_{C_j}(\sigma_j) = \pm 1$ and $I_D(\sigma_j) = 0$ for every other cylinder D of direction θ, whose interior misses the closure of C_j. So $\eta_j(\sigma_{j'})$ is $\pm h_{C_j}$ for $j' = j$ and 0 otherwise, and the η_j are linearly independent; as $V \cap Z = 0$, so are the $p(\eta_j)$. By (2.3), $p(\eta_j)$ is ϵ times the Poincaré dual of $\sum_{D\in P_j} h_D \alpha_D$, and core curves of distinct cylinders of one direction are disjoint, so the $p(\eta_j)$ span an isotropic subspace of $p(V)$. The cup product is non-degenerate on $p(V)$, which has dimension $|S|$ and is the sum of the pairs $H^1_a \oplus H^1_{-a}$; so $k \leq |S|/2 = \operatorname{rank} \mathcal{M}$. □

2.7. **Residues.** The arguments by cases choose characters $x, b \in \Phi$ with a prescribed sum and apply rule (iii). The next lemma reads membership in Φ off two residues, and in the coordinate given by a numerator prime to N.

Lemma 2.17. *Let i and k be distinct vertices.*

(a) *A character a lies in Φ if and only if $[ap_i] > 0$, $[ap_k] > 0$ and $[ap_i] + [ap_k] < N$.*

(b) *Let p_i be prime to N, $g = \gcd(p_k, N)$ and $n = N/g$, and for an integer y let $a_y \equiv y p_i^{-1} \pmod N$ and $\rho(y) \in \{0, \dots, n-1\}$ the residue of $y p_i^{-1}(p_k/g)$ modulo n. Then $[a_y p_i] = [y]$ and $[a_y p_k] = g\rho(y)$, so $a_y \in \Phi$ if and only if $[y] > 0$, $\rho(y) > 0$ and $[y] + g\rho(y) < N$. The map $y \mapsto a_y$ is a bijection of $\mathbb{Z}/N$ that preserves $\gcd(\cdot, N)$, and $a_y + a_{y'} \equiv c$ if and only if $y + y' \equiv c p_i$. If $p_k = N/3$, then $\rho(y) = 1$ for $y \equiv p_i \pmod 3$, and for such y, $a_y \in \Phi$ if and only if $0 < [y] < 2N/3$.*

(c) *In (b), let $c \in \mathbb{Z}/N$, $L = [cp_i]$, and let $y, y' \in (0, N)$ with $y + y' = L + \varepsilon N$, $\varepsilon \in \{0, 1\}$, and $\rho(y), \rho(y') > 0$; put $r = g\rho(y)$ and $r' = g\rho(y')$. Then $a_y, a_{y'} \in \Phi$ if and only if*

$$\max(0, L + \varepsilon N - N + r') < y < \min(N - r, L + \varepsilon N).$$

A class of y modulo n fixes r, and fixes the class of $y' = L - y$ and so r'; the y of the class with $a_y, a_{L-y} \in \Phi$ are those in the union of the two intervals above, for $\varepsilon = 0$ and $\varepsilon = 1$.

(d) *Let $C \ni 1$ be closed with unit part H, let $a' \in C$, and let $x \in G \cap \Phi$ and $b \in \Phi$ with $x + b = 1 - a'$. Then $b/x \in C$. If b is a unit, $b/x \in H$; if $d = \gcd(b, N) > 1$, then $K_{N/d} \subset H$, and $K_{\gcd(m, N/d)} \subset H$ for every $m \mid N$ with $K_m \subset H$.*

Proof. (a) If the two residues are positive with sum below N, the third, $N - [ap_i] - [ap_k]$, lies in $(0, N)$, and the three add up to N. Conversely, the residues of $a \in \Phi$ are positive with sum N.

(b) $a_y p_i \equiv y$, and $a_y p_k = g\, a_y(p_k/g) \equiv g\rho(y) \pmod{gn}$ with $0 \le g\rho(y) < N$; now apply (a). For $p_k = N/3$, $g = N/3$, $n = 3$ and $p_k/g = 1$, so $\rho(y) \equiv y p_i^{-1} \equiv 1 \pmod 3$ for $y \equiv p_i$.

(c) $y + y'$ lies in $(0, 2N)$ and is $\equiv L$, which fixes ε. By (b), $a_y, a_{y'} \in \Phi$ if and only if $y < N - r$ and $y' = L + \varepsilon N - y < N - r'$, with $y, y' > 0$.

(d) Rule (iii) with $u = a = x$, which lies in $xC \cap \Phi$ as $1 \in C$, puts b in xC. The rest is Lemma 2.6 and $K_m K_{N/d} = K_{\gcd(m, N/d)}$. □

3. Closed sets and witnesses

This section reduces Theorem 1.2 to three conditions on the unit parts of closed sets, one for the conductor N', one for the conductors strictly between 1 and N', and one for the group H_{12}, and proves Theorem 1.4, which gives the first condition on every triangle with a witness.

3.1. Three conditions.

Let Δ be scalene. We say that Δ satisfies

(N′): if no closed set containing 1 has a unit part $H \ne \{\pm 1\}$ of conductor N';

(D): if every closed set containing 1 whose unit part H has a conductor c with $1 < c < N'$ has $12 \mid c$ and $H \supset H_{12}$;

(12): if $12 \nmid N$, or every closed set containing 1 whose unit part contains H_{12} is F.

We say that (D) holds *at* c if its conclusion holds for the closed sets whose unit part has conductor c.

Proposition 3.1. *Let $N > 30$ and let Δ be scalene and satisfy* (N′), (D) *and* (12). *Then every closed set $C \ni 1$ with $|C| \ge 4$ is F.*

Proof. Let H be the unit part of C and c its conductor. As $|C| \ge 4$, $H \ne \{\pm 1\}$ by Lemma 2.7, which also gives $c \mid N'$; and $c \ne N'$ by (N′). If $c = 1$, then $G = K_1 \subset H$, and $C = F$ by Theorem 1.5. Otherwise $1 < c < N'$, (D) gives $12 \mid c$ and $H \supset H_{12}$, and (12) gives $C = F$. □

Corollary 3.2. *Let $N > 58$ and let Δ be a scalene triangle not in* (1.1) *that satisfies* (N′), (D) *and* (12). *Then $S = F$ and $\mathcal{M} = \mathcal{L}$.*

Proof. The scalene triangles of rank one with $N > 58$ are the three families of (1.1) [19, Theorem 1.1], so $\operatorname{rank} \mathcal{M} \ge 2$ and $|S| \ge 4$ by (1.2). As S is closed and contains 1 (Section 2.1), $S = F$ by Proposition 3.1, and $\mathcal{M} = \mathcal{L}$ by Corollary 2.4. □

Condition (N′) is a statement about subgroups of G alone, since a closed set whose unit part has conductor N' is that unit part (Lemma 2.7); and closedness of a subgroup is a condition on sums of two holomorphic characters. We call a pair (x, b) of elements of Φ with $x + b = c$ a *pair on the diagonal* $c \in \mathbb{Z}/N$; then (b, x) is one too. For a subgroup $H \ni -1$ of G consider the condition

(P): for every $a' \in H$, the two members x, b of every pair on the diagonal $1 - a'$ are both non-units, or both units with $b/x \in H$.

Lemma 3.3. *A subgroup $H \ni -1$ of G is closed if and only if it satisfies* (P). *Hence Δ satisfies* (N′) *if and only if no subgroup $H \ne \{\pm 1\}$ of conductor N' satisfies* (P)*; and if the diagonal 2 carries a pair with exactly one unit member, no subgroup containing -1 is closed, and Δ satisfies* (N′).

Proof. Every unit lies in $\Phi \cup -\Phi$ and is odd at even N, so $H \subset F$, and rules (i) and (ii) hold for a subgroup containing -1. Let H be closed, $a' \in H$, and (x, b) a pair on the diagonal $1 - a'$ with x a unit. Rule (iii) with $u = a = x$ puts b in xH, so b is a unit and $b/x \in H$; the case of a unit b is the same with x and b exchanged. Conversely, let H satisfy (P), and in rule (iii) let $a \in uH \cap \Phi$, $a' \in H$ and $b = 1 - a - a' \in \Phi$. Then a is a unit with $aH = uH$, and (a, b) is a pair on the diagonal $1 - a'$; by (P), $b \in aH = uH$. The second statement follows with Lemma 2.7, and the third is (P) at $a' = -1$. □

3.2. **Proof of Theorem 1.4.** Let x be a witness, $C \ni 1$ a closed set, H its unit part and c its conductor. The $m \mid N$ with $K_m \subset H$ are the multiples of c, as $K_m K_c = K_{\gcd(m,c)}$, and $K_m = \{1\}$ only for $m \in \{N', N\}$ (Section 2.4); so H contains some $K_f \neq \{1\}$ if and only if c is a proper divisor of N', which is the equivalence in the theorem. Suppose that $c = N'$. Then $C = H$ by Lemma 2.7, so H is closed, and we shall find some $K_f \neq \{1\}$ in H, a contradiction. Put $d = x - 1$ and $n_i = N/g_i$ for $i = 1, 2, 3$; as p_i/g_i is prime to n_i, $ap_i \equiv 0$ if and only if $n_i \mid a$.

Lemma 3.4. *The element $\rho = (2 - x)/x$ lies in H, $\rho \neq 1$, and for every $h \in H$ such that no n_i divides $h + d$, $h + d$ is a unit and $(h + d)/x \in H$.*

Proof. By rule (iii) with $u = a = x$ and $a' = -1$, $2 - x \in xH$; so $2 - x$ is a unit and $\rho \in H$, and $\rho \neq 1$ as $2x \not\equiv 2$. Let $h \in H$ with no n_i dividing $h + d$. Then $h + d \in \Phi \cup -\Phi$; at even N it is odd, as h and x are. If $-(h + d) = 1 - x - h$ lies in Φ, rule (iii) with $(u, a, a') = (x, x, h)$ puts it in xH. Otherwise $h + d = 1 - (2 - x) - (-h)$ lies in Φ, and rule (iii) with $(u, a, a') = (2 - x, 2 - x, -h)$ puts it in $(2 - x)H = xH$. In both cases $(h + d)/x \in H$, as $-1 \in H$. □

So $\tau(h) = (h + d)/x$, an injective map, sends H into H off the set of h with $n_i \mid h + d$ for some i. The rest is arithmetic in $\mathbb{Z}/n$ for a modulus n, and we state it in that generality, since at odd N it is applied at $n = 2N$ and at divisors of N. For $f \mid n$ we write K_f for the group of units modulo n that are $\equiv 1 \pmod f$, and $\mathrm{rad}(m)$ for the product of the primes of m. Let $H \ni -1$ be a subgroup of $(\mathbb{Z}/n)^\times$ and $d \in \mathbb{Z}/n$ with $1 + d$ and $1 - d$ units, $2d \not\equiv 0$, and $\rho = (1 - d)/(1 + d) \in H$; put $x = 1 + d$ and $\tau(h) = (h + d)/x = 1 + (h - 1)/x$. For a subset $E \subset H$ consider

(T): for every $h \in H \setminus E$, the residue $h + d$ is a unit and $\tau(h) \in H$.

The map τ preserves each class $1 + f\mathbb{Z}/n$, $f \mid n$, and sums of powers over subgroups do the counting.

Lemma 3.5. *Let s be an odd prime, $a \geq 1$, and μ a subgroup of $(\mathbb{Z}/s^a)^\times$ of order k prime to s. Then μ is cyclic, reduction modulo s is injective on μ, and $\sum_{z \in \mu} z^i \equiv 0 \pmod{s^a}$ for every integer i with $k \nmid i$.*

Proof. $(\mathbb{Z}/s^a)^\times$ is cyclic of order $s^{a-1}(s-1)$, and the kernel of reduction modulo s has order s^{a-1}, so μ is cyclic and meets the kernel trivially. If ζ generates μ and $k \nmid i$, then $\zeta^i - 1$ is a unit, and $(\zeta^i - 1)\sum_{j<k} \zeta^{ij} = \zeta^{ik} - 1 = 0$. □

Lemma 3.6. *Let $n = 2^\alpha m$ with $\alpha \geq 1$ and m odd, let r be an odd divisor $r > 1$ of m, or $r = \infty$, and let* (T) *hold for $E = \{h \in H : \ r \mid h + d\}$ (empty if $r = \infty$).*

(i) *If $E = \emptyset$, then $H + d = xH$, $\mathrm{rad}(m) \mid d$, and H contains some $K_f \neq \{1\}$ with $2^{\min(\alpha,2)} \mathrm{rad}(m) \mid f \mid n$.*

(ii) *If $E \neq \emptyset$, then r is a prime, $r \geq 5$, $r \nmid d$, and H maps onto $(\mathbb{Z}/r)^\times$.*

Proof. (i) By (T), the injective map τ sends H into H, so $H + d = xH$. Reduce modulo a prime $s \mid m$ and sum over the image $\bar{H}$ of H: its elements cancel in pairs $\pm z$, so $|\bar{H}|d \equiv 0 \pmod{s}$ with $0 < |\bar{H}| < s$, and $s \mid d$. So $\rho - 1 = -2d/x \equiv 0 \pmod{\mathrm{rad}(m)}$, and if $\alpha \geq 2$, $\rho - 1 = -d(1+\rho)$ is divisible by 4, as d and $1+\rho$ are even. So $\rho \neq 1$ lies in K_{f_0}, $f_0 = 2^{\min(\alpha,2)}\,\mathrm{rad}(m)$. By the Chinese remainder theorem K_{f_0} is the product of the groups of units $\equiv 1 \pmod{s}$ modulo $s^{v_s(n)}$, $s \mid m$, cyclic of order $s^{v_s(n)-1}$, and of the group of units $\equiv 1 \pmod 4$ modulo 2^α, cyclic of order $2^{\alpha-2}$ if $\alpha \geq 2$ and trivial otherwise. These orders are pairwise coprime, so every subgroup of K_{f_0} is a product of subgroups of the factors, that is, some K_f with $f_0 \mid f \mid n$; and $\langle\rho\rangle$ is such a $K_f \neq \{1\}$.

(ii) Let $h_0 \in E$; then $d \equiv -h_0$ is a unit modulo r. Let $\bar{H}$ be the image of H in $(\mathbb{Z}/r)^\times$ and $k = |\bar{H}|$; then $-d \in \bar{H}$. For $z \in \bar{H} \setminus \{-d\}$ the elements of H above z lie outside E, and τ maps them above $(z+d)/x$; so $z \mapsto (z+d)/x$ maps $\bar{H} \setminus \{-d\}$ injectively into $\bar{H}$, and

$$(\bar{H} \setminus \{-d\}) + d = x\bar{H} \setminus \{e\}$$

for one $e \in x\bar{H}$. The sum S_1 of the elements of $\bar{H}$ is 0 modulo r, as they cancel in pairs $\pm z$. Summing the two sides gives $kd \equiv -e \pmod r$, so k is prime to r, as d and e are units. Let $s^a \parallel r$ and let μ be the image of $\bar{H}$ in $(\mathbb{Z}/s^a)^\times$, of order $k_s \mid k$, prime to s and even. If $k_s = 2$, then $-d \equiv \pm 1 \pmod s$, and s divides one of the units $1 \pm d$; so $k_s \geq 4$, and by Lemma 3.5 the sum S_2 of the squares of the elements of $\bar{H}$, whose fibers over μ have equal size, is $\equiv 0 \pmod{s^a}$. Summing the squares of the two sides gives $S_2 + 2dS_1 + kd^2 \equiv x^2 S_2 - e^2$, that is, $k(k+1)d^2 \equiv 0 \pmod{s^a}$, and $s^a \mid k+1$. Hence $r \mid k+1$, and as $k \leq \varphi(r) \leq r-1$, $k = r - 1 = \varphi(r)$: r is a prime and $\bar{H} = (\mathbb{Z}/r)^\times$. Finally $k_s = r - 1 \geq 4$, so $r \geq 5$. □

Lemma 3.7. *In Lemma 3.6(ii), H contains some $K_f \neq \{1\}$ with $f \mid n$.*

Proof. Write $n = r^k n'$ with $r \nmid n'$. Let $B = H \cap K_r$, so that $E = h_0 B$ is a coset of B, and $\phi(z) = (z+d)/x$, a bijection of $\mathbb{Z}/r$ with $\phi(-d) = 0$.

Step 1: every odd prime $q \neq r$ of n divides d. Let $\bar{H}$ be the image of H in $(\mathbb{Z}/q)^\times$, $k_q = |\bar{H}|$, and $H[\pi]$ the fiber of H over $\pi \in \bar{H}$. If every fiber has an element outside E, then, as in Lemma 3.6(i), $\bar{H} + d = x\bar{H}$ and $q \mid d$. Otherwise some fiber lies in the coset E, so $H \cap K_q \subset B$, and $\psi(h \bmod q) = h \bmod r$ is a well-defined homomorphism $\bar{H} \to (\mathbb{Z}/r)^\times$, onto by Lemma 3.6. Let $\kappa = |\ker\psi|$, so $k_q = \kappa(r-1)$, and let $\Pi_E = \psi^{-1}(-d)$ and $\Pi' = \psi^{-1}(d/x)$. For $\pi \notin \Pi_E$ the fiber $H[\pi]$ misses E, and τ maps it into H above $(\pi+d)/x$ modulo q and above $\phi(\psi(\pi)) \neq \phi(0) = d/x$ modulo r. So $\pi \mapsto (\pi+d)/x$ maps $\bar{H} \setminus \Pi_E$ injectively into $\bar{H} \setminus \Pi'$, which has as many elements, and

$$(\bar{H} \setminus \Pi_E) + d = x(\bar{H} \setminus \Pi') \quad \text{in } \mathbb{Z}/q.$$

If $\kappa \geq 2$, the sums over the cosets of $\ker\psi$ vanish by Lemma 3.5, and summing gives $\kappa(r-2)d \equiv 0 \pmod q$ with $0 < \kappa(r-2) < k_q < q$; so $q \mid d$. If $\kappa = 1$, $\bar{H}$ is the group of k_q-th roots of unity, $k_q = r - 1 \geq 4$, and $\Pi_E = \{\pi_0\}$, $\Pi' = \{\pi_1\}$. For $1 \leq j \leq 3$, $\sum_{z\in\bar{H}}(z+d)^j = k_q d^j$, and the j-th power sums of the two sides give

$$k_q d^j - u^j + e^j \equiv 0 \pmod q, \qquad u = \pi_0 + d,\ e = x\pi_1.$$

Suppose $q \nmid d$; also $q \nmid k_q$. Then $j = 1$ gives $e = u - k_q d$, $j = 2$ gives $k_q d((k_q+1)d - 2u) \equiv 0$, so $2u \equiv (k_q+1)d$, and $j = 3$ then gives $k_q d^3(1 - k_q^2)/4 \equiv 0$. So $q \mid (k_q - 1)(k_q + 1)$ with $3 \leq k_q - 1 < k_q + 1 \leq q$, and $q = k_q + 1 = r$, which is excluded.

Step 2: translations. For $h \in B$, $h + d \equiv x \not\equiv 0 \pmod r$, so $h \notin E$ and $\tau(h) \in H \cap K_r = B$; hence $\tau(B) = B$. For $u \in B$, the bijection $z \mapsto u\,\tau(u^{-1}\tau^{-1}(z))$ of B is $z \mapsto z + (u-1)d/x$,

as $\tau^{-1}(z) = 1 + x(z-1)$. So B is stable under translation by the additive subgroup $f\mathbb{Z}/n$ generated by the $(u-1)d/x$, $u \in B$, and $1 + f\mathbb{Z}/n = K_f \subset B \subset H$. If $(u-1)d \not\equiv 0 \pmod n$ for some $u \in B$, then $f \neq n$ and $K_f \ni 1 + f$ is not $\{1\}$.

Step 3: $B \not\subset K_q$ for every odd prime $q \neq r$ of n, and $B \not\subset K_4$ if $4 \mid n$. Let q be such a prime, or $q = 4$ when $4 \mid n$, and suppose $B \subset K_q$. Then $\lambda(h \bmod r) = h \bmod q$ is a well-defined homomorphism $(\mathbb{Z}/r)^\times \to (\mathbb{Z}/q)^\times$, defined everywhere as H maps onto $(\mathbb{Z}/r)^\times$. By Step 1, or for $q = 4$ because d and $1 - h$ are even, $\tau(h) - h = d(1-h)/x \equiv 0 \pmod q$. For $z \in (\mathbb{Z}/r)^\times$, $z \neq -d$, an $h \in H$ above z is not in E, and $\tau(h)$ lies above $\phi(z)$ with $\tau(h) \equiv h \pmod q$; so $\phi(z)/z = (1 + d/z)/x \in \ker\lambda$. These values are all of $(\mathbb{Z}/r)^\times$ except $1/x$, so $\ker\lambda$ has at least $r - 2 > (r-1)/2$ elements, and λ is trivial; but $\lambda(-1) = -1 \neq 1$.

Step 4. If some odd prime $q \neq r$ has $v_q(d) < v_q(n)$, take $u \in B$ with $u \not\equiv 1 \pmod q$; if $4 \mid n$ and $v_2(d) \leq \alpha - 2$, take $u \in B$ with $u \equiv 3 \pmod 4$. In both cases $(u-1)d \not\equiv 0 \pmod n$, and Step 2 gives the lemma.

Step 5. Otherwise $n' \mid 2d$, so $\tau(h) \equiv h \pmod{n'}$ for every $h \in H$, as $1 - h$ is even, and $\rho - 1 = -2d/x \equiv 0 \pmod{n'}$. Let $J = H \cap K_{n'}$, which contains ρ, and $\rho \not\equiv 1 \pmod r$, as $r \nmid 2d$. Then τ maps $J \setminus E$ into J. Let J_r be the image of J in $(\mathbb{Z}/r)^\times$, of order $m_J \geq 2$. If $-d \notin J_r$, then $J_r + d = xJ_r$, and summing gives $m_J d \equiv 0 \pmod r$, impossible. So $-d \in J_r$, and as in Lemma 3.6(ii), $(J_r \setminus \{-d\}) + d = xJ_r \setminus \{e\}$ for one e. A subgroup of order 2 would be $\{\pm 1\}$, and $-d \equiv \pm 1$ is excluded; so $m_J \geq 3$, and the sums of the elements of J_r and of their squares vanish modulo r (Lemma 3.5). The sums of the two sides and of their squares give $e \equiv -m_J d$ and $m_J(m_J + 1)d^2 \equiv 0 \pmod r$, so $m_J = r - 1$. If $k = 1$, reduction modulo r is injective on $K_{n'}$, which has $r - 1$ elements; so $K_{n'} = J \subset H$, and $K_{n'} \neq \{1\}$. Let $k \geq 2$, and $B' = J \cap K_r$. As in Step 2, $\tau(B') = B'$ and $B' + (u-1)d/x = B'$ for $u \in B'$; if $B' \neq \{1\}$, an element $u \neq 1$ of B' has $u \not\equiv 1 \pmod{r^k}$ and so $(u-1)d \not\equiv 0 \pmod n$, which gives the lemma. If $B' = \{1\}$, then J has $r - 1$ elements and is the subgroup of order $r - 1$ of $K_{n'} \cong (\mathbb{Z}/r^k)^\times$, whose power sums of degrees 1 to $r - 2$ vanish modulo r^k (Lemma 3.5). With $h_0' \in J$ above $-d$ and $e_0 \in J$ outside $\tau(J \setminus \{h_0'\})$, $(J \setminus \{h_0'\}) + d = x(J \setminus \{e_0\})$, and the computation of Step 1 modulo r^k, with $k_q = r - 1 \equiv -1$ and d units modulo r, gives $r^k \mid (1 - k_q)(1 + k_q) = r(2 - r)$, which is impossible. □

At odd N up to three numerators share primes with N, and the exceptional h lie in up to three cosets. Let $N > 1$ be odd, H, d, x, τ as above with $n = N$, and $n_1, n_2, n_3 > 1$ divisors of N with $\operatorname{lcm}(n_i, n_j) = N$ for $i \neq j$; put $e_i = N/n_i$, which are pairwise coprime, $E_i = \{h \in H : n_i \mid h + d\}$, $E = E_1 \cup E_2 \cup E_3$ and $B_m = H \cap K_m$, $B_i = B_{n_i}$. Then each E_i is empty or a coset of B_i; $E_i \cap E_j \subset \{-d\}$ for $i \neq j$; d is prime to n_i if $E_i \neq \emptyset$; for each prime $s \mid N$ at most one i has $s \nmid n_i$; and $-d \not\equiv \pm 1$ modulo every prime of N, as $1 \pm d$ are units.

Lemma 3.8. *Let $n > 1$ be odd, $r > 1$ a divisor of n, and let* (T) *hold for $E = \{h \in H : r \mid h + d\}$. Then H contains K_f for a proper divisor f of n, and if $E \neq \emptyset$, r is a prime, $r \geq 5$, $r \nmid d$, and H maps onto $(\mathbb{Z}/r)^\times$.*

Proof. Reduction is an isomorphism $(\mathbb{Z}/2n)^\times \to (\mathbb{Z}/n)^\times$. Let $\tilde{H}$ be the preimage of H and $\tilde{d}$ the even lift of d; then $1 \pm \tilde{d}$ are units, $2\tilde{d} \not\equiv 0 \pmod{2n}$, $(1 - \tilde{d})/(1 + \tilde{d}) \in \tilde{H}$, and (T) holds for $\tilde{H}$, $\tilde{d}$ and the set of $\tilde{h} \in \tilde{H}$ with $r \mid \tilde{h} + \tilde{d}$. Lemmas 3.6 and 3.7 at the modulus $2n$ give $\tilde{K} \subset \tilde{H}$, $\tilde{K} \neq \{1\}$, the units $\equiv 1$ modulo some $f \mid 2n$, which we may take odd as units modulo $2n$ are odd; it reduces to $K_f \subset H$, $K_f \neq \{1\}$, so f is a proper divisor of n. The rest is Lemma 3.6(ii). □

Lemma 3.9. *Let $m \mid N$, $B = B_m$, and $a \in H$ with $aB \cap E = \emptyset$, and let* (T) *hold for E. Then $B+(u-1)d/a = B$ for every $u \in B$, and $K_f \subset H$ with $f = \gcd(N, \{(u-1)d : u \in B\})$. If d is a unit and $B \neq \{1\}$, then f is a proper divisor of N.*

Proof. By (T), τ maps aB injectively into H, and its image is $\equiv (a+d)/x \pmod m$, so it is the coset $\tau(a)B$: $aB + d = x\tau(a)B$. Multiplying by $u \in B$ gives $aB + ud = aB + d$, so $B + (u-1)d/a = B$. As in Step 2 of Lemma 3.7, $1 + f\mathbb{Z}/N = K_f \subset B$. If d is a unit and $u \neq 1$, then $(u-1)d \not\equiv 0$. □

Lemma 3.10. *Let s be a prime, $\mu \subset (\mathbb{Z}/s)^\times$ the subgroup of order $k \geq 5$, $d, x \in (\mathbb{Z}/s)^\times$ with $-d \in \mu$, and suppose that $(\mu \setminus \{-d, \pi\}) + d \subset x\mu$ for some $\pi \in \mu$, $\pi \neq -d$. Then $k = s-1$.*

Proof. Here $s \geq 7$. Let f_1, f_2 be the two elements of $x\mu$ outside $(\mu \setminus \{-d, \pi\}) + d$, and $c = \pi + d$. The power sums of degree $1 \leq j \leq k-1$ over μ vanish, so

$$k d^j - c^j + f_1^j + f_2^j = 0 \quad \text{in } \mathbb{Z}/s, \qquad 1 \leq j \leq k-1.$$

For $R(T) = (1-dT)^k(1-f_1T)(1-f_2T)/(1-cT)$ in $(\mathbb{Z}/s)[[T]]$ this says $TR'/R \equiv 0 \pmod{T^k}$, and as $1, \dots, k-1$ are invertible modulo s, $R \equiv 1 \pmod{T^k}$, that is, $(1-dT)^k(1-\sigma_1 T + \sigma_2 T^2) \equiv 1 - cT \pmod{T^k}$ with $\sigma_1 = f_1 + f_2$, $\sigma_2 = f_1 f_2$. The coefficients of T^2, T^3, T^4 vanish, so $(1, \sigma_1/d, \sigma_2/d^2)$ lies in the kernel of the matrix with rows $(\binom{k}{j}, \binom{k}{j-1}, \binom{k}{j-2})$, $j = 2, 3, 4$, modulo s, whose determinant is $k^2(k+1)^2(k-1)(k+2)/144$. As $s \geq 7$ and $k \leq s-1$, s divides $k+1$ or $k+2$; and $s = k+2$ would give $k \mid k+1$. So $s = k+1$. □

Proposition 3.11. *If* (T) *holds for $E = E_1 \cup E_2 \cup E_3$, then H contains K_f for a proper divisor f of N.*

Proof. Suppose not; at odd N, $K_f \neq \{1\}$ for every proper divisor f, so H contains no $K_f \neq \{1\}$.

If d is not a unit, at most one E_i is non-empty, as d is prime to n_i when $E_i \neq \emptyset$ and $\operatorname{lcm}(n_i, n_j) = N$. If $E_i \neq \emptyset$, then $E = E_i$, and if all are empty, then $-d \notin H$ and $E = \{h \in H : N \mid h + d\}$; in both cases Lemma 3.8 gives a contradiction.

Let d be a unit. By Lemma 3.9, for every $m \mid N$ with $B_m \neq \{1\}$, every coset of B_m in H meets E. For a prime $s \mid N$ let $A_s = B_s$ and $\bar{H}$ the image of H in $(\mathbb{Z}/s)^\times$. If $A_s \neq \{1\}$, there is exactly one i_0 with $s \nmid n_{i_0}$, and B_{i_0} maps onto $\bar{H}$. Indeed, A_s meets some E_i, in an $h \equiv 1 \pmod s$; $s \mid n_i$ would give $x \equiv 0 \pmod s$, so $s \nmid n_i$, and $i_0 = i$ is unique. For $\pi \in \bar{H} \setminus \{-d\}$ the coset of A_s above π meets E, not in the E_j with $s \mid n_j$, which lie above $-d$; so it meets E_{i_0}. So a coset of the image of B_{i_0} contains $\bar{H} \setminus \{-d\}$, and as $1, -1, -d$ are distinct modulo s, it is all of $\bar{H}$.

Case 1: $A_s \neq \{1\}$ for every prime s of N. Then $s^{v_s(N)} \mid e_{i_0(s)}$ for every s, so $N = e_1e_2e_3$. Take i with $e_i > 1$; then $B_i \neq \{1\}$, and the coset B_i meets some E_l: an $h \equiv 1 \pmod{n_i}$ with $h \equiv -d \pmod{n_l}$, so $\gcd(n_i, n_l)$ divides the unit x. Hence $l \neq i$, and the third index k has $e_k = \gcd(n_i, n_l) = 1$: $N = e_ie_l$ with $n_i = e_l > 1$ and $n_l = e_i$. In $G = (\mathbb{Z}/e_i)^\times \times (\mathbb{Z}/e_l)^\times$, $B_i = H \cap ((\mathbb{Z}/e_i)^\times \times 1)$, E_i is the set of elements of H with second coordinate $-d$, E_l those with first coordinate $-d$, and $E_k \subset \{(-d, -d)\}$. A prime of e_l gives $B_l \neq \{1\}$, and the cosets of B_l are the fibers of the first projection; each fiber over $a \neq -d$ meets E, hence E_i, so $(a, -d) \in H$ for every $a \neq -d$ in the first projection H_i of H. As in the previous paragraph, $H_i \times 1 \subset H$, so $H = H_i \times H_l$ and $-d \in H_l$. For $b \in H_l$ with $b \not\equiv -d$, $(1, b) \notin E$, so $b + d$ is a unit modulo e_l and $(b+d)/x \in H_l$; Lemma 3.8 at the modulus e_l with $r = e_l$ makes e_l a prime and $H_l = (\mathbb{Z}/e_l)^\times$. Then $K_{e_i} = 1 \times (\mathbb{Z}/e_l)^\times \subset H$, a contradiction.

Case 2: $A_{s_0} = \{1\}$ for some prime s_0. Then H embeds in $(\mathbb{Z}/s_0)^\times$ and is cyclic, and for the at least two i with $s_0 \mid n_i$, $B_i = \{1\}$ and $|E_i| \le 1$. Suppose first $B_i \ne \{1\}$ for some i. Every coset of B_i meets E, and H/B_i, the image of H modulo n_i, contains $-1 \ne 1$. If $E_i \ne \emptyset$, the image contains the distinct elements $1, -1, -d$, so there are at least three cosets, each met by the coset E_i or by one of the at most two points of $E_j \cup E_k$; so the image has order 3, which is odd, although it contains $-1 \ne 1$. So $E_i = \emptyset$, $[H : B_i] = 2$, and the two other $E_j = \{h_j\}$, $E_k = \{h_k\}$ lie in different cosets; but $h_j \equiv -d \equiv h_k \pmod{s_0}$, so $h_j = h_k$. Suppose now every $B_i = \{1\}$. If $-d \in H$, or $-d \notin H$ and at most one E_i is non-empty, E is $\{h \in H : \ r \mid h + d\}$ for $r = N$ or $r = n_i$, and Lemma 3.8 gives a contradiction. Otherwise $E_i = \{h_i\}$ and $E_j = \{h_j\}$ with $i \ne j$ and $h_i \ne h_j$. Then $A_s = \{1\}$ for every prime s of N, by the first paragraph of the case d a unit, so H embeds modulo every prime of N, and no prime divides both n_i and n_j; so $N = e_i e_j$, $n_i = e_j$ and $n_j = e_i$ are coprime and greater than 1, $n_k = N$ and $E_k = \emptyset$. For a prime $s \mid e_j$, modulo s the group H is the subgroup μ of order $|H|$, $h_i \equiv -d$, and $(\mu \setminus \{-d, h_j\}) + d \subset x\mu$ by (T). Here $|H| \ge 4$ is even, as $\rho \notin \{\pm 1\}$. If $|H| \ge 6$, Lemma 3.10 gives $s = |H| + 1$, and the same holds for the primes of e_i; so N is a power of one prime, against $N = e_i e_j$. If $|H| = 4$, then $\rho^2 = -1$, so $d^2 = -1$ and $\rho = (1-d)^2/(1-d^2) = -d$, and $-d \in H$, which is excluded. □

End of the proof of Theorem 1.4. Recall that H is closed, of conductor N', and that $d = x - 1$. Here $1 + d = x$ and $1 - d = 2 - x$ are units, $2d \not\equiv 0$ and $\rho \in H$ (Lemma 3.4). Let N be even, p_e the even numerator, and $r = n_e$ if n_e is odd and $r = \infty$ otherwise; as $h + d$ is odd for $h \in H$ and n_i is even for the odd numerators, $n_i \mid h + d$ for some i only if $r \mid h + d$. By Lemma 3.4, (T) holds for $E = \{h \in H : \ r \mid h + d\}$, and Lemmas 3.6 and 3.7 give some $K_f \ne \{1\}$ in H. Let N be odd. The n_i are greater than 1 and $\operatorname{lcm}(n_i, n_j) = N/\gcd(g_i, g_j) = N$; by Lemma 3.4, (T) holds for $E = E_1 \cup E_2 \cup E_3$, and Proposition 3.11 gives some $K_f \ne \{1\}$ in H. In both cases this contradicts $c = N'$. □

4. Triangles without a witness

This section lists the triangles without a witness for $N > 58$ and proves condition (12). For even N we write $\nu = N/2$. The families are

$$\mathcal{A}_d = (1, (N-d)/2 - 1, (N+d)/2)/N \quad (d \mid N,\ N/d \ge 3 \text{ odd}),$$
$$\Lambda = (1, (\nu-1)/2, (3\nu-1)/2)/N \quad (\nu \text{ odd}),$$
$$\Gamma_1 = (1, \nu-2, \nu+1)/N, \quad \Theta_0 = (2, \nu-3, \nu+1)/N \quad (4 \mid N),$$
$$\Gamma_2 = (2, N/4-1, 3N/4-1)/N \quad (8 \mid N),$$
$$\Theta_1 = (1, 4, N-5)/N, \quad \Theta_2 = (4, \nu-5, \nu+1)/N \quad (N \equiv 4 \pmod 8),$$
$$\Theta_3 = (4, \nu-3, \nu-1)/N, \quad \Gamma_4 = (4, N/4-2, 3N/4-2)/N \quad (N \equiv 4 \pmod 8),$$

and the family $\mathcal{B}$ of the triangles

$$\mathcal{B}_{k,d} = (k, \nu - \nu/d - k, \nu + \nu/d)/N,$$

where N is even, $d \ge 5$ is an odd divisor of N with $d \mid 2k-1$, k is an odd prime not dividing N, $k \le N/(2d)$, and every prime $\ell < 2k$ with $\ell \ne k$ and $\ell \not\equiv 1 \pmod d$ divides N. We write $\mathcal{B}_k = \mathcal{B}_{k,2k-1}$. The member $\mathcal{A}_{N/3}$ of $\mathcal{A}$ has the numerator $2N/3$; $\mathcal{A}_d$ with $d = 2$ is Γ_1 in form, but $N/2$ is odd there and even on Γ_1.

Proposition 4.1. *Let $N > 58$ and let Δ be scalene and not in (1.1). If Δ has no witness, then it has a numerator $2N/3$, or it is $\mathcal{A}_d$ with $N/d \ge 5$, or it lies in one of the other nine families above.*

family	source	treated by
$\mathcal{A}_d$, $N/d \geq 5$	[16, Theorem 4.1(a)]	Theorem 6.20 ($d = 1$), Theorem 6.19 ($d \geq 3$), Theorem 6.17 ($d = 2$)
$\mathcal{B}_{k,d}$	[16, Theorem 4.1(a), (b)]	Theorem 6.21, Proposition 8.3
Γ_1, Θ_0, Θ_2	[16, Theorem 4.1(a)]	Theorem 6.11; Theorem 6.16, Theorem 6.18(a); Theorem 6.18(b)
Θ_3	[19, Theorem 1.7]	Theorem 6.18(c)
Θ_1, Λ, Γ_2, Γ_4	[26, Theorem 4.1]	Theorem 6.18(b); Theorem 6.15; Theorem 6.12; Theorem 6.13
numerator $2N/3$		Theorem 6.3

TABLE 2. The triangles without a witness for $N > 58$, off (1.1), where each family is found, and the statements that treat it. The denominators 2^j, $2P$ and $3P$ are treated in Section 5, and $N \leq 400$ in Section 8.

Proof. We sort by the largest numerator p_3. If Δ is acute, Part I lists the triangles without a witness [19, Theorem 1.7]; the scalene ones with $N > 42$ are the Θ_3 with $N \equiv 4 \pmod 8$. If Δ is right, then after renumbering $\Delta = (a, \nu - a, \nu)/N$ with a odd and prime to N, and by Proposition 10.1 of Part I, whose proof is Apisa's argument for his Lemma 7.4 [2], Δ has a witness unless $a \in \{1, \nu-1, \nu-2\}$; these are $(1, k, k+1)/(2k+2)$ and $(2, 2k+1, 2k+3)/(4k+6)$, which are in (1.1) [19, Proposition 10.1].

If $N/2 < p_3 \leq 2N/3$, let $s = 2p_3 - N$. By [16, Theorem 4.1(a)] the triangles without a witness are the family $\mathcal{A}$ of that paper ($p_1 = 1$, $s \mid N$, N/s odd), which is $\mathcal{A}_d$ with $d = s$; its family $\mathcal{B}$ ($s \mid N$, $d = N/s$ odd, $2 \leq p_1 \leq s/2$, and a condition on the units a with $2a \not\equiv 2$ and $[ap_1] < 2p_1$); its family $\mathcal{C}$, which consists of Γ_1 and Θ_0 at $4 \mid N$ and Θ_2 at $N \equiv 4 \pmod 8$; and thirty triangles with $N \leq 48$. A member of that family $\mathcal{B}$ has $p_3 = \nu + \nu/d$ and $p_2 = \nu - \nu/d - k$ with $k = p_1$, and by [16, Theorem 4.1(b)]: if $\gcd(k, N) > 1$, then $k = 3$ and $N = 3s$, so $d = 3$; if $\gcd(k, N) = 1$, then k is prime, $d \mid 2k - 1$, and every prime $\ell < 2k$ with $\ell \neq k$ and $\ell \not\equiv 1 \pmod d$ divides N. The members of $\mathcal{A}$ with $N/d = 3$ and those of $\mathcal{B}$ with $d = 3$ have $p_3 = 2N/3$. Let $d \geq 5$. Then $\gcd(k, N) = 1$; $\ell = 2$ is a prime $< 2k$, $\not\equiv 1 \pmod d$, and $\neq k$ unless $k = 2$, which would give $d \mid 3$; so N is even, $k \geq 3$ is odd, $k \leq s/2 = N/(2d)$, and $\Delta = \mathcal{B}_{k,d}$.

If $p_3 > 2N/3$, then by [26, Theorem 4.1] the triangles without a witness are $(1, 1, N-2)/N$, $(1, 2, N-3)/N$ at even N, which is in (1.1), Θ_1 at $N \equiv 4 \pmod 8$, Λ, Γ_2 at $8 \mid N$, Γ_4 at $N \equiv 4 \pmod 8$, and seven triangles with $N \leq 42$. On obtuse triangles the witness of [16] and [26], a unit a with $2a \not\equiv 2$ such that $[ap_i] < [2p_i]$ for two indices i, is ours [19, Lemma 2.7]. As $N > 58$, the single triangles do not occur. □

4.1. **Condition (12).**

Proposition 4.2. *Let $12 \mid N$, $N > 58$, and let Δ be scalene with no numerator $N/3$ or $2N/3$. Then every closed $S \ni 1$ with $S \cap G \supset H_{12}$ is F. So Δ satisfies* (12).

Throughout this subsection $12 \mid N$, $N_3 = N/3$, $v = v_3(N)$, and Δ is scalene with no numerator $N/3$ or $2N/3$. The subgroups of G containing H_{12} correspond to the subgroups of $(\mathbb{Z}/12)^\times/\{\pm 1\}$, a group of order 2, so they are H_{12} and G. By Theorem 1.5, a closed S with $S \cap G = G$ is F, as $N > 30$. So Proposition 4.2 says that no closed $S \ni 1$ has $S \cap G = H_{12}$.

For a unit β modulo N_3 the character 3β is well defined modulo N, $\gcd(3\beta, N) = 3$, and every element of O_3 has this form. It lies in $\Phi \cup -\Phi$, since $3\beta p_i \equiv 0 \pmod N$ would mean $N_3 \mid p_i$, and it is odd, since β is odd ($4 \mid N_3$). So $O_3 \subset F$. An *instance* is a pair (x, β) of a holomorphic unit $x \equiv 2 \pmod 3$ and a unit β modulo N_3 such that 3β is holomorphic, $\beta \equiv -x \pmod 4$, and $1 - x - 3\beta$ is a unit.

Lemma 4.3. *Let $S \ni 1$ be closed with $S \cap G \supset H_{12}$. If $v = 1$ and an instance exists, or if $v \geq 2$ and there are instances (x, β) and (x_2, β_2) with $\beta \not\equiv \beta_2 \pmod 3$, then $S \cap G = G$.*

Proof. Suppose $H = S \cap G = H_{12}$. For an instance (x, β) let $b = 3\beta$ and $a' = 1 - x - b$, a unit. Modulo 3, $a' \equiv 1 - 2 - 0 = -1$. Modulo 4, $b \equiv -\beta \equiv x$, so $a' \equiv 1 - 2x \equiv -1$, as x is odd. So $a' \equiv -1 \pmod{12}$ and $a' \in H_{12} \subset S$. Rule (iii) with $u = x$, the holomorphic $x \in xS$, a' and the holomorphic $b = 1 - x - a'$ gives $b \in xS$, that is $x^{-1}b \in S \cap O_3$.

Let $v = 1$. By Lemma 2.6, $K_{N_3} \subset H$. As $3 \nmid N_3$ and $4 \mid N_3$, the Chinese remainder theorem gives a unit $u \equiv 1 \pmod{N_3}$ with $u \equiv 2 \pmod 3$; then $u \equiv 5 \pmod{12}$, so $u \notin H_{12}$, a contradiction.

Let $v \geq 2$, so $12 \mid N_3$. By Lemma 2.6, $S \cap O_3$ is one H-orbit, so $x_2^{-1} \cdot 3\beta_2 \equiv h\, x^{-1} \cdot 3\beta \pmod N$ for some $h \in H_{12}$, that is $\beta_2 \equiv h x_2 x^{-1} \beta \pmod{N_3}$. Modulo 4, $\beta \equiv -x$ and $\beta_2 \equiv -x_2$ give $h \equiv 1 \pmod 4$, so $h \equiv 1 \pmod{12}$. Modulo 3, $x \equiv x_2 \equiv 2$ then gives $\beta_2 \equiv \beta$, a contradiction.

So $H \neq H_{12}$, and $H = G$ as $H \supset H_{12}$. □

To produce instances we count holomorphic units in congruence classes modulo 4, 3 and 12, at the level N and at the level N_3. For $n \geq 2$, a *triple modulo n* is $(p_1, p_2, p_3) \in \mathbb{Z}^3$ with $p_1 + p_2 + p_3 \equiv 0 \pmod n$, $n \nmid p_j$ for each j, and $\gcd(p_1, p_2, p_3, n) = 1$. Put $g_j = \gcd(p_j, n)$, $n_j = n/g_j \geq 2$ and $q_j = p_j/g_j$, a unit modulo n_j. For a unit β modulo n put $s(\beta) = 3 - 2\sum_j \{\beta p_j/n\}$, and call β *holomorphic for the triple* if $s(\beta) = 1$.

Lemma 4.4. (a) *For a triple modulo n and a unit β, $s(\beta) \in \{1, -1\}$, $s(-\beta) = -s(\beta)$, and $s(\beta) = \sum_j s_j(\beta)$ with $s_j(\beta) = 1 - 2\{\beta q_j/n_j\}$.*

(b) $\operatorname{lcm}(n_i, n_j) = n$ *for $i \neq j$.*

(c) *The numerators of Δ form a triple modulo N, and a unit is holomorphic for it if and only if it is a holomorphic character. They also form a triple modulo N_3, and a unit β modulo N_3 is holomorphic for it if and only if the character 3β is holomorphic.*

Proof. (a) Each $\{\beta p_j/n\}$ lies in $(0, 1)$, as β is a unit and $n \nmid p_j$, and their sum is an integer, as $\beta \sum_j p_j \equiv 0$; so it is 1 or 2, and $s = \pm 1$. Then $\{-t\} = 1 - \{t\}$ for $t \notin \mathbb{Z}$ gives $s(-\beta) = -s(\beta)$, and $\beta p_j/n = \beta q_j/n_j$. (b) A common divisor of g_i and g_j divides p_i, p_j and n, hence $p_k \equiv -p_i - p_j \pmod n$, hence $\gcd(p_1, p_2, p_3, n) = 1$. So $\gcd(g_i, g_j) = 1$ and $\operatorname{lcm}(n/g_i, n/g_j) = n/\gcd(g_i, g_j) = n$. (c) At level N: $0 < p_j < N$, $\sum_j p_j = N$, and a unit x is holomorphic if and only if $\sum_j \{x p_j/N\} = 1$. At level N_3: $N_3 \nmid p_j$ as $p_j \notin \{N/3, 2N/3\}$, $\sum_j p_j \equiv 0 \pmod{N_3}$, $\gcd(p_1, p_2, p_3) = 1$, and $\{3\beta p_j/N\} = \{\beta p_j/N_3\}$; as $3\beta \in \Phi \cup -\Phi$, it is holomorphic if and only if $\sum_j \{3\beta p_j/N\} = 1$. □

A *datum* on n is $\mathfrak{t} = (m, c, E, e)$: $m \in \{1, 3, 4, 12\}$ with $m \mid n$; c a unit modulo m; E a set of primes $\ell \geq 5$ dividing n; and $e = (e_\ell)_{\ell \in E}$ with $e_\ell \not\equiv 0 \pmod \ell$. Its *congruence set* is

$$C(n; \mathfrak{t}) = \{y \in (\mathbb{Z}/n)^\times : \ y \equiv c \pmod m, \ y \not\equiv e_\ell \pmod \ell \text{ for } \ell \in E\},$$

of size $|C(n; \mathfrak{t})| = \frac{\varphi(n)}{\varphi(m)} \prod_{\ell \in E} \frac{\ell - 2}{\ell - 1} > 0$. For $n' \mid n$ with $n' \geq 2$, the *restriction* $\mathfrak{t}|n'$ keeps the factor 4 of m if $4 \mid n'$, the factor 3 of m if $3 \mid n'$, the primes of E that divide n', and the

same classes; for a unit q modulo n', $q\mathfrak{t}|n'$ multiplies c and every e_ℓ by q. Let $\alpha(n;\mathfrak{t})$ be the average of $1-2y/n$ over $y \in C(n;\mathfrak{t})$, y read in $(0,n)$, and $A^\sharp(n)$ the maximum of $-\alpha(n;\mathfrak{t})$ over all data on n. The map $y \mapsto n-y$ shows $\alpha(n;(1,1,\emptyset,\emptyset)) = 0$, so $A^\sharp(n) \ge 0$. Let ϖ be the multiplicative function of $n \ge 2$ with $\varpi(2) = 2$, $\varpi(2^k) = 2^{2-k}$ for $k \ge 2$, $\varpi(3^k) = 3^{1-k}$ and $\varpi(\ell^k) = 3/(\ell^{k-1}(\ell-2))$ for $\ell \ge 5$.

Lemma 4.5. *For a triple modulo n and a datum $\mathfrak{t}$ on n, with $C = C(n;\mathfrak{t})$, the number of $\beta \in C$ holomorphic for the triple is*

$$\tfrac{1}{2}|C|\,(1+\alpha_1+\alpha_2+\alpha_3), \qquad \alpha_j = \alpha(n_j;\, q_j\mathfrak{t}|n_j).$$

In particular, if no $\beta \in C$ is holomorphic for the triple, then $A^\sharp(n_1)+A^\sharp(n_2)+A^\sharp(n_3) \ge 1$.

Proof. By Lemma 4.4(a) the number is $\sum_{\beta\in C}(1+s(\beta))/2 = |C|/2 + \frac{1}{2}\sum_j \sum_{\beta\in C} s_j(\beta)$, and $s_j(\beta)$ depends only on β modulo n_j. Reduction modulo n_j carries the uniform measure on C to the uniform measure on $C_j = C(n_j;\mathfrak{t}|n_j)$. Indeed, by the Chinese remainder theorem $(\mathbb{Z}/n)^\times = \prod_\ell (\mathbb{Z}/\ell^{k_\ell})^\times$ and $C = \prod_\ell C^{(\ell)}$, where $C^{(2)}$ is given by $y \equiv c \pmod 4$ if $4 \mid m$, $C^{(3)}$ by $y \equiv c \pmod 3$ if $3 \mid m$, $C^{(\ell)}$ by $y \not\equiv e_\ell \pmod \ell$ for $\ell \in E$, and $C^{(\ell)}$ is the whole factor otherwise; reduction is the product of the surjections $(\mathbb{Z}/\ell^{k_\ell})^\times \to (\mathbb{Z}/\ell^{j_\ell})^\times$ with $j_\ell = v_\ell(n_j)$. If $C^{(\ell)}$ is the whole factor, or its condition is a condition modulo ℓ^{j_ℓ} (that is, $j_\ell \ge 2$ for $\ell = 2$ and $j_\ell \ge 1$ for odd ℓ), then $C^{(\ell)}$ is the full preimage of the set given by the same condition, and the uniform measure goes to the uniform measure; otherwise the target factor is trivial ($j_\ell = 0$, or $\ell = 2$ and $j_2 = 1$), and $\mathfrak{t}|n_j$ has no condition at ℓ. Hence $\sum_{\beta\in C} s_j(\beta)$ is $|C|$ times the average of $1 - 2\{wq_j/n_j\}$ over $w \in C_j$, and $y = wq_j$ runs over $C(n_j; q_j\mathfrak{t}|n_j)$, with $\{wq_j/n_j\} = y/n_j$ for y read in $(0,n_j)$. This is the formula. If the number is 0, then $\alpha_1+\alpha_2+\alpha_3 = -1$, and $-\alpha_j \le A^\sharp(n_j)$. □

Lemma 4.6. *Let $\mathfrak{t} = (m,c,E,e)$ be a datum on n and $\hat{n} = \operatorname{lcm}(m, \operatorname{rad} n)$. Then $\alpha(n;\mathfrak{t}) = (\hat{n}/n)\,\alpha(\hat{n};\mathfrak{t})$ and $|\alpha(n;\mathfrak{t})| \le \varpi(n)$. Hence $A^\sharp(n) \le \varpi(n)$, and $A^\sharp(n)$ is the maximum over $m \in \{1,3,4,12\}$ with $m \mid n$ of $(\hat{n}_m/n)A^\sharp_m(\hat{n}_m)$, where $\hat{n}_m = \operatorname{lcm}(m, \operatorname{rad} n)$ and $A^\sharp_m$ is the maximum of $-\alpha$ over the data with that m.*

Proof. With $((t))$ as in Lemma 2.12, $1-2y/n = -2((y/n))$ for $0 < y < n$. The indicator of "$y \not\equiv e_\ell \pmod \ell$ for $\ell \in E$" is $\sum_{\delta \mid \prod E} (-1)^{\omega(\delta)}[y \equiv e_\ell \pmod \ell \text{ for } \ell \mid \delta]$. For each δ, let $q_\delta = m\delta$, a divisor of n, and c_δ the class modulo q_δ that is $\equiv c \pmod m$ and $\equiv e_\ell \pmod \ell$ for $\ell \mid \delta$, a unit class. Let R_δ be the product of the primes of n not dividing q_δ. By Lemma 2.12(b) with $a = 1$ and $q = q_\delta$,

$$\sum_{y \in C(n;\mathfrak{t})} \Big(\Big(\frac{y}{n}\Big)\Big) = \sum_{\delta \mid \prod E} (-1)^{\omega(\delta)} \sum_{e' \mid R_\delta} \mu(e') \Big(\Big(\frac{t_{\delta,e'}}{q_\delta}\Big)\Big),$$

where $t_{\delta,e'} \equiv c_\delta e'^{-1} \pmod{q_\delta}$; the right-hand side depends on n only through its set of primes. Among the n with a given set of primes and $m \mid n$, $|C(n;\mathfrak{t})|$ is proportional to n; and $\hat{n}$ has the primes of n, with $m \mid \hat{n} \mid n$. As $\alpha = -2\sum((y/n))/|C|$, this gives $\alpha(n;\mathfrak{t}) = (\hat{n}/n)\alpha(\hat{n};\mathfrak{t})$. For the bound, each term has absolute value at most $\frac{1}{2}$ and there are $\sum_\delta 2^{\omega(R_\delta)} = 2^{\omega(n)-\omega(m)}(3/2)^{|E|}$ terms; with $\varphi(m) = 2^{\omega(m)}$ for the four values of m,

$$|\alpha(n;\mathfrak{t})| \le \frac{2^{\omega(n)}}{\varphi(n)} \prod_{\ell \in E} \frac{3(\ell-1)}{2(\ell-2)}.$$

Each factor is larger than 1, so the bound is largest when E is the set of all primes $\ell \geq 5$ of n, where it is $\varpi(n)$: the factor of ℓ^k is $2/\varphi(2^k)$ at $\ell = 2$, $2/\varphi(3^k)$ at $\ell = 3$, and $3/(\ell^{k-1}(\ell-2))$ at $\ell \geq 5$. □

Proposition 4.7. (a) *$A^\sharp(n) \leq 5/6$ for every $n \geq 2$, with equality only at $n = 12$, and $B^\sharp = \{n : A^\sharp(n) \geq 1/12\}$ has 76 elements, the largest 1,020, listed with their values in the supplement (§S8).*

(b) *Let $\bar{A}(n) = A^\sharp(n)$ if $\varpi(n) \geq 1/12$ and $\bar{A}(n) = \varpi(n)$ otherwise. The integers $n = \operatorname{lcm}(n_1, n_2)$ with $n_1, n_2 \in B^\sharp$, $A^\sharp(n_1) \geq A^\sharp(n_2)$ and $A^\sharp(n_1)+2A^\sharp(n_2) \geq 1$, for which some $n_3 \geq 2$ dividing n with $\operatorname{lcm}(n_3, n_1) = \operatorname{lcm}(n_3, n_2) = n$ has $A^\sharp(n_1) + A^\sharp(n_2) + \bar{A}(n_3) \geq 1$, form the set $\mathcal{N}_0$ of the 39 integers 3, 4, 6, 8, 12, 15, 18, 20, 24, 28, 30, 36, 42, 48, 60, 66, 72, 84, 90, 96, 108, 120, 132, 156, 168, 180, 204, 228, 240, 252, 264, 276, 300, 336, 396, 420, 660, 924 and 1,020.*

(c) *Let $12 \mid N$, $N > 58$, with N or $N/3$ in $\mathcal{N}_0$, other than 60, 72, 108 and 180, and Δ a scalene triangle at N with $\gcd(p_1, p_2, p_3) = 1$ and no numerator $N/3$ or $2N/3$. If $9 \nmid N$, an instance exists; if $9 \mid N$, there are instances (x, β) and (x_2, β_2) with $\beta \not\equiv \beta_2 \pmod 3$.*

(d) *At $N = 60$, 72, 108 and 180, for every such triangle, the smallest closed set containing H_{12} is F.*

We find these facts as follows. By Lemma 4.6, $A^\sharp(n) \leq \varpi(n)$; every prime power factor of ϖ other than $\varpi(2) = 2$ is at most 1 and tends to 0 with the prime power, so the n with $\varpi(n) \geq 1/12$ are finitely many: 394 of them, the largest 30,030. For each of them $A^\sharp(n)$ is computed exactly from the formula in the proof of Lemma 4.6, at the levels $\hat{n}_m$, over all data; every other n has $A^\sharp(n) < 1/12$. This gives (a), and (b) is a finite search. For (c) the instances are listed by enumeration, and for (d) the closure of H_{12} is computed by iterating the rules until nothing is added [20].

Lemma 4.8. *If $n \notin \mathcal{N}_0$, then for every triple modulo n and every datum $\mathfrak{t}$ on n, the set $C(n; \mathfrak{t})$ contains a unit holomorphic for the triple.*

Proof. If not, Lemma 4.5 gives $A^\sharp(n_1) + A^\sharp(n_2) + A^\sharp(n_3) \geq 1$. Number the n_j so that $A_1 \geq A_2 \geq A_3$, with $A_j = A^\sharp(n_j)$. As $A_1 \leq 5/6$, $A_2 + A_3 \geq 1/6$, so $A_2 \geq 1/12$ and $n_1, n_2 \in B^\sharp$. Moreover $\operatorname{lcm}(n_1, n_2) = n$ by Lemma 4.4(b), $A_1 + 2A_2 \geq 1$, and $n_3 \geq 2$ divides n, has $\operatorname{lcm}(n_3, n_1) = \operatorname{lcm}(n_3, n_2) = n$, and has $A^\sharp(n_3) \geq 1 - A_1 - A_2$. By Proposition 4.7(b), $n \in \mathcal{N}_0$. □

Proof of Proposition 4.2. Let $S \ni 1$ be closed with $S \cap G \supset H_{12}$. By the first paragraph of this subsection it suffices to show $S \cap G = G$, and by Lemma 4.3 it suffices to find one instance if $v = 1$ and two instances (x, β_+), (x_2, β_-) with $\beta_+ \equiv 1$ and $\beta_- \equiv 2 \pmod 3$ if $v \geq 2$.

Suppose first that $N \notin \mathcal{N}_0$ and $N_3 \notin \mathcal{N}_0$. By Lemma 4.4(c) and Lemma 4.8 at the level N with the datum $(3, 2, \emptyset, \emptyset)$, there is a holomorphic unit $x \equiv 2 \pmod 3$. Let E be the set of primes $\ell \geq 5$ dividing N with $x \not\equiv 1 \pmod \ell$; they divide N_3. For $\ell \in E$ let $e_\ell \equiv (1-x)/3 \pmod \ell$, which is not 0. If $v = 1$, then $4 \mid N_3$ and $3 \nmid N_3$, and Lemma 4.8 at the level N_3 with the datum $(4, -x, E, e)$ gives a unit β modulo N_3 with 3β holomorphic, $\beta \equiv -x \pmod 4$ and $3\beta \not\equiv 1 - x \pmod \ell$ for $\ell \in E$. If $v \geq 2$, then $12 \mid N_3$, and the data $(12, c_\pm, E, e)$ with $c_\pm \equiv -x \pmod 4$ and $c_\pm \equiv \pm 1 \pmod 3$ give two such units $\beta_\pm$, with $\beta_\pm \equiv \pm 1 \pmod 3$. In each case $1 - x - 3\beta$ is a unit modulo N: it is odd, as x and β are odd; it is $\equiv 1 - 2 - 0 \pmod 3$; at a prime $\ell \geq 5$ of N with $x \equiv 1 \pmod \ell$ it is $\equiv -3\beta \not\equiv 0$, as $\ell \mid N_3$ and β is a unit modulo N_3; and at $\ell \in E$ it is $\not\equiv 0$ by the choice of β. So these pairs are instances.

Otherwise N or N_3 lies in $\mathcal{N}_0$. With $12 \mid N$ and $N > 58$ these are the 44 values 60, 72, 84, 96, 108, 120, 132, 144, 156, 168, 180, 204, 216, 228, 240, 252, 264, 276, 288, 300, 324, 336, 360, 396, 420, 468, 504, 540, 612, 660, 684, 720, 756, 792, 828, 900, 924, 1,008, 1,020, 1,188, 1,260, 1,980, 2,772 and 3,060. At each of them other than 60, 72, 108 and 180, the instances required above exist on every scalene triangle with $\gcd(p_1, p_2, p_3) = 1$ and no numerator $N/3$ or $2N/3$ (Proposition 4.7(c)). At $N = 60$, 72, 108 and 180 the smallest closed set containing H_{12} is F on every such triangle (Proposition 4.7(d)), so $S = F$. □

5. Smaller conductors

This section states the results that give condition (D) for $N > 400$ (Theorems 5.3 and 5.7) and those for the denominators 2^j, $2P$ and $3P$, explains the method, and proves Theorem 5.2 and one case in full: the steps at which a count of the units of Φ in the classes modulo the step gives a witness modulo the conductor (Proposition 5.5). The other cases are proved in the supplement (§§S1 and S7).

5.1. **Steps.**

Lemma 5.1. *Let $C \ni 1$ be closed, H its unit part and c its conductor, with $1 < c < N'$. Then $H \supset H_c$, c is the conductor of H_c, $\varphi(c) > 2$, and $c \not\equiv 2 \pmod 4$ if N is even. Let f, the step of c, be c if N is odd or c is even, and $2c$ if N is even and c is odd. Then $H_f = H_c$, $e = N/f \geq 2$, and $e = 2$ only if $4 \mid N$, with $c = N/2$ if $8 \mid N$ and $c = N/4$ if $N \equiv 4 \pmod 8$.*

Proof. As $K_c \subset H$ and $-1 \in H$, $H \supset H_c$. The conductor of H_c divides c, as $K_c \subset H_c$, and is divisible by c, as $H \supset H_c$. If $\varphi(c) \leq 2$, every unit is $\equiv \pm 1 \pmod c$, so $H_c = G = H$ and $c = 1$. If N is even and $c \equiv 2 \pmod 4$, a unit $\equiv 1 \pmod{c/2}$ is odd, hence $\equiv 1 \pmod c$, so $K_{c/2} = K_c \subset H$, against the choice of c. If $f = 2c$, a unit $\equiv \pm 1 \pmod c$ is odd, hence $\equiv \pm 1 \pmod{2c}$, so $H_f = H_c$. In both cases $f \mid N$ and $f < N$: if $f = 2c$ with c odd, then $2c \leq N/2$ when $4 \mid N$ and $2c < 2N' = N$ when $N \equiv 2 \pmod 4$. If $e = 2$, then N is even, and $f = N/2$; as $c < N'$, this needs $4 \mid N$, and then $c = N/2$, which is $\not\equiv 2 \pmod 4$ only if $8 \mid N$, or $2c = N/2$ with $c = N/4$ odd, that is $N \equiv 4 \pmod 8$. □

A statement proved for the closed sets $C \ni 1$ whose unit part H contains H_f, with the conclusion that $H = G$, or that the conductor of H properly divides that of H_f, or that $12 \mid f$ and $H \supset H_{12}$, gives (D) at c: a closed set whose unit part has conductor c has $H \supset H_c = H_f$ and $H \neq G$, so only the last alternative remains, and $12 \mid f$ forces $f = c$. For a divisor f of N with $e = N/f$ let Q be the set of primes of N that do not divide f, $w = |Q|$, $D_e = \sum_j \gcd(p_j, e)$, and

$$h_0(f) = \frac{e}{2} \prod_{\ell \in Q} \Big(1 - \frac{1}{\ell}\Big), \qquad \kappa(Q) = \prod_{\ell \in Q,\ \ell \geq 5} \frac{3(\ell - 1)}{2(\ell - 2)},$$

so that $h_0(f)$ is half the number of units modulo N in a class of units modulo f, and $\kappa(Q) = 1$ if $Q \subset \{2, 3\}$.

5.2. **The results.**

Let $c \mid N$. A *witness modulo c* is a pair (x, x'') of elements of Φ such that x is a unit, $x + x'' \equiv 2 \pmod c$, and $x + x'' - 1$ is a unit; it is *nontrivial* if $2x \not\equiv 2 \pmod c$. A witness x gives the witness $(x, 2 - x)$ modulo every c, nontrivial when $2x \not\equiv 2 \pmod c$. A nontrivial witness modulo c excludes the conductor c, as a witness excludes N' (Theorem 1.4).

Theorem 5.2. *Let $c \mid N$ with $c < N$, and suppose that Δ has a nontrivial witness modulo c. Then no closed set containing 1 has a unit part of conductor c. In particular, if Δ is scalene and $1 < c < N'$, Δ satisfies* (D) *at c.*

At $e = 2$, $f = N/2$ and $H_f = H_\nu = \{\pm 1, \pm(1+\nu)\}$, $\nu = N/2$, the group that is closed on Γ_1, Γ_2 and Γ_4 (Section 6).

Theorem 5.3. *Let $4 \mid N$, $N > 400$, N not a power of 2, and let Δ be scalene and not in* (1.1)*, other than Γ_1, Γ_2 with $8 \mid N$ and Γ_4 with $N \equiv 4 \pmod 8$, with no numerator $2N/3$ and no numerator $N/3$. Then no closed set containing 1 has a unit part of conductor $N/2$ if $8 \mid N$, or $N/4$ if $N \equiv 4 \pmod 8$. So Δ satisfies* (D) *at this conductor.*

Lemma 5.4. *If $e \geq 3$ divides N and divides no numerator of Δ, then $D_e \leq e$.*

Proof. The numbers $m_j = \gcd(p_j, e)$ are proper divisors of e. A common divisor of m_i and m_j divides p_i, p_j and N, hence the third numerator, so it is 1: the m_j are pairwise coprime and their product divides e. If all m_j are 1, the sum is $3 \leq e$. If exactly one exceeds 1, then $e \geq 4$, as 3 has no proper divisor above 1, and the sum is at most $e/2 + 2 \leq e$. If two or three exceed 1, the sum is at most $\prod_j m_j \leq e$, since $x + y \leq xy - 1$ for coprime $x, y \geq 2$ and $x + y + z \leq xyz$ for $x, y, z \geq 2$. □

Proposition 5.5. *Let $c \neq 12$ divide N, with $1 < c < N'$ and c the conductor of H_c, let f be its step and $e = N/f$, and suppose that $h_0(f) \geq \kappa(Q)\, 2^w D_e/2$. Then Δ has a nontrivial witness modulo c. This is so if every prime of N divides f and $e \geq 3$ divides no numerator.*

Theorem 5.6. *Let $N > 4{,}200$, and let Δ have $\gcd(p_1, p_2, p_3) = 1$, no numerator $2N/3$, and no numerator $N/3$ if $12 \mid N$. Then no closed set containing 1 has a unit part whose conductor c satisfies $c \neq 12$ and $1 < c < N'$ and has a step with $e \geq 3$.*

For $61 \leq N \leq 4{,}200$ we find, on every triangle as in the next theorem, a nontrivial witness modulo c at every $c \mid N$ with $c < N'$, $\varphi(c) > 2$ and $c \not\equiv 2 \pmod 4$, the conductor 12 and the conductors whose step has $e = 2$ included.

Theorem 5.7. *Let $N > 60$ be composite, and let Δ be scalene and not in* (1.1)*, other than Γ_1, Γ_2 and Γ_4, with no numerator $2N/3$, and with no numerator $N/3$ if $12 \mid N$. Then Δ satisfies* (D) *at every conductor c with $1 < c < N'$ whose step has $e \geq 3$.*

Proof. Let c be the conductor of the unit part H of a closed set $C \ni 1$, with $1 < c < N'$, and let f be its step and $e = N/f \geq 3$. By Lemma 5.1, $H \supset H_c$, c is the conductor of H_c, $\varphi(c) > 2$, and $c \not\equiv 2 \pmod 4$ if N is even. If $c = 12$, then $H \supset H_{12}$, which is the conclusion of (D). Let $c \neq 12$. If every prime of N divides f and e divides no numerator, Proposition 5.5 gives a nontrivial witness modulo c; otherwise, if $N \leq 4{,}200$, the computation above gives one. In both cases Theorem 5.2 shows that there is no such C. If $N > 4{,}200$, Theorem 5.6 shows it. □

Proposition 5.8. *Let $N = 2^j \geq 64$ and let Δ be scalene. If Δ has a witness, the closure of $\{1\}$ is F. If not, the closed sets containing 1 other than F are $\{\pm 1\}$ and, exactly on Γ_1 and Γ_2, also $H_\nu = \{\pm 1, \pm(1+\nu)\}$, $\nu = N/2$. In particular, if Δ is neither Γ_1 nor Γ_2, every closed $C \ni 1$ with $|C| \geq 4$ is F.*

Proposition 5.9. *Let $P \neq 13$ be an odd prime and $N = 2P$. For every scalene Δ and every subgroup $H \ni -1$ of G with $4 \leq |H| < P - 1$, no closed set has unit part H. Hence the unit part of a closed set containing 1 is $\{\pm 1\}$ or G.*

Proposition 5.10. *Let $P \geq 23$ be prime and $N = 3P$. For every scalene Δ, every closed $C \ni 1$ with $|C| \geq 4$ is F, except $C = H_P$ on $(3, P-3, 2P)/3P$, where this set is closed.*

5.3. **The method.** Witnesses modulo c are found by counting the units of Φ in a class modulo f. The count is $h_0(f)$ up to an error that the numerators control (Lemma 5.16); where the error is small against $h_0(f)$, every pair of unit classes a, b with $a+b\equiv 2$ carries units $x\equiv a$, $x''\equiv b$ of Φ with $x+x''-1$ a unit (Proposition 5.5). By Lemma 5.4 this is so whenever every prime of N divides f and e divides no numerator. For $N>4{,}200$ the other steps with $e\ge 3$ (Theorem 5.6) are treated at the divisors R of N with $f\mid R$, by a nontrivial witness (x,x'') modulo c with $x+x''\equiv 2 \pmod R$. If N/R divides no numerator, counts of the residues in a class modulo R that lie in Φ or are not generic give one, under conditions on the primes of N that do not divide R. If N/R divides a numerator p_j, the fractional part of xp_j/N depends only on the class of x modulo $n_j=N/\gcd(p_j,N)$, and a unit class x modulo R with $2x\not\equiv 2 \pmod c$ for which it and that of $(2-x)p_j/N$ lie in a window $(0,\lambda)$ gives one; a class modulo n_j with both below $3/5$ exists except in 66 small cases, all with $n_j\le 30$. A choice of R, by the primes of N that do not divide f and the numerators that N/f divides, covers every step but one family, $e=3$ with $3\parallel N$ and 3 dividing a numerator. There a numerator $N/3$, $N/6$ or $5N/6$ gives a nontrivial witness modulo c directly; otherwise the closed set contains every residue whose greatest common divisor with N is 3 and whose class modulo c lies in $\bar H$, and the translation is run with residues whose greatest common divisor with N divides 3.

At $e=2$ the classes modulo $f=N/2$ have only two lifts. Write $\Delta=(o_1,o_2,q)/N$ with $o_1<o_2$ odd and q even. A nontrivial witness modulo the conductor comes from one odd class x modulo ν such that x and $2-x$ each have a lift in Φ, x or $2-x$ is prime to the odd part of N, and $x\not\equiv 1 \pmod{\nu/2}$. If the residues $[xq]$ and $[(2-x)q]$ lie in $(0,\nu]$, both classes have a lift in Φ; these classes form the fibers of a window, which contain such an x on every triangle outside seven families named by the value of q. On six of them x is named explicitly, and on the seventh, $q=\nu+\gcd(q/2,\nu)$ with $q\ne 2N/3$, it is named in some cases and found by counting along an arithmetic progression in the others.

At $N=2^j$ every closed set containing 1 is one of the groups H_m, $m=4,8,\dots,N$, and counts of the units of Φ in the classes modulo m decide which are closed. At $N=2P$ every element of F is a unit and $G\cong(\mathbb{Z}/P)^\times$, and the arguments of Part I at a prime denominator [19, Propositions 5.2 and 5.3] apply to the image of the units of Φ in $(\mathbb{Z}/P)^\times$; at $N=3P$ we use the lattice of the triangle modulo P, as Part I does at a prime denominator, and Gauss periods. In both cases this settles $P\ge 2{,}000$; the smaller P are finitely many, and a search over the subgroups of G settles them (supplement, §S1).

5.4. **Proof of Theorem 5.2.** A nontrivial witness (x,x'') modulo c acts as a witness does in Theorem 1.4, at the modulus c. Let $C\ni 1$ be closed with unit part H of conductor c. Rule (iii) with $u=x$ puts x'' in xC and maps $h\in H$ to $(h+x-1)/x\in C$ when $h+x-1$ is generic (Lemma 5.11). Changing h within $hK_c\subset H$ makes $h+x-1$ prime to the primes of N that do not divide c (Lemma 5.13), and Lemma 2.6 makes it prime to c (Lemma 5.14); so the translation descends to the image $\bar H$ of H in $(\mathbb{Z}/c)^\times$ (Proposition 5.15), where Lemmas 3.6, 3.7 and 3.8 apply at the modulus c and give a group $K_{f'}\subset H$ with f' a proper divisor of c.

As in Section 3.2, $n_i=N/g_i$, so that $ap_i\equiv 0 \pmod N$ if and only if $n_i\mid a$, and a residue is generic if and only if no n_i divides it; as the g_i are pairwise coprime, $\operatorname{lcm}(n_i,n_j)=N$ for $i\ne j$.

Lemma 5.11. *Let $C\ni 1$ be closed, $H=C\cap G$, $c\mid N$ with $K_c\subset H$, (x,x'') a witness modulo c, $d=x-1$ and $k=x+x''-1$.*

(a) $x''\in xC$.

(b) *If $z \in C$ and $-(z+d)$ is holomorphic, then $(z+d)/x \in C$.*
(c) *If $z \in C$, $z+d$ is holomorphic and $z+k-1 \in C$, then $(z+d)/x \in C$.*

In particular, $(h+d)/x \in C$ for every $h \in H$ such that $h+d$ is generic and $h+k-1$ is a unit.

Proof. We apply rule (iii) with $u = x$ throughout; $x \in xC \cap \Phi$, as $1 \in C$. (a) Take $a = x$ and $a' = -k$, which lies in C by rule (i), as $k \in K_c \subset H$. Then $b = 1 - x + k = x''$ is holomorphic, so $x'' \in xC$. (b) Take $a = x$ and $a' = z$: $b = 1 - x - z = -(z+d)$ is holomorphic, so $-(z+d) \in xC$, and $(z+d)/x \in C$ by rule (i). (c) Take $a = x''$, which lies in $xC \cap \Phi$ by (a), and $a' = -(z+k-1) \in C$: $b = 1 - x'' + z + k - 1 = z + x - 1 = z + d$ is holomorphic, so $z + d \in xC$.

For the last statement, $h + k - 1 \equiv h \pmod{c}$, as $k \equiv 1 \pmod{c}$; being a unit, it lies in $hK_c \subset H \subset C$. As $h + d$ is generic, exactly one of $\pm(h+d)$ is holomorphic (Section 2.1); apply (b) or (c) with $z = h$. □

Lemma 5.12. *Let $C \ni 1$ be closed, $H = C \cap G$ and c the conductor of H. Then $K_c \subset H$, and H is the full preimage of its image $\bar{H}$ in $(\mathbb{Z}/c)^\times$. For every $a \in C$, $\delta = \gcd(a, N)$ divides N/c, $C \cap O_\delta = Ha$, and $K_{N/\delta} \subset H$.*

Proof. $K_c \subset H$ by the definition of the conductor, and K_c is the kernel of the reduction $G \to (\mathbb{Z}/c)^\times$. For $a \in C$, $\delta < N$ as $0 \notin F$; by Lemma 2.6, $C \cap O_\delta$ is the orbit Ha and $K_{N/\delta} \subset H$, and $c \mid N/\delta$ by Lemma 2.7. □

A prime q of N is *free* if $q \nmid c$, and *shared* if q divides both c and N/c.

Lemma 5.13. *In Lemma 5.11 let c be the conductor of H, and let $h \in H$. There is $h^* \in hK_c$ with $h^* \equiv 1 \pmod{q^{v_q(N)}}$ for every free prime q and $\gcd(h^* + d, q^{v_q(N)}) = \gcd(h + d, q^{v_q(c)})$ for every shared prime q. For such an h^*:*

(a) *$h^* + d$ and $h^* + k - 1$ are prime to every free prime, and $h^* + k - 1$ is a unit,*
(b) *$\gcd(h^* + d, N) = \gcd(h + d, c)$,*
(c) *$n_i \mid h^* + d$ if and only if $n_i \mid c$ and $n_i \mid h + d$.*

Proof. By the Chinese remainder theorem, K_c is the product over the primes q of N of the groups of units modulo $q^{v_q(N)}$ that are $\equiv 1 \pmod{q^{v_q(c)}}$. So $h^* \in hK_c$ may be chosen modulo each $q^{v_q(N)}$ independently, subject to $h^* \equiv h \pmod{q^{v_q(c)}}$ and to h^* being prime to q. At a free prime take $h^* \equiv 1$. At a shared prime q with $q^{v_q(c)} \nmid h + d$, every choice has $\gcd(h^* + d, q^{v_q(N)}) = \gcd(h + d, q^{v_q(c)})$. If $q^{v_q(c)} \mid h + d$, write $h + d \equiv q^{v_q(c)} s \pmod{q^{v_q(N)}}$ and take $h^* \equiv h + q^{v_q(c)} t$ with $t \equiv 1 - s \pmod{q}$; then $h^* \equiv h \pmod{q}$ is prime to q, and $h^* + d \equiv q^{v_q(c)}(s + t)$ with $s + t \equiv 1 \pmod{q}$. At the primes q with $q \nmid N/c$, $v_q(c) = v_q(N)$ and $h^* \equiv h \pmod{q^{v_q(N)}}$ is forced.

(a) Modulo a free prime, $h^* + d \equiv 1 + d = x$ and $h^* + k - 1 \equiv k$, both units. Modulo a prime of c, $h^* + k - 1 \equiv h^*$, as $k \equiv 1 \pmod{c}$. Every prime of N is free or divides c. (b) At a free prime both sides are prime to q, by (a); at a shared prime this is the choice of h^*; at the other primes q of N, $v_q(c) = v_q(N)$ and $h^* \equiv h \pmod{q^{v_q(N)}}$. (c) As $n_i \mid N$, $n_i \mid h^* + d$ if and only if $n_i \mid \gcd(h^* + d, N) = \gcd(h + d, c)$. □

Let $c < N$. As $\operatorname{lcm}(n_i, n_j) = N$ for $i \neq j$, at most one n_i divides c. Let $r = n_i$ if $n_i \mid c$, and $r = \infty$ if no n_i divides c, where ∞ divides no residue. By Lemma 5.13(c), $h^* + d$ is generic if and only if $r \nmid h + d$, a condition on h modulo c.

Lemma 5.14. *In Lemma 5.11 let c be the conductor of H, and let $h \in H$ be such that $h+d$ is generic and $h+k-1$ is a unit. Then $h+d$ is prime to c.*

Proof. Let $y = h+d$ and $\delta = \gcd(y, N)$. By Lemma 5.11, $y/x \in C \cap O_\delta$, so by Lemma 5.12, $\delta \mid N/c$, $K_{N/\delta} \subset H$ and $C \cap O_\delta = Hy/x$. Suppose that a prime ℓ divides δ and c. Then ℓ is shared. Let $\alpha = v_\ell(c) \geq 1$ and $j = v_\ell(\delta)$, so that $1 \leq j \leq v_\ell(N/c) < v_\ell(N)$; let $M = N/\ell^{v_\ell(N)}$ and $\delta_0 = \gcd(y, M)$, so that $\delta = \ell^j \delta_0$. Let Y be the set of residues y' modulo N with $y' \equiv y \pmod{M\ell^\alpha}$ and $v_\ell(y') = j$, which is well defined as $j < v_\ell(N)$.

For $y' \in Y$ put $h' = y' - d$. Then $h' \equiv h \pmod{M\ell^\alpha}$. Every prime of N divides $M\ell^\alpha$, so h' is a unit and $h'+k-1 \equiv h+k-1 \pmod{M\ell^\alpha}$ is a unit; and $c \mid M\ell^\alpha$, so $h'/h \in K_c \subset H$ and $h' \in H$. The residue $y' = h'+d$ is generic: if $n_i \mid y'$, then $v_\ell(n_i) \leq j$, so $\ell^{v_\ell(n_i)} \mid y$, and the prime-to-$\ell$ part of n_i divides M and y', hence y, as $y' \equiv y \pmod{M}$; so $n_i \mid y$, which is false. By Lemma 5.11, $y'/x \in C$, and $\gcd(y', N) = \ell^j \gcd(y, M) = \delta$. So $y'/x \in C \cap O_\delta = Hy/x$: there is $w \in H$ with $y' = wy$.

Write $y = \delta\eta$ and $y' = \delta\eta'$ with units η, η' modulo $N/\delta = (M/\delta_0)\,\ell^{v_\ell(N)-j}$; then $w \equiv \eta'/\eta \pmod{N/\delta}$. As $y' \equiv y \pmod{M}$, $\eta' \equiv \eta \pmod{M/\delta_0}$. Modulo $\ell^{v_\ell(N)-j}$: if $j < \alpha$, every $y' \equiv y \pmod{\ell^\alpha}$ has $v_\ell(y') = j$, and η' runs over the units $\equiv \eta \pmod{\ell^{\alpha-j}}$; if $j \geq \alpha$, η' runs over all units modulo $\ell^{v_\ell(N)-j}$. By the Chinese remainder theorem the quotients η'/η, $y' \in Y$, fill the group

$$W = \{w \in (\mathbb{Z}/(N/\delta))^\times : \ w \equiv 1 \pmod{b}\}, \qquad b = (M/\delta_0)\,\ell^{\max(\alpha-j,0)}.$$

So the image of H in $(\mathbb{Z}/(N/\delta))^\times$ contains W. As $K_{N/\delta} \subset H$, H contains the preimage of W in G, which is K_b. Hence $c \mid b$; but $v_\ell(c) = \alpha > \max(\alpha - j, 0) = v_\ell(b)$, as $j \geq 1$, a contradiction. □

Proposition 5.15. *In Lemma 5.11 let $c < N$ be the conductor of H, let $\bar{H}$ be the image of H in $(\mathbb{Z}/c)^\times$, and let $\bar{d}$ and $\bar{x}$ be the classes of d and x modulo c.*

(a) *For every $\bar{h} \in \bar{H}$ with $r \nmid \bar{h}+\bar{d}$, the residue $\bar{h}+\bar{d}$ is a unit modulo c and $(\bar{h}+\bar{d})/\bar{x} \in \bar{H}$.*

(b) *$1+\bar{d}$ and $1-\bar{d}$ are units modulo c, and $\bar{\rho} = (1-\bar{d})/(1+\bar{d})$ lies in $\bar{H}$.*

Proof. (a) Let $h \in H$ lie above $\bar{h}$, and let h^* be as in Lemma 5.13. As $r \nmid h+d$, h^*+d is generic, and h^*+k-1 is a unit by Lemma 5.13(a). By Lemma 5.14, h^*+d is prime to c; by Lemma 5.13(a) it is prime to the free primes; so it is a unit. By Lemma 5.11, $(h^*+d)/x \in C \cap G = H$, and its class modulo c is $(\bar{h}+\bar{d})/\bar{x}$, as $h^* \equiv h \pmod{c}$.

(b) $1+\bar{d} = \bar{x}$ is a unit. As $x'' \equiv 2-x \pmod{c}$, $-1+\bar{d} \equiv -x'' \pmod{c}$. If r divided $-1+\bar{d}$, then $r = n_i$ would divide c and x'', against x'' generic. So (a) applies to $\bar{h} = -1$: $1-\bar{d}$ is a unit, and $(-1+\bar{d})/\bar{x} = -\bar{\rho}$ lies in $\bar{H}$, as does -1. □

Proof of Theorem 5.2. Let $C \ni 1$ be closed with unit part H of conductor c, and let (x, x'') be a nontrivial witness modulo c, $d = x-1$ and $k = x+x''-1$, as in Lemma 5.11. Then $2\bar{d} \not\equiv 0$, so $c \geq 3$. By Proposition 5.15(b), $\bar{H}$ and $\bar{d}$ satisfy, at the modulus $n = c$, the hypotheses of Section 3.2 stated before Lemma 3.5: $\bar{H} \ni -1$ is a subgroup of $(\mathbb{Z}/c)^\times$, $1+\bar{d}$ and $1-\bar{d}$ are units, $2\bar{d} \not\equiv 0$ and $\bar{\rho} \in \bar{H}$; and $\bar{x} = 1+\bar{d}$. At the modulus c, K_f for $f \mid c$ denotes, as there, the group of units modulo c that are $\equiv 1 \pmod{f}$.

c even. Write $c = 2^\alpha m$ with $\alpha \geq 1$ and m odd, and let $r' = r$ if r is odd and $r' = \infty$ otherwise. An odd $r = n_i$ divides c, and $n_i > 1$ as $g_i \leq p_i < N$; so it is an odd divisor $r > 1$ of m. An even r divides no $\bar{h}+\bar{d}$, which is odd, as $\bar{h}$ is a unit and $\bar{d} = \bar{x}-1$ is even. So Proposition 5.15(a) gives (T) for $E = \{\bar{h} \in \bar{H} : \ r' \mid \bar{h}+\bar{d}\}$. By Lemma 3.6, and Lemma 3.7 if $E \neq \emptyset$, $\bar{H}$ contains some $K_f \neq \{1\}$ with $f \mid c$; so f is a proper divisor of c.

c odd. Let $r' = r$ if $r \neq \infty$, an odd divisor $r > 1$ of c, and $r' = c$ if $r = \infty$. As $r' \nmid \bar{h} + \bar{d}$ implies $r \nmid \bar{h} + \bar{d}$, Proposition 5.15(a) gives (T) for $E = \{\bar{h} \in \bar{H} : \ r' \mid \bar{h} + \bar{d}\}$. By Lemma 3.8 at $n = c$, $\bar{H}$ contains K_f for a proper divisor f of c.

In both cases the preimage of K_f in G is the group K_f of units modulo N that are $\equiv 1 \pmod f$, and it lies in H, the full preimage of $\bar{H}$ (Lemma 5.12). So the conductor c of H divides the proper divisor f of c, a contradiction. Hence no closed set containing 1 has a unit part of conductor c. If Δ is scalene and $1 < c < N'$, (D) at c concerns these closed sets only, so it holds. □

5.5. **Proof of Proposition 5.5.** Let $f \mid N$, $e = N/f$, Q, w as above, and $q_Q = \prod_{\ell \in Q} \ell$. With $((t))$ and μ as in Lemma 2.12, $((t)) = -\frac{1}{2}$ at integers and $|((t))| < \frac{1}{2}$ otherwise. For a unit class ξ modulo f let $h(\xi)$ be the number of units x modulo N in Φ with $x \equiv \xi \pmod f$; when the modulus $f' \mid N$ has to be named we write $h_{f'}$.

Lemma 5.16. *For $j = 1, 2, 3$ let $m_j = \gcd(p_j, e)$, $p_j' = p_j/m_j$, let Q_j^+ be the set of $\ell \in Q$ with $\ell \nmid e/m_j$, $Q_j^- = Q \setminus Q_j^+$, and $q_j^- = \prod_{\ell \in Q_j^-} \ell$. For $\delta \mid q_Q$ let $\bar{\delta}$ be an inverse of δ modulo f. Then for every unit class ξ modulo f*

$$h(\xi) = h_0(f) - \sum_{j=1}^{3} T_j(\xi), \qquad T_j(\xi) = m_j \prod_{\ell \in Q_j^+} \Big(1 - \frac{1}{\ell}\Big) \sum_{\delta \mid q_j^-} \mu(\delta) \Big(\Big(\frac{\xi \bar{\delta} p_j'}{f}\Big)\Big).$$

Proof. For a unit x the residues $[xp_j]$ are non-zero and their sum is N or $2N$, the first exactly when $x \in \Phi$; so the indicator of Φ at x is $2 - \sum_j \{xp_j/N\} = \frac{1}{2} - \sum_j ((xp_j/N))$. The units $x \equiv \xi \pmod f$ are $2h_0(f)$ in number, so the constant $\frac{1}{2}$ contributes $h_0(f)$. By Lemma 2.12(b) with $n = N$, $q = f$, $\gamma = \xi$ and $a = p_j$, the d with $\mu(d) \neq 0$ there being the divisors δ of q_Q, and with $m_{j,\delta} = \gcd(p_j, e/\delta)$ and $x_\delta \equiv \xi \bar{\delta} \pmod f$,

$$\sum_{x \in G,\ x \equiv \xi \ (f)} \Big(\Big(\frac{xp_j}{N}\Big)\Big) = \sum_{\delta \mid q_Q} \mu(\delta)\, m_{j,\delta} \Big(\Big(\frac{x_\delta p_j}{m_{j,\delta} f}\Big)\Big).$$

Write $\delta = \delta^+ \delta^-$ with $\delta^\pm \mid q_j^\pm$, where $q_j^+ = \prod_{\ell \in Q_j^+} \ell$. A prime $\ell \in Q$ divides e to the power $v_\ell(N) \geq 1$. For $\ell \in Q_j^-$, $v_\ell(p_j) < v_\ell(e)$, so dividing e by ℓ does not change $\gcd(p_j, e)$; for $\ell \in Q_j^+$, $v_\ell(p_j) \geq v_\ell(e)$, and dividing e by ℓ divides the greatest common divisor by ℓ. So $m_{j,\delta} = m_j/\delta^+$ and $x_\delta p_j/(m_{j,\delta} f) = x_\delta \delta^+ p_j'/f$, which modulo 1 equals $\xi \overline{\delta^-} p_j'/f$, as $x_\delta \delta^+ \equiv \xi \overline{\delta^-} \pmod f$. Summing $\mu(\delta^+) m_j/\delta^+$ over $\delta^+ \mid q_j^+$ gives $m_j \prod_{\ell \in Q_j^+} (1 - 1/\ell)$, and the lemma follows. □

Corollary 5.17. *Let $f \geq 2$ and $B(f) = \frac{1}{2} \sum_j m_j \prod_{\ell \in Q_j^+} (1 - 1/\ell)\, 2^{|Q_j^-|}$. Then $|h(\xi) - h_0(f)| < B(f) \leq 2^w D_e/2$ for every unit class ξ modulo f.*

Proof. The sum over $\delta \mid q_j^-$ in T_j has $2^{|Q_j^-|}$ terms $\mu(\delta)((\cdot))$, each of absolute value at most $\frac{1}{2}$, and of absolute value $\frac{1}{2}$ only when it equals $-\mu(\delta)/2$. So its absolute value is at most $2^{|Q_j^-|}/2$, with equality only if every term is $-\mu(\delta)/2$ and all have one sign. If $Q_j^- \neq \emptyset$, $\mu(\delta)$ takes both signs, and the inequality is strict. If $Q_j^- = \emptyset$, the only term is $((\xi p_j'/f))$, and equality needs $f \mid \xi p_j'$, so $f \mid p_j$; this does not hold for all three j, as $f \geq 2$ and $\gcd(p_1, p_2, p_3) = 1$. So $\sum_j |T_j(\xi)| < B(f)$. Finally $\prod_{\ell \in Q_j^+} (1 - 1/\ell)\, 2^{|Q_j^-|} \leq 2^w$ and $\sum_j m_j = D_e$. □

For $\delta \mid q_Q$, $f\delta$ divides N and $h_0(f\delta) = h_0(f)/\prod_{\ell\mid\delta}(\ell-1)$. Let $Q_5 = \{\ell \in Q : \ \ell \ge 5\}$ and $q_5 = \prod_{\ell\in Q_5}\ell$.

Lemma 5.18. *Let $f \ge 3$ and $h_0(f) \ge \kappa(Q)\,2^w D_e/2$. For all units a, b modulo f with $a+b \equiv 2 \pmod f$ there are units $x \equiv a$ and $y \equiv b \pmod f$ in Φ such that $x+y-1$ is a unit.*

Proof. For $\delta \mid q_Q$, Corollary 5.17 at $f\delta$, whose set of primes Q has $w-\omega(\delta)$ elements, gives $B(f\delta) \le 2^{w-\omega(\delta)}D_e/2$, since $\gcd(p_j, e/\delta) \le \gcd(p_j, e)$. If $3 \in Q$, the units $x \equiv a \pmod f$ with $x \equiv 1 \pmod 3$ form one unit class modulo $3f$, and the number of those in Φ exceeds $h_0(3f) - B(3f) \ge h_0(f)/2 - 2^{w-1}D_e/2 \ge 0$, as $\kappa(Q) \ge 1$; choose such an x. If $3 \notin Q$, choose any unit $x \equiv a \pmod f$ in Φ; one exists, as $h(a) > h_0(f) - B(f) \ge 0$. Let R be the set of $\ell \in Q_5$ with $x \not\equiv 1 \pmod\ell$ and $r = \prod_{\ell\in R}\ell$. By inclusion and exclusion over $\delta \mid r$, the number of units $y \equiv b \pmod f$ in Φ with $y \not\equiv 1-x \pmod\ell$ for every $\ell \in R$ is $\sum_{\delta\mid r}\mu(\delta)h_{f\delta}(c_\delta)$, where c_δ is the class modulo $f\delta$ that is $\equiv b \pmod f$ and $\equiv 1-x \pmod\ell$ for $\ell \mid \delta$; it is a unit class, as $1-x \not\equiv 0 \pmod\ell$ for $\ell \in R$. By Corollary 5.17 this number exceeds

$$h_0(f)\prod_{\ell\in R}\frac{\ell-2}{\ell-1} - \sum_{\delta\mid r}B(f\delta) \ \ge \ h_0(f)\prod_{\ell\in Q_5}\frac{\ell-2}{\ell-1} - \frac{2^w D_e}{2}\sum_{\delta\mid q_5}2^{-\omega(\delta)}$$
$$= \prod_{\ell\in Q_5}\frac{\ell-2}{\ell-1}\Big(h_0(f) - \kappa(Q)\frac{2^w D_e}{2}\Big) \ge 0,$$

using $\sum_{\delta\mid q_5}2^{-\omega(\delta)} = (3/2)^{|Q_5|}$. Choose such a y. Then $x+y-1 \equiv 1 \pmod f$ is prime to every prime of f. If $2 \in Q$, x and y are odd and $x+y-1$ is odd; if $3 \in Q$, $x+y-1 \equiv y \not\equiv 0 \pmod 3$; for $\ell \in Q_5$, $x+y-1 \equiv y \not\equiv 0$ if $x \equiv 1 \pmod\ell$, and $x+y-1 \not\equiv 0$ by the choice of y if $\ell \in R$. So $x+y-1$ is a unit. □

Proof of Proposition 5.5. As c is the conductor of H_c and $c > 1$, $H_c \ne G$, so some unit is $\not\equiv \pm 1 \pmod c$ and $\varphi(c) > 2$; in particular $c \ge 3$, and $f \ge 3$ divides N. By Lemma 5.18, for all units a, b modulo f with $a+b \equiv 2 \pmod f$ there are units $x \equiv a$ and $x'' \equiv b \pmod f$ in Φ with $x+x''-1$ a unit. As $c \mid f$, (x, x'') is a witness modulo c, nontrivial if $2a \not\equiv 2 \pmod c$. So it suffices to find a unit a modulo f with $2-a$ a unit and $2a \not\equiv 2 \pmod c$. We choose a modulo each prime power $\ell^v \parallel f$; at $\ell = 2$ every odd a has $2-a$ odd. If a prime $\ell \ge 5$ divides c, take $a \equiv 3$ modulo its power in f and $a \equiv 1$ modulo the other prime powers of f: then $2-a \equiv -1$ or 1, and $2a-2 \equiv 4 \not\equiv 0 \pmod\ell$. Otherwise $c = 2^i 3^j$. If $9 \mid c$, take $a \equiv 4 \pmod{3^j}$ and $a \equiv 1$ modulo the power of 2 in f: then $2-a \equiv -2 \pmod{3^j}$, and $2a-2 \equiv 6 \not\equiv 0 \pmod 9$. If $8 \mid c$, then $f = c$; take $a \equiv 3 \pmod{2^i}$ and $a \equiv 1 \pmod{3^j}$: then $2-a \equiv -1 \pmod{2^i}$, and $2a-2 \equiv 4 \not\equiv 0 \pmod 8$. Otherwise $c \mid 12$, and $\varphi(c) > 2$ gives $c = 12$, which is excluded. In the last case of the statement, $w = 0$, $\kappa(Q) = 1$ and $h_0(f) = e/2$, and $D_e \le e$ by Lemma 5.4. □

6. Families without a witness and an angle $2\pi/3$

This section proves $S = F$ on the triangles with an angle $2\pi/3$, through relative periods, and on the three families Γ_1, Γ_2, Γ_4, through cylinders, and states for the other families of Proposition 4.1 the results that give (N′) or $S = F$ on them. Five of these have short proofs, which we give; the others repeat methods shown here in full and are proved in the supplement (§§S2–S4). For even N we write $\nu = N/2$, and for $4 \mid N$ we put $u_\iota = 1+\nu$. Then u_ι is a unit, $u_\iota^2 \equiv 1$, $u_\iota x \equiv x+\nu$ for odd x and $u_\iota x \equiv x$ for even x, and $K_\nu = \{1, u_\iota\}$.

6.1. **An angle $2\pi/3$.** Let $K > 16$, $1 \le p < K$ with $\gcd(p, K) = 1$, $N = 3K$ and $\Delta = (p, K-p, 2K)/N$. At the vertex of numerator $2K$, of angle $2\pi/3$, $g = K$; its K points have cone angle 4π, so they are zeros of ω, and the $c \in R$ with this vertex are the non-zero multiples of 3. For $a \in \Phi \cup -\Phi$, $3 \nmid a$, and $[2Ka]$ is $2K$ if $a \equiv 1$ and K if $a \equiv 2 \pmod 3$. So at this vertex rules (iv) and (v) take the following form, for a closed set $C \ni 1$ in place of S and a set $\mathcal{D}$ of non-zero multiples of 3 in $\mathbb{Z}/N$ in place of $\mathcal{C}$:

(iv′) if u is a unit, $x \in uC \cap \Phi$, $a \in C$, and $c = a + x - 1$ is a non-zero multiple of 3, then $u^{-1}c \in \mathcal{D}$;

(v′) if u is a unit, $c \in \mathcal{D}$, $x \in uC \cap \Phi$ with $x \equiv 2 \pmod 3$, and $b = 1 - x - c \in \Phi$, then $b \in uC$.

Theorem 6.1. *Let $K > 16$ and $\Delta = (p, K-p, 2K)/3K$ with $\gcd(p, K) = 1$. Let $C \ni 1$ be closed with $C \ne \{\pm 1\}$ and $\mathcal{D}$ a set of non-zero multiples of 3 in $\mathbb{Z}/N$ such that (iv′) and (v′) hold. Then $C = F$.*

The proof is in the supplement (§S2). It starts from the following elements of $\mathcal{D}$.

Lemma 6.2. *In Theorem 6.1, $1 - 2x^{-1} \in \mathcal{D}$ for every unit $x \in \Phi$ with $x \equiv 2 \pmod 3$ and $x \ne 2$.*

Proof. By rule (i), $-1 \in C$, and $x \in xC \cap \Phi$ as $1 \in C$. So (iv′) with $u = x$, $a = -1$ and $c = x - 2$, a non-zero multiple of 3, gives $x^{-1}(x-2) = 1 - 2x^{-1} \in \mathcal{D}$. □

The rest of the proof runs as follows. Label the vertices so that $3 \nmid p$ (if $3 \mid p$, then $3 \nmid K - p$). The holomorphic units $x \equiv 2 \pmod 3$ are those with $[px]$ in one class modulo 3, or modulo 6 for even N, in the window $(0, 2K)$, and on the diagonal $1 - c = 2x^{-1}$ of $c = 1 - 2x^{-1}$ rule (v′) pairs the elements of C in this window with further characters. Let $j(n)$ be Jacobsthal's function, the least j such that any j consecutive integers contain one prime to n; then any $j(n)$ consecutive terms of a progression whose difference is prime to n contain one prime to n. When a prime $\ell \ge 5$ of K satisfies $\lfloor \lceil (K-2)/2 \rceil / (\delta\ell) \rfloor \ge j(N_\ell)$, where δ is 3 for odd N and 6 for even N and N_ℓ is the product of the primes $\ell' \ge 5$ of N other than ℓ, this puts a non-unit s with $\ell \mid \gcd(s, N)$ into C. We use Jacobsthal's function as Puchta [29] and Larsen, Norton and Zykoski [26, Proposition 7.5] do. Then $K_{N/\ell^i} \subset H$ for some $i \ge 1$, by Lemma 2.6; rules (iv′) and (v′) then give $H = G$, in one more step when $8 \mid N$; and $C = F$ by Theorem 1.5. When no prime $\ell \ge 5$ of K satisfies the inequality, $K = 2^\alpha 3^\beta$, or $K = eP$ with $P \ge 5$ prime and $e \in \{1, 2, 3, 4, 6, 8, 12\}$, or K is one of 25, 35, 50, 55, 70, 77, 110, 154. In these cases counts of the holomorphic units of the window on one such diagonal give a non-unit in C or more than two units in H, except for finitely many values of K; for these we find, for every subgroup $H_0 \ni -1$ of G with $H_0/\{\pm 1\}$ of prime order, that the smallest pair $(C, \mathcal{D})$ with $H_0 \subset C$ satisfying the rules has $C = F$; as $C \ne \{\pm 1\}$, the unit part of C contains such a subgroup (Lemma 2.7).

Theorem 6.3. *Let $N > 48$ and let Δ be a scalene triangle with an angle $2\pi/3$. Then $S = F$ and $\mathcal{M} = \mathcal{L}$.*

Proof. Here $\Delta = (p, K-p, 2K)/N$ with $K = N/3 > 16$, and a common divisor of p and K divides the three numerators, so $\gcd(p, K) = 1$; and $\Delta \ne (1, 2, 3)/6$. Let $\mathcal{D}$ be the set of non-zero multiples of 3 in $\mathcal{C}$. The set S is closed and contains 1 (Section 2.1). If u is a unit, $x \in uS \cap \Phi$, $a \in S$ and $c = a + x - 1$ is a non-zero multiple of 3, then $c \in R$, and rule (iv) puts $u^{-1}c$, a non-zero multiple of 3, in $\mathcal{C}$, hence in $\mathcal{D}$. If $c \in \mathcal{D}$, its vertex is the one of numerator $2K$, and a character $x \equiv 2 \pmod 3$ in $uS \cap \Phi$ has $[2Kx] = K < 2K$; so rule (v) gives (v′).

By [19, Theorem 1.1], a scalene triangle of rank one with $N > 15$ is $(1, k, k+1)/(2k+2)$, $(2, 2k+1, 2k+3)/(4k+6)$ or $(1, 2, 2k-3)/2k$, whose largest numerators are $N/2$, $N/2$ and $N-3$. A numerator $2N/3$ would be the largest, and none of these is $2N/3$, as $N \neq 9$. So Δ has rank at least two, $|S| \geq 4$ by (1.2), and $S \neq \{\pm 1\}$. Theorem 6.1 gives $S = F$, and Corollary 2.4 gives $\mathcal{M} = \mathcal{L}$. □

6.2. **The three families Γ_1, Γ_2, Γ_4.** In this subsection $4 \mid N$. Let $\Gamma_1 = (1, \nu-2, \nu+1)/N$, $\Gamma_2 = (2, N/4-1, 3N/4-1)/N$ with $8 \mid N$, and $\Gamma_4 = (4, N/4-2, 3N/4-2)/N$ with $N \equiv 4 \pmod 8$. We begin with the holomorphic characters, which are known exactly on these triangles and on the triangle $(1, 2, N-3)/N$ of (1.1), and with the reason why the rules do not suffice on them.

Lemma 6.4. *Let Δ and Δ' be triangles with $p_i' \equiv u_\iota p_i \pmod N$ for $i = 1, 2, 3$. Then $\Phi(\Delta') = u_\iota \Phi(\Delta)$, and a subgroup $H \ni -1$ of G satisfies* (P) *on Δ if and only if it satisfies* (P) *on Δ'.*

Proof. For every x, $xp_i' \equiv (u_\iota x)p_i$, so $x \in \Phi(\Delta')$ if and only if $u_\iota x \in \Phi(\Delta)$; and $u_\iota^{-1} = u_\iota$. The diagonals $1 - a'$, $a' \in H$, are even, and $u_\iota c \equiv c$ for even c; so $(x, b) \mapsto (u_\iota x, u_\iota b)$ maps the pairs of Δ' on the diagonal $1 - a'$ bijectively onto those of Δ on the same diagonal, and keeps units, non-units and the quotient b/x. □

So $\Theta_0 = (2, \nu-3, \nu+1)/N$, whose numerators are u_ι times those of $(1, 2, N-3)/N$, and $(1, 2, N-3)/N$ have the same subgroups with (P). For an odd x let $[x]$ be its residue in $[0, N)$.

Lemma 6.5. *Let x be odd.*

(a) *On Γ_1, and on Γ_2 when $8 \mid N$, $x \in \Phi$ if and only if $[x] \in (0, N/4) \cup (\nu, 3N/4)$.*

(b) *On Γ_4, when $N \equiv 4 \pmod 8$, $x \in \Phi$ if and only if $0 < [4x] < \nu$.*

(c) *On $(1, 2, N-3)/N$, when $3 \nmid N$, $x \in \Phi$ if and only if $[x] \in (0, N/3) \cup (\nu, 2N/3)$.*

In (a) and (b) the set of odd elements of Φ is stable under multiplication by u_ι.

Proof. We use Lemma 2.17(a) in the form: $x \in \Phi$ if and only if the residues of xp_1, xp_2, xp_3 are non-zero and add up to N; otherwise they add up to $2N$ or one of them is 0.

(a) As x is odd, $x\nu \equiv \nu$. On Γ_1, for $[x]$ in $(0, N/4)$, $(N/4, \nu)$, $(\nu, 3N/4)$, $(3N/4, N)$ the residues of x, $x(\nu-2) \equiv \nu - 2x$ and $x(\nu+1) \equiv \nu + x$ are $(x, \nu-2x, \nu+x)$, $(x, 3\nu-2x, \nu+x)$, $(x, 3\nu-2x, x-\nu)$, $(x, 5\nu-2x, x-\nu)$, with sums N, $2N$, N, $2N$. On Γ_2, $xN/4 \equiv N/4$ or $3N/4$ as $x \equiv 1$ or $3 \pmod 4$, so the residues of $x(N/4-1)$ and $x(3N/4-1)$ are, in some order, those of $N/4-x$ and $3N/4-x$; with $2x$, on the same four intervals they are $(2x, N/4-x, 3N/4-x)$, $(2x, 5N/4-x, 3N/4-x)$, $(2x-N, 5N/4-x, 3N/4-x)$, $(2x-N, 5N/4-x, 7N/4-x)$, with sums N, $2N$, N, $2N$. The ends of the intervals are multiples of $N/4$, at which a residue vanishes when x is odd.

(b) Here $N/4$ is odd, and as in (a) the residues of $x(N/4-2)$ and $x(3N/4-2)$ are those of $N/4-2x$ and $3N/4-2x$. Let $y = [2x]$, which is even, so $y \neq N/4, 3N/4$. For y in $(0, N/4)$, $(N/4, \nu)$, $(\nu, 3N/4)$, $(3N/4, N)$ the residues of $4x$, $N/4-y$ and $3N/4-y$ are $(2y, N/4-y, 3N/4-y)$, $(2y, 5N/4-y, 3N/4-y)$, $(2y-N, 5N/4-y, 3N/4-y)$, $(2y-N, 5N/4-y, 7N/4-y)$, with sums N, $2N$, N, $2N$; and $[4x] = [2y]$ lies in $(0, \nu)$ exactly in the first and the third case. If $y \in \{0, \nu\}$, then $4x \equiv 0$ and $[4x] = 0$.

(c) For $[x]$ in $(0, N/3)$, $(N/3, \nu)$, $(\nu, 2N/3)$, $(2N/3, N)$ the residues of x, $2x$, $-3x$ are $(x, 2x, N-3x)$, $(x, 2x, 2N-3x)$, $(x, 2x-N, 2N-3x)$, $(x, 2x-N, 3N-3x)$, with sums N, $2N$, N, $2N$; none is 0, as x is odd and $3 \nmid N$.

Finally $u_\iota x \equiv x + \nu$ preserves the conditions in (a) and (b), as $[x]$ modulo ν and $[4x]$ do not change. □

Proposition 6.6. *Let Δ be Γ_1 with $N \geq 8$, Γ_2 with $8 \mid N$, or Γ_4 with $N \equiv 4 \pmod 8$ and $N \geq 12$. Then Δ has no witness, and $C = \{\pm 1, \pm u_\iota\}$ is closed. Its conductor divides ν, and $C \neq F$ when $\varphi(N) > 4$.*

Proof. No witness. On Γ_1 and Γ_2 let $x \in \Phi$ be a unit with $x \notin \{1, u_\iota\}$, and r its residue modulo ν. By Lemma 6.5(a), r is odd with $3 \leq r < N/4$, and the residue of $2 - x$ modulo ν is $\nu + 2 - r > N/4$, so $2 - x \notin \Phi$. On Γ_4 let $x \in \Phi$ be a unit and $r = [4x]$, so $0 < r < \nu$ and $4 \mid r$. If $r = 4$, then $x \equiv 1 \pmod{N/4}$, and as $N/4$ is odd the odd such x are 1 and u_ι. If $r = 8$, then $4(2 - x) \equiv 0$ and $2 - x \notin \Phi$. If $r \geq 12$, then $[4(2 - x)] = N + 8 - r > \nu$, and $2 - x \notin \Phi$. In each case $2x \equiv 2$ or $2 - x \notin \Phi$.

C is closed. As $u_\iota \neq \pm 1$, C is a subgroup of G of order 4; by Lemma 3.3 we check (P) on the diagonals $1 - a'$, $a' \in C$, and only pairs of odd characters need checking, since the diagonal is even and every unit is odd. The diagonal 0 carries no pair, as at most one of $\pm x$ lies in Φ. On the diagonal $1 - u_\iota = -\nu$, a pair (x, b) with a unit member, say x, has $b \equiv -x - \nu = -u_\iota x$, which is not in Φ by the stability in Lemma 6.5; so this diagonal carries no pair with a unit member. On the diagonal $1 + u_\iota = 2 + \nu$, the pairs of odd characters are the $(x, u_\iota(2 - x))$, as $2 - x$ is odd; by the stability, they are the images of the pairs $(x, 2 - x)$ of the diagonal 2, with the same units and with quotients multiplied by $u_\iota \in C$. On the diagonal 2, a pair with a unit member x has $2x \equiv 2$, as there is no witness; so $x = 2 - x \in \{1, u_\iota\}$, and (P) holds.

Finally $K_\nu = \{1, u_\iota\} \subset C$, so the conductor of C divides ν; and $G \subset F$ has $\varphi(N)$ elements. □

As $N' = N$ when $4 \mid N$, the conductor of C lies strictly between 1 and N' when $\varphi(N) > 4$, and C does not contain H_{12} once $\varphi(N) > 8$: on these triangles (D) fails. We use cylinders instead.

Free sets of cylinders. Let $\lambda \in \mathbb{C}^\times$ be such that $(X, \lambda\omega)$ is horizontally periodic, with maximal horizontal cylinders $C_1, \dots, C_r$ of heights h_i, circumferences c_i and moduli $m_i = h_i/c_i$, and let $\Xi_i = I_{C_i}$ be Wright's class of C_i (Section 2.6). A non-empty set $\mathcal{G}$ of these cylinders is *free* if the $\mathbb{Q}$-span of the moduli of the cylinders in $\mathcal{G}$ meets the $\mathbb{Q}$-span of the moduli of the other cylinders only in 0.

Lemma 6.7. *Let Δ be scalene, $\Delta \neq (1, 2, 3)/6$, let $\mathcal{G}$ be a free set of maximal horizontal cylinders of $(X, \lambda\omega)$, and $\xi = \sum_{C_i \in \mathcal{G}} h_i \Xi_i$. Then $(T^k)^* \xi \in V$ for every $k \in \mathbb{Z}/N$. If a segment σ joining two points of Σ meets C_i in finitely many open segments, each joining the two boundary components of C_i, then $\Xi_i(\sigma)$ is the number of these segments that run from the bottom of C_i to its top minus the number that run from its top to its bottom.*

Proof. Let $t_i = m_i$ for $C_i \in \mathcal{G}$ and $t_i = 0$ otherwise. If $\sum_i q_i m_i = 0$ with $q_i \in \mathbb{Q}$, then $\sum_{C_i \in \mathcal{G}} q_i m_i = -\sum_{C_i \notin \mathcal{G}} q_i m_i$ lies in both $\mathbb{Q}$-spans, so it is 0, and $\sum_i q_i t_i = 0$. So t satisfies every rational linear relation among the moduli, and Wright's Lemma 3.1 with his Corollary 3.4 [35], in the form [19, Lemma 2.8] with $\Sigma' = \Sigma$, give $\sum_i t_i c_i \Xi_i = \xi \in V$. As $T^* V = V$ [19, Lemma 2.4], $(T^k)^* \xi \in V$.

For the second statement let $y \in (0, h_i)$ be the height in C_i above its bottom, $\rho \colon (0, h_i) \to [0, 1]$ smooth, 0 near 0 and 1 near h_i, and β the closed form $d(\rho \circ y)$ on C_i, extended by 0. Its integral is 0 on relative cycles disjoint from C_i and on a core curve of C_i, and 1 on a path in the closure of C_i from a zero on its bottom to a zero on its top. Relative cycles of these

kinds span $H_1(X,\Sigma;\mathbb{Z})$ [35, p. 420], and Ξ_i takes the same values on them; so β represents Ξ_i. On each open segment of $\sigma\cap C_i$ the integral of β is 1 from the bottom to the top and -1 from the top to the bottom, and β vanishes on the rest of σ. □

The star. Let $\Delta=(1,q,r)/N$ be scalene with $r>N/2$, with vertices A, B, C of angles θ, $q\theta$, $r\theta$, $\theta=\pi/N$, scaled so that $|BC|=1$. For $j\in\mathbb{Z}/2N$ let

$$v_j=\rho_j\,(\sin j\theta,\cos j\theta),\qquad \rho_j=|AC|=\frac{\sin q\theta}{\sin\theta}\ (j\text{ even}),\qquad \rho_j=|AB|=\frac{\sin r\theta}{\sin\theta}\ (j\text{ odd}),$$

and let e_j be the side with ends v_{j-1} and v_j. The polygon $\mathcal{P}$ with vertices $v_0,v_{-1},v_{-2},\dots$ in counterclockwise order is the star of [16, §5.3], placed as in the proof of [16, Theorem 5.15] (there $\phi=\pi/2-j_0\theta$, $B_k=v_{j_0-2k}$ and $C_k=v_{j_0-2k-1}$ for a fixed odd j_0). It is the union of the $2N$ copies $Ov_{j-1}v_j$ of Δ with the vertex A at the origin O; the v_j with j even are copies of C, the others copies of B.

Lemma 6.8. (a) *The unfolding is $\mathcal{P}$ with, for even i, the side e_i glued by a translation to e_{i-2q-1}, v_i to v_{i-2q-2} and v_{i-1} to v_{i-2q-1}; O is a regular point, and ω is a non-zero multiple of dz.*

(b) *The rotation about O through 2θ maps v_j to v_{j-2} and e_j to e_{j-2}, and induces T.*

(c) *Suppose that every vertex of $\mathcal{P}$ lies in Σ, and let* a *be a side e_j with an orientation. Then $H_1(X,\Sigma;\mathbb{Z})$ is free with basis T^ka, $k\in\mathbb{Z}/N$; for $\ell\in\mathbb{Z}/N$, $H^1(X,\Sigma)_\ell$ is spanned by the class φ_ℓ with $\varphi_\ell(T^k\mathrm{a})=\zeta^{\ell k}$; and for $\xi\in H^1(X,\Sigma;\mathbb{C})$ the classes $(T^k)^*\xi$ span $\bigoplus_{\ell:\hat\xi(\ell)\neq0}H^1(X,\Sigma)_\ell$, where $\hat\xi(\ell)=\frac1N\sum_k\zeta^{-\ell k}\xi(T^k\mathrm{a})$.*

Proof. (a) This is [16, Lemma 5.12] in our labels: there $b_k=e_{j_0-2k}$ is glued to $c_{k-q-1}=e_{j_0-2k+2q+1}$, with $B_k\mapsto B_{k-q}$ and $C_k\mapsto C_{k-q-1}$; put $i=j_0-2k+2q+1$. The unfolding is (X,ω) up to a non-zero factor (Section 2.6).

(b) The rotation R adds 2θ to arguments and $\rho_{j-2}=\rho_j$, so $R(v_j)=v_{j-2}$. The rule of (a) is invariant under $j\mapsto j-2$, so R induces an automorphism of X with $R^*\omega=\zeta\omega$, which is a power of T [19, Theorem 6.2], hence T.

(c) The points of Σ, the N classes of glued pairs of sides, each containing one side of odd index, and the interior of $\mathcal{P}$ form a cell structure on X. Each 1-cell occurs twice in the boundary of the 2-cell, with opposite orientations, as the gluings are translations; so $H_1(X,\Sigma;\mathbb{Z})$ is free on the 1-cells, which by (b) are the T^ka up to orientation. So $(T^*\xi)(T^k\mathrm{a})=\xi(T^{k+1}\mathrm{a})$, $T^*\varphi_\ell=\zeta^\ell\varphi_\ell$, $\xi=\sum_\ell\hat\xi(\ell)\varphi_\ell$, and $\frac1N\sum_k\zeta^{-\ell k}(T^k)^*\xi=\hat\xi(\ell)\varphi_\ell$. □

The triangle Γ_1. Let $\nu\geq8$ be even, $N=2\nu$, $\Delta=\Gamma_1=(1,\nu-2,\nu+1)/N$, $\theta=\pi/N$ and $\kappa=2\cos2\theta$, and let $\mathcal{P}$, v_j, e_j, $j\in\mathbb{Z}/4\nu$, be as above with $q=\nu-2$, $r=\nu+1$. So $\rho_j=\cos2\theta/\sin\theta$ for even j and $\rho_j=\cot\theta$ for odd j, and Lemma 6.8(a) reads: *for even i, e_i is glued to $e_{i+2\nu+3}$, with $v_i\leftrightarrow v_{i+2\nu+2}$ and $v_{i-1}\leftrightarrow v_{i+2\nu+3}$*, the rule of the proof of [16, Theorem 5.15]. The copies of C form one point of cone angle $2\pi(\nu+1)$, and the copies of B form $g_B=\gcd(\nu-2,4)$ points of cone angle $2\pi(\nu-2)/g_B\geq4\pi$; so every vertex of $\mathcal{P}$ lies in Σ. The half-turn $z\mapsto-z$ is $T^\nu=\iota$; it maps v_j to $v_{j+2\nu}$ and e_j to $e_{j+2\nu}$.

Let y_j be the height of v_j, $x(v_j)=\rho_j\sin j\theta$ and $w_j=y_{j-1}-y_j$. By the proof of [16, Theorem 5.15], for $1\leq j\leq\nu$, $w_j=\sin((j+1)\theta)$ for even j and $w_j=\sin((j-2)\theta)$ for odd j, and

$$0=y_\nu<y_{\nu-1}<\cdots<y_3<y_2<y_0<y_1,\qquad y_1-y_0=\sin\theta,\qquad y_0-y_2=\kappa\sin\theta.$$

The reflection $x\mapsto-x$ maps v_j to v_{-j} and e_j to e_{1-j}. The part of $\partial\mathcal{P}$ in the upper half-plane is the chain $v_{-\nu},\dots,v_\nu$; its right half rises along e_1 from v_0 to v_1 and then descends strictly

to v_ν, and its left half is the mirror image. So a horizontal line at a height in $(0, y_1)$ that is not the height of a vertex meets $\mathcal{P}$ in: for heights in (y_j, y_{j-1}), $3 \le j \le \nu$, one chord from e_{1-j} to e_j, and these chords form the strip Π_j, of height w_j; for heights in (y_2, y_0), one chord from e_{-1} to e_2, passing below v_0, forming the neck N, of height $\kappa \sin\theta$; for heights in (y_0, y_1), two chords, from e_1 to e_2 and from e_{-1} to e_0, forming the right and the left tip, of height $\sin\theta$. The neck and the tips are the strips Π_2 and Π_1^{r}, Π_1^{l} of [19, §8.3], written there for an odd d in place of ν; that the chords lie in $\mathcal{P}$ is [16, Lemma 5.13] and the paragraph after it. The lower half of $\mathcal{P}$ is the union of the images $\Pi'_j = \iota(\Pi_j)$, with left side $e_{2\nu+j}$ and right side $e_{2\nu+1-j}$ and top at the height $-y_j$, of $\mathrm{N}' = \iota(\mathrm{N})$ and of the two lower tips.

Proposition 6.9. *The horizontal direction of X is completely periodic, with exactly ν maximal cylinders: the cylinders C_{T}, C_{W}, C_{Z_j} and C_{Y} of the table and their images under ι.*

cylinder	*made of*	*height*	*circumference*
C_{T}	*right tip, top slab of* Π'_5, *left tip,* Π'_3	$\sin\theta$	$2\kappa(\kappa+2)\cos\theta$
C_{W}	N, *bottom slab of* Π'_5	$\kappa\sin\theta$	$2\kappa(\kappa+1)\cos\theta$
C_{Z_j}, j *even,* $4 \le j \le \nu-4$	Π_j, Π'_{j+3}	$\sin((j+1)\theta)$	$2\kappa\cot\theta\,\sin((j+1)\theta)$
C_{Y}	$\Pi_{\nu-2}$, Π_ν	$\cos\theta$	$2\kappa\cot\theta\,\cos\theta$

Their moduli are $\tan\theta/(2\kappa(\kappa+2))$ *for* C_{T}, $\tan\theta/(2(\kappa+1))$ *for* C_{W}, *and* $\tan\theta/(2\kappa)$ *for* C_{Y} *and each* C_{Z_j}; ι *preserves moduli.*

Proof. Each step uses the gluing rule and [16, Lemma 5.14]: strips glued in a cycle, side to side at equal heights, form an annulus of closed horizontal leaves whose circumference is the sum of the lengths of the chords at corresponding heights, and it is a maximal cylinder if each of its boundary components contains a point of Σ.

C_{T}: the right tip leaves through $e_2 \to e_{2\nu+5}$, the left side of Π'_5, with $v_1 \mapsto v_{2\nu+5}$, the top of Π'_5; as $\sin\theta < w_5 = \sin 3\theta$, it fills the top slab of Π'_5, of height $\sin\theta$. This slab leaves through $e_{2\nu-4} \to e_{-1}$, with $v_{2\nu-5} \mapsto v_{-1}$, the apex of the left tip, which it fills. The left tip leaves through $e_0 \to e_{2\nu+3}$, the left side of Π'_3, with $v_{-1} \mapsto v_{2\nu+3}$; as $w_3 = \sin\theta$ it fills Π'_3, which leaves through $e_{2\nu-2} \to e_1$, the left side of the right tip, with $v_{2\nu-3} \mapsto v_1$. On the upper boundary the tips have width 0, so the circumference is $2x(v_5)+2x(v_3) = 2\cot\theta(\sin 5\theta+\sin 3\theta) = 16\cos^3\theta\cos 2\theta = 2\kappa(\kappa+2)\cos\theta$, as $\kappa+2 = 4\cos^2\theta$.

C_{W}: the neck has heights $(y_1 - \sin 3\theta, y_1 - \sin\theta)$ and leaves through $e_2 \to e_{2\nu+5}$, whose translation takes y_1 to $-y_5$; so it fills the part of Π'_5 of heights $(-y_4, -y_5 - \sin\theta)$, the bottom slab, which leaves through $e_{2\nu-4} \to e_{-1}$, whose translation takes $-y_5$ to y_1, and arrives at the left side of N. On the lower boundary the circumference is $2x(v_2) + 2x(v_4) = 4\rho_0 \sin 3\theta\cos\theta = 2\kappa(\kappa+1)\cos\theta$, as $\sin 3\theta/\sin\theta = \kappa+1$.

C_{Z_j}, j even, $4 \le j \le \nu-4$: $e_j \to e_{2\nu+j+3}$, the left side of Π'_{j+3}, with v_{j-1}, the top of Π_j, going to $v_{2\nu+j+3}$, the top of Π'_{j+3}, and $w_{j+3} = \sin((j+1)\theta) = w_j$. The strip Π'_{j+3} leaves through its right side $e_{2\nu-j-2} \to e_{1-j}$, the left side of Π_j, top to top. The circumference is $2x(v_{j-1}) + 2x(v_{j+3}) = 4\cot\theta\cos 2\theta\sin((j+1)\theta)$.

C_{Y}, where ν even enters: $e_{\nu-2} \to e_{1-\nu}$, the left side of Π_ν, with $v_{\nu-3}$, the top of $\Pi_{\nu-2}$, going to $v_{1-\nu}$, the top of Π_ν, and $w_{\nu-2} = \sin((\nu-1)\theta) = \cos\theta = w_\nu$. The strip Π_ν leaves through $e_\nu \to e_{3-\nu}$, the left side of $\Pi_{\nu-2}$, with $v_{\nu-1} \mapsto v_{3-\nu}$. The circumference is $2\cot\theta(\sin((\nu-3)\theta) + \sin((\nu-1)\theta)) = 4\cot\theta\cos 2\theta\cos\theta$.

The boundary components of C_{T}, C_{W}, C_{Z_j}, C_{Y} contain v_1 and v_0; v_0 and $v_{\pm 2}$; v_{j-1} and v_j; $v_{\nu-3}$ and $v_{\nu-2}$; all lie in Σ, so these annuli and their images under ι are maximal cylinders.

Each upper piece is used once: the tips by C_{T}, N by C_{W}, Π_3 and the two slabs of Π_5 by $\iota(C_{\mathrm{T}})$ and $\iota(C_{\mathrm{W}})$, Π_k by C_{Z_k} for even $k \in [4, \nu-4]$ and by $\iota(C_{\mathrm{Z}_{k-3}})$ for odd $k \in [7, \nu-1]$, and $\Pi_{\nu-2}$, Π_ν by C_{Y}. The lower pieces are the images under ι. So the cylinders cover X up to finitely many segments, and there are $2(3+(\nu-6)/2) = \nu$ of them. □

Lemma 6.10. *The set $\{C_{\mathrm{T}}, \iota(C_{\mathrm{T}})\}$ is free.*

Proof. Multiplied by $2\kappa(\kappa+1)(\kappa+2)/\tan\theta$, the moduli of C_{T}, C_{W} and of C_{Y} and the C_{Z_j} become $\kappa+1$, $\kappa(\kappa+2)$ and $(\kappa+1)(\kappa+2)$. If $\kappa+1 = \alpha\kappa(\kappa+2) + \beta(\kappa+1)(\kappa+2)$ with $\alpha, \beta \in \mathbb{Q}$, then κ is a root of $(\alpha+\beta)t^2 + (2\alpha+3\beta-1)t + (2\beta-1)$, which is not the zero polynomial, as $\alpha+\beta = 0$ and $2\beta = 1$ give $2\alpha+3\beta-1 = -\frac{1}{2}$. But $\kappa = 2\cos(2\pi/N)$ has degree $\varphi(N)/2 \geq 4$ over $\mathbb{Q}$, as $N \geq 16$. □

Theorem 6.11. *Let $4 \mid N$, $N \geq 16$, and $\Delta = \Gamma_1$. Then $V = E^-$; so $S = F$ and $\mathcal{M} = \mathcal{L}$.*

Proof. Let a be the side e_0 oriented from v_{-1} to v_0; by Lemma 6.8(b), $T^k\mathrm{a}$ is e_{-2k} oriented from v_{-2k-1} to v_{-2k}, and by Lemma 6.8(c) each $H^1(X,\Sigma)_\ell$ is a line. Let Ξ and Ξ' be the classes of C_{T} and $\iota(C_{\mathrm{T}})$, and $f(k) = \Xi(T^k\mathrm{a})$. By the proof of Proposition 6.9, the interior of C_{T} meets the sides of $\mathcal{P}$ only in open segments of e_2, e_0, $e_{2\nu-4}$ and $e_{2\nu-2}$, the right sides of its four pieces, each joining its top to its bottom; oriented from v_{i-1} to v_i, each runs downwards. By Lemma 6.7,

$$f(k) = -1 \quad \text{for } k \equiv 0,\ -1,\ 2-\nu,\ 1-\nu \pmod N, \qquad f(k) = 0 \text{ otherwise.}$$

The half-turn ι preserves the orientation of X and exchanges the tops and bottoms of horizontal cylinders, so $\Xi'(T^k\mathrm{a}) = -f(k+\nu)$. By Proposition 6.9 and Lemma 6.10, Lemma 6.7 applies to $\{C_{\mathrm{T}}, \iota(C_{\mathrm{T}})\}$, whose cylinders have height $\sin\theta$; so $(T^k)^*\eta \in V$ for all k, where $\eta = \Xi + \Xi'$. As $\eta(T^k\mathrm{a}) = f(k) - f(k+\nu)$ and $\zeta^\nu = -1$,

$$\hat\eta(\ell) = \frac{1-(-1)^\ell}{N} \sum_k \zeta^{-\ell k} f(k) = -\frac{1-(-1)^\ell}{N}(1+\zeta^\ell)(1+\zeta^{\ell(\nu-2)}).$$

Let ℓ be odd. Then $1+\zeta^\ell \neq 0$, as $\ell \not\equiv \nu$; and $\ell(\nu-2) \equiv \nu - 2\ell \pmod N$, so $1+\zeta^{\ell(\nu-2)} = 0$ would give $2\ell \equiv 0$. So $\hat\eta(\ell) \neq 0$ for every odd ℓ, and by Lemma 6.8(c) the $(T^k)^*\eta$ span E^-. With $V \subset E^-$ (Section 2.2), $V = E^-$. By (2.1) and (1.2), $S = F$, and $\mathcal{M} = \mathcal{L}$ by Lemma 2.2. □

On Γ_2 and Γ_4 the unfolding is the model of [16, Lemma 5.1]. There are no relative characters, so $V \cap Z = 0$. We find horizontal cylinders whose moduli are pairwise not rational multiples of each other, separated by a Galois automorphism, and bound the rank from below by Lemma 2.16(g); by Lemma 2.6 the bound forces $H = G$, and $S = F$ follows, by Theorem 1.5 if $N > 30$. On Γ_4 with $N \in \{28, 36, 44, 60\}$ the cylinders are found by computation. The proofs are in the supplement (§S3).

Theorem 6.12. *Let $8 \mid N$, $N \geq 16$, and $\Delta = \Gamma_2$. The unfolding has $N/4-1$ horizontal cylinders whose moduli are pairwise not rational multiples of each other. Hence $S = F$ and $\mathcal{M} = \mathcal{L}$.*

Theorem 6.13. *Let $N \equiv 4 \pmod 8$, $N \geq 28$, and $\Delta = \Gamma_4$. Then $\operatorname{rank}\mathcal{M} = N/4-1$, $S = F$ and $\mathcal{M} = \mathcal{L}$.*

6.3. **Five short proofs.** For even N and odd ν, reduction modulo ν maps G isomorphically onto $(\mathbb{Z}/\nu)^\times$; we write $\bar{H}$ for the image of a subgroup H, and for integers b, x prime to ν, $b/x \in \bar{H}$ means that the class of bx^{-1} modulo ν lies in $\bar{H}$.

Lemma 6.14. *Let N be even, $c, \sigma \geq 1$ with $c + 2\sigma = \nu$, and $\Delta = (c, \sigma, \sigma + \nu)/N$. An odd x lies in Φ if and only if $0 < [xc] < \nu$.*

Proof. Put $r = [xc]$. As x is odd, $2x\sigma = x\nu - xc \equiv \nu - r$, and $\nu - r$ is even, as $r \equiv c \equiv \nu \pmod 2$. So with $\rho = (\nu - r)/2$ the residues of $x\sigma$ and $x(\sigma + \nu) \equiv x\sigma + \nu$ are those of ρ and $\rho + \nu$. If $0 < r < \nu$, then $0 < \rho < \nu/2$ and the three residues add up to $r + \rho + (\rho + \nu) = N$. If $\nu < r < N$, then $-\nu/2 < \rho < 0$ and they add up to $r + (\rho + N) + (\rho + \nu) = 2N$. If $r \in \{0, \nu\}$, a residue is 0. □

Theorem 6.15. *Let $\nu \geq 5$ be odd, $N = 2\nu$, and $\Lambda = (1, (\nu - 1)/2, (3\nu - 1)/2)/N$. The subgroups $H \ni -1$ of G with* (P) *on Λ are $\{\pm 1\}$, the group G when ν is prime, and $\{\pm 1, \pm 5\}$ when $\nu = 13$. In particular Λ satisfies* (N′) *when $\nu \geq 9$ is composite.*

Proof. By Lemma 6.14 with $c = 1$, the odd elements of Φ are the odd integers of $(0, \nu)$, read as residues. Let $H \ni -1$ be a subgroup and A the set of elements of H in $(0, \nu)$; then $H = A \sqcup (-A)$. A pair on a diagonal $1 - a'$, $a' \in H$, with a unit member consists of odd characters, so of two odd integers $x, b \in (0, \nu)$.

Step 1: (P) in integers. H has (P) if and only if for every $\alpha \in A$: (I_α) for all odd $x, b \geq 1$ with $x + b = \alpha + 1$, x and b are both prime to ν or both not, and $b/x \in \bar{H}$ in the first case; (II_α) for all even $y, z \geq 2$ with $y + z = \alpha - 1$, y and z are both prime to ν or both not, and $z/y \in \bar{H}$ in the first case. Indeed, for $a' = -\alpha$, $2 \leq x + b \leq N - 2$ and $2 \leq 1 + \alpha \leq \nu$, so $x + b = 1 + \alpha$. For $a' = \alpha$, $x + b = N + 1 - \alpha$; with $x = \nu - y$, $b = \nu - z$ this is $y + z = \alpha - 1$ with y, z even and positive, $\gcd(\nu - y, \nu) = \gcd(y, \nu)$, and $b/x \equiv z/y \pmod \nu$.

Step 2: A is a progression. Let H have (P). For $\alpha < \alpha'$ in A, ($\mathrm{I}_{\alpha'}$) with $x = \alpha$ shows that $b = \alpha' + 1 - \alpha$ is a unit with $b/\alpha \in \bar{H}$, so $b \in H$, and b is odd in $[3, \alpha']$, so $b \in A$. Hence $D = \{\alpha - 1 : \alpha \in A\}$ contains 0 and $\delta' - \delta$ for $\delta < \delta'$ in D, and if g is its least positive element, D is the set of multiples of g up to its largest element. So $A = \{1 + jg : 0 \leq j \leq n\}$ with $g \geq 2$ even, and $n = 0$ if and only if $H = \{\pm 1\}$.

Step 3: the cases. Let $H \neq \{\pm 1\}$ have (P), so $n \geq 1$ and $1 + g \leq \nu - 2$. If $g = 2$ and $n \geq 3$, then $7 \in A$, and (II_7) on $(2, 4)$ gives $2 \in \bar{H}$; so the element of H that is $\equiv -2 \pmod \nu$, which is $\nu - 2$, lies in A, and A is the set of all odd integers of $(0, \nu)$, all prime to ν; so ν is prime and $H = G$. If $g = 2$ and $n \leq 2$, then $9 \in H$ is $\equiv \pm 1, \pm 3$, or $\pm 1, \pm 3, \pm 5 \pmod \nu$, so ν divides one of $8, 10, 6, 12, 4, 14$; with $2n + 1 \leq \nu - 2$ this leaves $(\nu, n) = (5, 1), (7, 2)$, and again $H = G$. If $g = 4$ and $n \geq 2$, then $9 \in A$, and (II_9) on $(2, 6)$ gives $3 \in \bar{H}$, so $3 \in A$, which is not $\equiv 1 \pmod 4$. So $n = 1$, $H = \{\pm 1, \pm 5\}$, and $25 \equiv \pm 1$ or $\pm 5 \pmod \nu$; so ν divides 24, 26, 20 or 30, and as $5 \nmid \nu$ and $\nu \geq 7$, $\nu = 13$. If $g \geq 6$, (II_{1+g}) on $(2, g - 2)$ gives $k = g/2 - 1 \in \bar{H}$, with $2 \leq k < 1 + g$. If $4 \mid g$, k is odd, so $k \in A$ with $1 < k < 1 + g$, which is impossible. So $g = 2u$ with $u \geq 3$ odd, $k = u - 1$ is even, the element of H that is $\equiv -k$ is $\nu - k \in A$, and $\nu - u + 1 = 1 + 2uj'$ with $1 \leq j' \leq n$. So $\nu = um$ with $m = 2j' + 1 \geq 3$, and $A = \{1 + 2uj : 0 \leq j \leq (m - 1)/2\}$, as $1 + 2un < \nu$. Put $w = 1 + 2u$. For $0 \leq j \leq (m - 1)/2$ the element $w(1 + 2uj) = 1 + 2u(1 + jw)$ of H is $\equiv 1 \pmod u$, so it is not in $-A$; it lies in A, and it is the residue $1 + 2us_0$ with $s_0 = (1 + jw) \bmod m$, which must be at most $(m - 1)/2$. Hence $j \mapsto (1 + jw) \bmod m$ maps $J = \{0, \dots, (m - 1)/2\}$ injectively into J, so it permutes J. Summing over J, $(m + 1)/2 + (w - 1)(m^2 - 1)/8 \equiv 0 \pmod m$, and multiplying by 8, $w \equiv 5 \pmod m$; as w is a unit, $m \neq 5$. If $m \geq 7$, let j_0 be the least $j \geq 0$ with $1 + 5j > (m - 1)/2$; then $1 \leq j_0 \leq (m - 1)/2$ and $(m - 1)/2 < 1 + 5j_0 \leq (m - 1)/2 + 5 < m$ for $m \geq 11$, so

$(1+5j_0) \bmod m \notin J$; for $m = 7, 9$, $j = 1$ gives $6 \notin J$. So $m = 3$, $\nu = 3u$, $w \equiv 2 \pmod 3$, $u \equiv 2 \pmod 3$, $u \geq 5$, and $H = \{\pm 1, \pm w\}$. Now (I_w) on $(x, b) = (5, 2u-3)$: $b \equiv 1 \pmod 3$ and $\gcd(b, u) = \gcd(3, u) = 1$, so b is a unit. If $5 \mid u$, x is not a unit, against (I_w). If $5 \nmid u$, (I_w) asks $2u-3 \equiv \pm 5$ or $\pm 5w \pmod{3u}$, that is, $3u$ divides $2u-8$, $2u+2$, $8u+8$ or $12u+2$; none holds for odd $u \geq 5$.

Converse. For $\{\pm 1\}$, (I_1) is the pair $(1, 1)$. For ν prime and $H = G$, every integer in sight is prime to ν and every quotient lies in $\bar{G}$. For $\nu = 13$ and $A = \{1, 5\}$: (I_5) is $(1, 5), (3, 3), (5, 1)$, with quotients 5, 1, $5^{-1} \equiv -5$, and (II_5) is $(2, 2)$.

For composite $\nu \geq 9$, a closed set containing 1 whose unit part has conductor $N' = \nu$ is that unit part and has (P) (Lemmas 2.7 and 3.3), so it is $\{\pm 1\}$. □

Theorem 6.16. *Let $4 \mid N$, $3 \nmid N$ and $N \geq 40$. Every subgroup $H \ni -1$ of G with* (P) *on $\Theta_0 = (2, \nu-3, \nu+1)/N$ is $\{\pm 1\}$, or N is a power of 2 and $H = G$. So Θ_0 satisfies* (N′).

Proof. By Lemma 6.4 we may replace Θ_0 by $(1, 2, N-3)/N$. Let I_1 be the set of odd x with $[x] \in (0, N/3)$ and I_2 the set with $[x] \in (\nu, 2N/3)$, so that the odd elements of Φ form $I_1 \cup I_2$ (Lemma 6.5(c)); we identify residues with these integers. Put $A_1 = H \cap I_1$ and $\Gamma = \{\gamma \text{ odd} : \ 0 < \gamma < N/6, \ \nu + \gamma \in H\}$, so that $H = \pm(A_1 \cup (\nu + \Gamma))$.

Three rules. For $\alpha \in A_1$ the pairs on the diagonal $1 + \alpha$ include the $x, b \in I_1$ with $x + b = \alpha + 1$; on the diagonal $1 - \alpha$, the $x \in I_1$, $b \in I_2$ with $x + b = N + 1 - \alpha$; for $\gamma \in \Gamma$, on the diagonal $1 + \nu + \gamma$, the $x \in I_1$ and $b = \nu + \eta \in I_2$ with $x + \eta = \gamma + 1$, and the $x = \nu + \xi$, $b \in I_1$ with $\xi + b = \gamma + 1$. Taking for x an element of H, (P) makes b a unit with $b = x \cdot (b/x) \in H$:

(C1) if $\alpha \leq \alpha'$ lie in A_1, then $1 + \alpha' - \alpha \in A_1$;

(C2) if $\gamma \leq \gamma'$ lie in Γ, then $1 + \gamma' - \gamma \in A_1$;

(C3) if $\alpha \in A_1$, $\gamma \in \Gamma$ and $\alpha + \gamma > N/6 + 1$, then $\nu + 1 - \alpha - \gamma \in A_1$ (diagonal $1 - \alpha$, $x = \nu + \gamma$; then $b = \nu + 1 - \alpha - \gamma$ is odd and lies in $(0, N/3)$).

If $A_1 \neq \{1\}$, let $1 + g$ be its least element above 1; by (C1), $\alpha' - g \in A_1$ for $\alpha' \in A_1$, $\alpha' > 1$, so $A_1 = \{1 + jg : \ 0 \leq j \leq n\}$, and g is even.

The element $3g - 1$. If $N \equiv 2 \pmod 3$, or $3g - 1 < \nu$, then $3g - 1 \in H$. We use the diagonal $1 - (1+g) = -g$. If $N \equiv 1 \pmod 3$, let $x = (N-1)/3 \in I_1$ and $b = (2N+1-3g)/3$, an odd integer below $2N/3$, and above ν when $3g - 1 < \nu$. Then $x + b = N - g$, $3x \equiv -1$, so x is a unit, and $3b \equiv 1 - 3g$, so $b/x \equiv 3g - 1$. If $N \equiv 2 \pmod 3$, let $x = (N+1)/3 - g$, odd and in $(0, N/3)$ as $2 \leq g < N/3 - 1$, and $b = (2N-1)/3 = \nu + (N-2)/6 \in I_2$. Then $x + b = N - g$, $3b \equiv -1$ and $3x \equiv 1 - 3g$, so $x/b \equiv 3g - 1$.

Step 1: $A_1 = \{1\}$. By (C2), $|\Gamma| \leq 1$. Let $\Gamma = \{\gamma\}$. If $\gamma \geq 3$: on the diagonal $1 + \nu + \gamma$, $x = 3$ (a unit, as $3 \nmid N$) and $b = \nu + \gamma - 2 \in I_2$ form a pair, so $b \equiv \pm 3$ or $b \equiv \pm(\nu + 3\gamma)$; but $b \in (\nu, 2N/3)$ is neither 3 nor $N-3$, $b \equiv \nu + 3\gamma$ gives $2\gamma + 2 \equiv 0$, impossible as $0 < 2\gamma + 2 < N$, and $b \equiv -\nu - 3\gamma$ gives $4\gamma - 2 \equiv 0$, impossible modulo 4. If $\gamma = 1$, then $H = \{\pm 1, \pm u_\iota\}$, and the pairs on the diagonal $2 + \nu$ include the $x, b \in I_1$ with $x + b = \nu + 2$. If $N \equiv 4 \pmod 8$, take $x = N/4 + 2$ and $b = N/4$: x is odd with $\gcd(x, N) \mid 8$, so a unit, while b is not, against (P). If $8 \mid N$, take $x = N/4 + 3$ and $b = N/4 - 1$, units as $\gcd(x, N) \mid 12$ and $\gcd(b, N) \mid 4$; and $b/x \in \{\pm 1, \pm u_\iota\}$ would give $4 \equiv 0$, $\nu + 2 \equiv 0$, $\nu + 4 \equiv 0$ or $2 \equiv 0$. So $H = \{\pm 1\}$.

Step 2: $A_1 \neq \{1\}$ and $3g - 1 < N/3$. Then $3g - 1 \in A_1$, so $3g - 1 = 1 + jg$, $g \mid 2$ and $g = 2$. We show by induction that every odd $n < \nu$ lies in H; $1, 3 \in A_1$. Let $n \geq 5$. If $3 \mid n$, $n = 3 \cdot (n/3) \in H$. Otherwise let $t = 1$ if $n \equiv 2$ and $t = 5$ if $n \equiv 1 \pmod 3$; then $t < n$, $6 \mid n + t$, and $\alpha = 1 + (n + t)/3$ is odd, below n and below $N/3$, so $t \in H$ and $\alpha \in A_1$. Of n and t one, u, is $\equiv N$ and the other, v, is $\equiv 2N \pmod 3$; let $x = (N - u)/3 \in I_1$ and

$b = (2N - v)/3 \in I_2$. Then $x + b = N + 1 - \alpha$, so (x, b) is a pair on the diagonal $1 - \alpha$, with $-3x \equiv u$ and $-3b \equiv v$; the member that belongs to t is a unit, so the other is, n is a unit, and n/t or t/n lies in H, so $n \in H$. Hence every odd integer below ν is prime to N; as an odd prime of N would be at most $N/4$, N is a power of 2, and $H = G$.

Step 3: $A_1 \neq \{1\}$ and $3g - 1 > N/3$. Then $A_1 \subset \{1, 1 + g, 1 + 2g\}$, and as $2g > N/6$, by (C2) two elements of Γ differ by 0 or g. On the diagonal $1 + (1 + g)$, $x = 3$ and $b = g - 1$ form a pair, so $g - 1 \in 3H$: $g - 1$ is $\equiv \pm 3$, $\pm 3(1 + g)$, $\pm 3(1 + 2g)$ (the last only if $1 + 2g \in A_1$, so $g < N/6$), or $\pm(\nu + 3\gamma)$ with $\gamma \in \Gamma$. Here $g - 1 \equiv 3$ gives $g = 4$ and $N < 33$; $g - 1 \equiv -3$, $3 + 3g$ or $3 + 6g$ give $g + 2$, $2g + 4$ or $5g + 4 \equiv 0$, impossible as these lie in $(0, N)$; $g - 1 \equiv -3 - 3g$ gives $4g + 2 \equiv 0$, impossible modulo 4; and $g - 1 \equiv \nu + 3\gamma$ is impossible as $\nu + 3\gamma + 1 - g \in (N/6, N)$. Two cases remain. *Case $g - 1 \equiv -3 - 6g$.* Then $7g + 2 = N$, $g = (N - 2)/7$, and $1 + 2g \in A_1$. Here $3g - 1 = (3N - 13)/7 \in (N/3, \nu)$, so $3g - 1 \in H$, and as it is not in Φ, $N + 1 - 3g \in H \cap I_2$, that is, $\gamma^\circ = \nu + 1 - 3g = (N + 26)/14 \in \Gamma$. Then (C3) with $\alpha = 1 + g$ and γ° gives $(2N - 11)/7 \in A_1 = \{1, (N + 5)/7, (2N + 3)/7\}$, so $N \in \{9, 16\}$. *Case $g - 1 \equiv -\nu - 3\gamma$.* Then $g - 1 + 3\gamma \in (0, 5N/6)$ is $\equiv \nu$, so $\gamma^* = (\nu + 1 - g)/3 \in \Gamma$, and (C3) with $\alpha = 1 + g$ and γ^* gives $\beta = (N - 1 - 2g)/3 \in A_1$. If $\beta = 1$, then $g = (N - 4)/2 > N/3$, which is impossible. If $\beta = 1 + 2g$, then $g = (N - 4)/8$ and $\beta = N/4$, not a unit. If $\beta = 1 + g$, then $g = (N - 4)/5$, $1 + 2g > N/3$, $\gamma^* = (N + 6)/10$ and $\gamma^* \pm g \notin (0, N/6)$, so $H = \pm\{1, (N + 1)/5, 3(N + 1)/5\} = \pm\{1, 5^{-1}, 3 \cdot 5^{-1}\}$; then $5^{-2} \in H$, so N divides one of $24, 26, 4, 6, 14, 16$. So Step 3 does not occur for $N \geq 40$. For the last statement, a closed set containing 1 whose unit part has conductor $N' = N$ is that unit part, with (P) (Lemmas 2.7 and 3.3), so it is $\{\pm 1\}$. □

6.4. **The other families.** The following statements are proved in the supplement (§S4). For $N \not\equiv 0 \pmod 4$ let $\sigma_0 = 0$ if N is odd and $\sigma_0 = \nu$ if $N \equiv 2 \pmod 4$.

Theorem 6.17. *Let N be composite with $4 \nmid N$ and with composite odd part, and let Δ have $\gcd(p_i, N) \leq 2$ for each i and $2 + \sigma_0 \in \Phi$. Then Δ satisfies* (N′).

Two instances of rule (iii) on the diagonal $1 + k$, for a unit k of a closed set, act like the map $k \mapsto (1 \pm k)/2$ on its unit part; a unit part of conductor N' is then forced to inject modulo every odd prime of N and to be stable under this map, which is impossible when the odd part of N is composite. The theorem applies to $\mathcal{A}_2 = (1, \nu - 2, \nu + 1)/N$ with $N \equiv 2 \pmod 4$ and ν composite: the residues of $(2 + \nu)(1, \nu - 2, \nu + 1)$ are $\nu + 2$, $\nu - 4$ and 2.

Theorem 6.18. *Let $N = 4m$.*

(a) *If $12 \mid N$ and $N \geq 84$, no subgroup $H \ni -1$ of G other than $\{\pm 1\}$ with conductor N satisfies* (P) *on Θ_0.*

(b) *Let $m > 1$ be odd, $\Theta_1 = (1, 4, N - 5)/N$ and $\Theta_2 = (4, \nu - 5, \nu + 1)/N$. If $N \geq 76$ and m is not prime, no subgroup $H \ni -1$ of G other than $\{\pm 1\}$ satisfies* (P) *on Θ_1 or on Θ_2. If $m \geq 7$ is prime, every subgroup $H \ni -1$ with* (P) *on Θ_1 or on Θ_2 is $\{\pm 1\}$ or G.*

(c) *Let $m \geq 45$ be odd and $\Theta_3 = (4, \nu - 3, \nu - 1)/N$. Every subgroup $H \ni -1$ of G other than $\{\pm 1\}$ with* (P) *on Θ_3 has conductor different from N.*

So these triangles satisfy (N′) *at these N.*

Here Θ_2 has the numerators of Θ_1 multiplied by u_ι, so Lemma 6.4 reduces it to Θ_1.

Theorem 6.19. *Let $d \mid N$ with $n = N/d \geq 5$ odd, and suppose that N is odd and $d \geq 3$, or $N \equiv d \equiv 0 \pmod 4$, or $N \equiv d \equiv 2 \pmod 4$ and $d \geq 6$; suppose $N \neq 15$. On the unfolding of $\mathcal{A}_d = (1, (N - d)/2 - 1, (N + d)/2)/N$ every unit lies in S. Hence $S = F$ when $N > 30$.*

The last sentence follows from Theorem 1.5, as S is closed.

Theorem 6.20. *Let $N \geq 7$ be odd, $N \neq 9$, and $\Delta = \mathcal{A}_1 = (1, (N-3)/2, (N+1)/2)/N$. Then $V = H^1(X, \Sigma; \mathbb{C})$, and the orbit of the unfolding is dense in its connected component of $\mathcal{H}((N-1)/2, (N-5)/2)$ if $3 \nmid N$, and of $\mathcal{H}((N-1)/2, ((N-9)/6)^3)$ if $3 \mid N$. In particular $S = F$.*

Its proof is that of Theorem 6.11: the unfolding is the star, and one free set of cylinders and its images under T span $H^1(X, \Sigma; \mathbb{C})$.

Theorem 6.21. *Let $N > 400$ and let $\Delta = \mathcal{B}_{k,d}$ be a triangle of the family $\mathcal{B}$ of Proposition 4.1 with $d \geq 5$, other than the sixteen triangles of Proposition 8.3. Then Δ satisfies* (N′).

Remark 6.22. Delecroix and Rüth ask whether the tangent vectors that the cylinder deformation theorem gives in the directions with cylinders eventually span the tangent space of the orbit closure [10, Question 3.1]. On Γ_1 with $4 \mid N$, $N \geq 16$, and on $\mathcal{A}_1$ with $N \geq 7$ odd, $N \neq 9$, those of finitely many directions span it. The twist ξ of a free set $\mathcal{G}$ of cylinders (Lemma 6.7) lies in the span of the vectors that one step of their algorithm gives in the direction of $\mathcal{G}$ (Section 8.1), and $(T^k)^*\xi$ is the twist of the free set $T^{-k}(\mathcal{G})$; in the proofs of Theorems 6.11 and 6.20, the $(T^k)^*\xi$ for one such ξ span V.

7. An angle $\pi/3$

In this section $12 \mid N$ and Δ has an angle $\pi/3$. Let p be the smaller of the two other numerators. Then

$$\Delta = (p, N/3, 2N/3 - p)/N, \qquad 1 \leq p < N/3, \qquad \gcd(p, N/3) = 1,$$

and conversely every such triple is a scalene triangle with an angle $\pi/3$ (its numerators are distinct as $p \neq N/3$, and their greatest common divisor is $\gcd(p, N/3)$). We name the vertices so that A has the angle $p\pi/N$, B the angle $\pi/3$ and C the angle $(2N/3 - p)\pi/N$, and we write

$$\mu = N/12, \qquad \rho = p/\mu \in (0, 4), \qquad g = \gcd(p, N).$$

As $N/3 = 4\mu$ is even, p is odd; and $g \in \{1, 3\}$, with $g = 3$ exactly when $3 \mid p$.

By Proposition 2.8 the rules alone cannot give $S = F$ here. We find the units $\equiv \pm 1 \pmod{12}$ in S by the rules (Section 7.3), and exclude $S \cap G = H_{12}$ with one cylinder of the direction of a side of Δ, through Lemma 2.16 (Section 7.2). The cylinder must be written down exactly, and which cylinder works depends on ρ.

Theorem 7.1. *Let $N > 58$ with $12 \mid N$, and let $\Delta = (p, N/3, 2N/3 - p)/N$ with $1 \leq p < N/3$ and $\gcd(p, N/3) = 1$. Then every unit lies in S, $S = F$, and $\mathcal{M} = \mathcal{L}$.*

The last two assertions follow from the first by Theorem 1.5 and Corollary 2.4. The proof is organized by four settings, which are disjoint and cover every Δ of Theorem 7.1:

(I) $N = 12 \cdot 2^a 3^b$ $(a, b \geq 0)$ and $3 \nmid p$;
(II) $N = 3 \cdot 2^{a+2}$ $(a \geq 0)$ and $3 \mid p$;
(III) some prime $q \geq 5$ divides N, and $3 \nmid p$;
(IV) some prime $q \geq 5$ divides N, and $3 \mid p$.

Indeed, if $3 \mid p$ then $3 \nmid N/3$, so $9 \nmid N$, and if moreover no prime $q \geq 5$ divides N then $N = 3 \cdot 2^{a+2}$. In (I) and (III), $g = 1$; in (II) and (IV), $g = 3$. In (I) and (II) every element of F is a unit, since it is prime to 6 (proof of Proposition 2.8).

Section 7.1 describes the unfolding as a star of N isosceles triangles and $N/3$ equilateral ones (Figure 1) and follows the leaves of the directions of the sides AB and AC. Section 7.2 states what one cylinder forces when $S \cap G = H_{12}$, as a test on the list of the cylinder's crossings. Section 7.3 proves that $H_{12} \subset S$. Section 7.4 constructs cylinders of the direction of AC that pass the test on whole ranges of ρ and carries the case $p = 1$ through in full (Proposition 7.21), and Section 7.5 gives the plan of the proof in the four settings, whose cases are treated in the supplement (§S5).

7.1. **The star.** Let $\vartheta = \pi/N$ and $\alpha = p\vartheta$, the angle at A, so that $0 < \alpha < \pi/3$. Scale Δ so that its circumscribed circle has diameter 1; then

$$|BC| = s := \sin\alpha, \qquad |CA| = \tfrac{\sqrt{3}}{2}, \qquad |AB| = \ell := \sin(\tfrac{\pi}{3} + \alpha) = \tfrac{\sqrt{3}}{2}\cos\alpha + \tfrac{1}{2}\sin\alpha.$$

Directions in the plane are angles modulo 2π, and $\zeta = e^{2\pi i/N}$; for a real x we write $\zeta^x = e^{2\pi i x/N}$.

Lemma 7.2. *The unfolding (X, ω) is obtained from the following pieces, glued by translations.*

(1) *For each $J \in \mathbb{Z}/N$ a* corner *Q_J: an isosceles triangle with apex angle 2α, legs of length $\sqrt{3}/2$ and base of length $\sqrt{3}\,s$ at distance $\frac{\sqrt{3}}{2}\cos\alpha$ from the apex, whose base has outward normal of direction $2\pi J/N$. The leg of Q_J on the side of the direction $2\pi J/N + \alpha$ is glued to a leg of Q_{J+p}, and the other leg to a leg of Q_{J-p}.*

(2) *For each $J \in \mathbb{Z}/N$ taken modulo $N/3$, an equilateral triangle E_J of side $\sqrt{3}\,s$, glued along its three sides to the bases of Q_J, $Q_{J+4\mu}$, $Q_{J+8\mu}$.*

The apices of the corners are the g points over A; the corners with apex at one of them are the Q_J with J in one class modulo g, and its cone angle is $2\pi p/g$. The center of E_J is a regular point over B, at distance $\ell = \frac{\sqrt{3}}{2}\cos\alpha + \frac{s}{2}$ from the apex of each of the three corners glued to E_J, and its vertices are the points over C. The rotation of the star that takes Q_J to Q_{J+1} is the deck transformation T.

Proof. The unfolding is the union of the $2N$ images of Δ under the group generated by the reflections in its sides, glued along their sides [19, §2.1]. Glue each image to its mirror image across its side AB: the union is a kite $ACBC'$ with angle 2α at A, angle $2\pi/3$ at B and sides $|AC| = |AC'| = \sqrt{3}/2$, $|BC| = |BC'| = s$. The segment CC' cuts the kite into the isosceles triangle ACC' (apex angle 2α, base $2 \cdot \frac{\sqrt{3}}{2}\sin\alpha = \sqrt{3}s$ at distance $\frac{\sqrt{3}}{2}\cos\alpha$ from A), which is a corner, and the triangle CBC', isosceles with apex angle $2\pi/3$ at B and legs s. The $2N$ images are the images of Δ under the $2N$ elements of the dihedral group generated by the reflections; this group contains the N rotations by the multiples of $2\pi/N$ [19, §2.1], and each kite contains exactly one image $\Theta\Delta$ with Θ a rotation (the other image is $\Theta\Delta$ reflected in $\Theta(AB)$). Index the kite of $\Theta\Delta$ by $J \in \mathbb{Z}/N$ when Θ is the rotation by $2\pi J/N$; then the vector from A to B in the kite has direction $2\pi J/N$, and it is the outward normal of CC'. Two kites that share a copy of AC are mirror images across it, so their directions of AB differ by $\pm 2\alpha = \pm 2\pi p/N$: this is the gluing of the legs. The angle at B is $\pi/3 = \pi(N/3)/N$ and $\gcd(N/3, N) = N/3$, so each point over B has cone angle 2π and is surrounded by six images of Δ, that is by three kites, whose directions of AB differ by $2\pi/3 = 2\pi \cdot 4\mu/N$. Their three triangles CBC' form an equilateral triangle of side $\sqrt{3}s$ with center the point over B and circumradius s; this is E_J. The center of E_J is at distance $|AB| = \ell$ from the apex of each of its three corners, and the identity $\ell = \frac{\sqrt{3}}{2}\cos\alpha + \frac{s}{2}$ is the addition formula. Around a point over A the corners follow each other through the leg gluings, so the corners

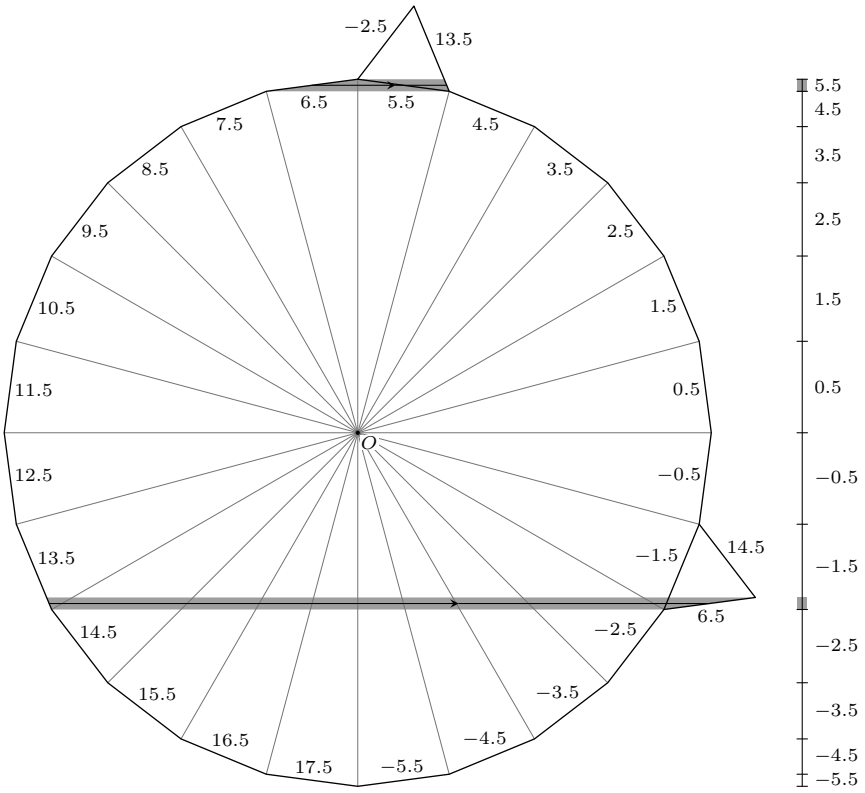


FIGURE 1. The star of the unfolding of $(1, 8, 15)/24$ ($p = 1$, $\mu = 2$), with the common apex O of its corners, in the frame of the flow of the direction of AC, which runs to the right. The base of index y is marked y inside the star, $-6 < y < 18$; the right bases are $-5.5, \dots, 5.5$. Of the equilateral triangles only the two on the bases $y_0 = 5.5$ and $y_1 = -1.5$ are drawn; each of their other two sides is marked with the index of the base to which it is glued, which is $y + 8$ for the side through the lower end of the base y (side 1) and $y + 16$ for the other (side 2), modulo 24. The shaded pieces form the cylinder $\mathcal{Z}$ of Proposition 7.21, and the lines with arrows are its leaf with $\eta = \Psi/2$. On the right, on the same vertical scale, are the windows (7.1) of the right bases, marked by their indices; the heights at which the leaves of $\mathcal{Z}$ leave the star, the top window and the bottom part of length Ψ of the window of y_1, are shaded.

with a common apex are the Q_{J+kp}, $k \in \mathbb{Z}$, that is the $Q_{J'}$ with $J' \equiv J \pmod g$; there are N/g of them, each with angle 2α, so the cone angle is $2\pi p/g$. Finally the rotation T' of the star taking Q_J to Q_{J+1} respects all the gluings and turns every direction by $2\pi/N$, so $T'^*\omega = \zeta\omega$; by [19, Theorem 6.2] the automorphisms with $T'^*\omega \in \mathbb{C}\omega$ are the powers of T, and T^k multiplies ω by ζ^k, so $T' = T$. □

The two side directions. The direction of AB is the set of directions $2\pi J/N$ (modulo π), and we let the flow run in the direction 0. As p is odd, the directions of the copies of AC, which make the angle $\pm\alpha$ with those of AB, are the odd multiples of π/N; for the direction of AC we let the flow run in the direction $-\vartheta$. In both cases we use the frame in which the flow is horizontal and runs to the right, and we index the bases by the angle between their

outward normal and the flow: the base of Q_J has index $y = J$ for AB and $y = J + \frac{1}{2}$ for AC, so that its outward normal has angle $2y\vartheta$ in that frame. A base is *right* if $\cos 2y\vartheta > 0$, that is $|y| < 3\mu$ for the representative y of its index in $(-6\mu, 6\mu]$. A leaf leaves the star through right bases and enters it through the other bases.

For a leaf leaving the star through the right base y we write c for its height above the apex of that corner, measured in the frame of the flow. The ends of the base y are at heights $\frac{\sqrt{3}}{2}\sin((2y \mp p)\vartheta)$, so

$$\tfrac{\sqrt{3}}{2}\sin\big((2y-p)\vartheta\big) < c < \tfrac{\sqrt{3}}{2}\sin\big((2y+p)\vartheta\big); \tag{7.1}$$

this open interval is the *window* of the base y.

Lemma 7.3. *Let a leaf of the direction of AB or AC leave the star through the right base y at height c, and let it meet no point over A or C before it leaves the star again.*

(a) *It crosses the equilateral triangle glued to the base y and enters the star through the base $x = y + 4\mu$ (*side 1*) if $c < (\ell + s)\sin 2y\vartheta$, and through the base $x = y + 8\mu$ (*side 2*) if $c > (\ell + s)\sin 2y\vartheta$. Its height above the apex of the corner of the base x is then*

$$c' = c - \ell\sin 2y\vartheta + \ell\sin 2x\vartheta = c - \sqrt{3}\,\ell\sin(2w\vartheta), \qquad w = \begin{cases} y-\mu & \textit{(side 1)},\\ y+\mu & \textit{(side 2)}, \end{cases}$$

and $|w| < 2\mu$. This w is the passage *of the crossing.*

(b) *It then leaves the star through the right base y' with $y' \equiv x \pmod p$ if $c' > 0$ and $y' \equiv x - N \pmod p$ if $c' < 0$, where x is read as the number $y + 4\mu$ or $y + 8\mu$ in $(3\mu, 9\mu)$; y' is the unique such index with c' in its window, and its height is still c'.*

A closed leaf with passages $w_1, \dots, w_n$ (one for each crossing of a triangle, in order) has length $\sqrt{3}\,\ell\sum_i \cos(2w_i\vartheta)$, and $\sum_i \sin(2w_i\vartheta) = 0$.

Proof. (a) In the frame of the corner of the base y, with its apex at the origin, the center of the triangle E glued to the base is at $\ell e^{2iy\vartheta}$, and the vertex of E opposite the base at $(\ell + s)e^{2iy\vartheta}$. The sides of E other than the base y are glued to the corners whose bases have outward normals $2y\vartheta + 2\pi/3$ and $2y\vartheta + 4\pi/3$, that is to the bases $y + 4\mu$ and $y + 8\mu$, as $2 \cdot 4\mu\vartheta = 2\pi/3$. Let P and P' be the lower and upper ends of the base y. The leaf enters E between P and P'; if it passes below the opposite vertex V it leaves E through the side PV, and otherwise through $P'V$. The side PV has outward normal (for E) of angle $2y\vartheta - \pi/3$, so the corner glued to it has outward normal $2y\vartheta + 2\pi/3$: it is the base $y + 4\mu$. This proves the rule. The gluings are translations, so the leaf keeps its height in the plane; the center of E is at height $\ell\sin 2y\vartheta$ above the first apex and $\ell\sin 2x\vartheta$ above the second, which gives c'. For side 1, $\sin 2x\vartheta - \sin 2y\vartheta = \sin(2y\vartheta + \frac{2\pi}{3}) - \sin 2y\vartheta = -\sqrt{3}\sin(2y\vartheta - \frac{\pi}{6})$, and for side 2, $\sin(2y\vartheta - \frac{2\pi}{3}) - \sin 2y\vartheta = -\sqrt{3}\sin(2y\vartheta + \frac{\pi}{6})$; as $2\mu\vartheta = \pi/6$ this is $-\sqrt{3}\sin 2w\vartheta$ in both cases. A leaf running to the right enters the corner x through its base only if that base faces left, $\cos 2x\vartheta < 0$: for side 1 this means $2y\vartheta \in (-\pi/6, 5\pi/6)$, which with $|y| < 3\mu$ gives $-\mu < y < 3\mu$ and $|w| < 2\mu$; for side 2 it means $2y\vartheta \in (-5\pi/6, \pi/6)$, so $-3\mu < y < \mu$ and again $|w| < 2\mu$.

(b) Develop the corners around the apex of Q_x in the plane, starting from Q_x. The leaf runs to the right at the height c', which is not 0 as it meets no point over A. If $c' > 0$, the direction of its point seen from the apex decreases from about π towards 0, so the leaf meets the corners in the order $Q_x, Q_{x-p}, Q_{x-2p}, \dots$, whose bases have normals $2x\vartheta, 2x\vartheta - 2\alpha, \dots$ (as real numbers, starting in $(\pi/2, 3\pi/2)$). The leaf passes from each corner to the next across their common leg, until it leaves a corner through its base; it does so after finitely

many corners, because the developed corners lie in the disc of radius $\sqrt{3}/2$ around the apex while the leaf moves to the right at unit speed. Each corner is convex, and a leaf running to the right leaves a convex region through a part of the boundary whose outward normal has positive horizontal component; so the base $y' = x - kp$ through which it leaves is a right base. Its normal $2y'\vartheta$ lies within $\alpha < \pi/3$ of a direction in $(0, \pi)$ and has positive cosine, so $2y'\vartheta \in (-\pi/2, \pi/2)$ as a real number. If $c' < 0$ the direction increases from about π towards 2π, the corners met are Q_{x+kp}, and the exit base has normal $2(x + kp)\vartheta \in (3\pi/2, 5\pi/2)$, that is index $y' = x + kp - N$. The point of exit is on the base y' at height c', so c' lies in its window. The window of a right base y' is an interval of length $\sqrt{3}\cos(2y'\vartheta)\sin\alpha > 0$, and the windows of y' and $y' + p$ have a common end, the second lying above the first; so the windows of the right bases in one class modulo p are disjoint, and y' is determined by c'.

For the length, let ξ be the horizontal coordinate of the point of the leaf relative to the apex of its current corner. It grows at unit speed along the leaf, is continuous in the star (all corners around one apex are developed with the apex fixed), and at the crossing of a triangle from the base y to the base x it changes by $\ell\cos 2x\vartheta - \ell\cos 2y\vartheta$, the difference of the horizontal coordinates of the center in the two frames. Around a closed leaf the total change of ξ is 0, so the length is $\ell\sum_i(\cos 2y_i\vartheta - \cos 2x_i\vartheta)$. For side 1, $\cos 2y\vartheta - \cos(2y\vartheta + \frac{2\pi}{3}) = \sqrt{3}\cos(2y\vartheta - \frac{\pi}{6})$, and for side 2, $\cos 2y\vartheta - \cos(2y\vartheta - \frac{2\pi}{3}) = \sqrt{3}\cos(2y\vartheta + \frac{\pi}{6})$; both are $\sqrt{3}\cos 2w\vartheta$. The same argument for the vertical coordinate gives $\sum_i(c_i' - c_i) = 0$, that is $\sum_i \sin 2w_i\vartheta = 0$. □

Along a fixed sequence of crossings every condition in Lemma 7.3 is an inequality between the first height c_0 and a number that does not depend on c_0, as the heights change by translations. Hence a closed leaf that meets no point over A or C lies in a cylinder, the leaves of the cylinder are the leaves with the same sequence of crossings, and its height is the length of the open interval of their first heights c_0. The *exponents* of a crossing with passage w are

$$e = w \ \text{ (direction } AB), \qquad e = w - \tfrac{1}{2} \ \text{ (direction } AC);$$

in both cases e is an integer in the *window of exponents* $\mathcal{X} = \{-2\mu, -2\mu+1, \dots, 2\mu-1\}$, as $|w| < 2\mu$ and w is an integer for AB and a half-integer for AC. For a cylinder Y' of one of the two directions with exponents $e_1, \dots, e_n$ we put

$$\Sigma_{Y'} = \sum_{i=1}^{n} \zeta^{e_i} \in \mathbb{Q}(\zeta).$$

By Lemma 7.3, $\sum_i \zeta^{w_i}$ is real and is the circumference of Y' divided by $\sqrt{3}\ell$; and $\Sigma_{Y'} = \sum_i \zeta^{w_i}$ for AB, $\Sigma_{Y'} = \zeta^{-1/2}\sum_i \zeta^{w_i}$ for AC. So for two cylinders Y, Y' of one direction, $\Sigma_{Y'}/\Sigma_Y$ is the ratio of their circumferences, a positive real number.

7.2. **What one cylinder forces.** The cylinders of one direction θ and the classes $I_{Y'}$ are those of Section 2.6. For cylinders Y, Y' of the direction of AB or of AC we put $t_{Y'} = \Sigma_{Y'}/\Sigma_Y = c_{Y'}/c_Y$.

Lemma 7.4. *Let Y be a cylinder of the direction of AB or AC and $\mathcal{E}$ its $\mathcal{M}$-parallel class. If $H_{12} \subset S$ and some unit is not in S, then $t_{Y'} \in \mathbb{Q}(\sqrt{3})$ for every $Y' \in \mathcal{E}$, and $\sum_{Y'\in\mathcal{E}} h_{Y'}\,\bar{t}_{Y'} = 0$, where $\bar{t}$ is the conjugate of t in $\mathbb{Q}(\sqrt{3})$. In particular some $Y' \in \mathcal{E}$ has $\bar{t}_{Y'} < 0$.*

Proof. By Lemma 2.6, $S \cap G$ is a subgroup of G; it contains H_{12}, which has index 2 in G as $G/H_{12} \cong (\mathbb{Z}/12)^\times/\{\pm 1\}$, and it is not G; so $S \cap G = H_{12}$. The automorphisms σ_v, $v \in H_{12}$, are those that fix $\zeta^\mu + \zeta^{-\mu} = 2\cos(\pi/6) = \sqrt{3}$, so their fixed field is $\mathbb{Q}(\sqrt{3})$, and

$t_{Y'} \in \mathbb{Q}(\sqrt{3})$ by Lemma 2.16(f1) with $A_0 = S$. Let $v \equiv 5 \pmod{12}$ be a unit; then $v \notin S$ and $\sigma_v(\sqrt{3}) = 2\cos(5\pi/6) = -\sqrt{3}$, so Lemma 2.16(f2) gives $\sum_{Y' \in \mathcal{E}} h_{Y'} \bar{t}_{Y'} = 0$. As $t_Y = 1$ and all $h_{Y'} > 0$, some $\bar{t}_{Y'}$ is negative. □

Definition 7.5. Let Y be a cylinder of the direction of AB or AC, with exponents $e_1, \dots, e_n \in \mathcal{X}$. We say that Y *passes* if there are no function $m\colon \mathcal{X} \to \mathbb{Z}_{\geq 0}$ and rational numbers a, b with $b > 0$, $|a| < b\sqrt{3}$ and

$$\sum_{x \in \mathcal{X}} m(x)\, \zeta^x = (a + b\sqrt{3})\, \Sigma_Y.$$

Whether Y passes depends only on its list of exponents.

Proposition 7.6. *Suppose that $H_{12} \subset S$ and that some cylinder of the direction of AB or of AC passes. Then every unit lies in S.*

Proof. If not, Lemma 7.4 gives a cylinder Y' of the same direction with $t_{Y'} = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$, $t_{Y'} > 0 > \bar{t}_{Y'} = a - b\sqrt{3}$; so $b > 0$ and $|a| < b\sqrt{3}$. The function $m(x) = \#\{i :\ e_i(Y') = x\}$ on $\mathcal{X}$ has $\sum_x m(x)\zeta^x = \Sigma_{Y'} = t_{Y'}\Sigma_Y$, so Y does not pass. □

Two ways to show that a cylinder passes are used below.

Proposition 7.7. *Let Y have exponents $e_1, \dots, e_n$. Suppose there is a $\mathbb{Q}$-linear map $\phi\colon \mathbb{Q}(\zeta) \to \mathbb{R}$ such that $f(x) = \phi(\zeta^x) \geq 0$ for every $x \in \mathcal{X}$ and, with*

$$\alpha_\phi = \sum_{j=1}^{n} f(e_j), \qquad \beta_\phi = \sum_{j=1}^{n} \bigl(f(e_j + \mu) + f(e_j - \mu)\bigr),$$

$\beta_\phi < -\sqrt{3}\,\alpha_\phi$. Then Y passes.

Proof. Since $\zeta^\mu + \zeta^{-\mu} = \sqrt{3}$, $\phi(\Sigma_Y) = \alpha_\phi \geq 0$ and $\phi(\sqrt{3}\,\Sigma_Y) = \beta_\phi$. If m, a, b are as in Definition 7.5, then, ϕ being $\mathbb{Q}$-linear and m, a, b rational,

$$0 \leq \sum_x m(x) f(x) = \phi((a + b\sqrt{3})\Sigma_Y) = a\,\alpha_\phi + b\,\beta_\phi < a\,\alpha_\phi - b\sqrt{3}\,\alpha_\phi = (a - b\sqrt{3})\,\alpha_\phi \leq 0,$$

using $b > 0$ for the strict inequality and $a < b\sqrt{3}$, $\alpha_\phi \geq 0$ for the last one. This is a contradiction. □

When $N = 12 \cdot 2^a 3^b$, the N-th cyclotomic polynomial is $X^{4\mu} - X^{2\mu} + 1$, of degree 4μ, so the numbers ζ^x, $x \in \mathcal{X}$, are a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta)$, and

$$\zeta^{r+2\mu} = \zeta^r - \zeta^{r-2\mu}, \qquad \zeta^{r-3\mu} = \zeta^{r-\mu} - \zeta^{r+\mu}. \tag{7.2}$$

For $0 \leq r < \mu$ the window $\mathcal{X}$ is the disjoint union of the blocks $\{r - 2\mu, r - \mu, r, r + \mu\}$.

Proposition 7.8. *Let $N = 12 \cdot 2^a 3^b$, and for $0 \leq r < \mu$ and $k \in \{-2, -1, 0, 1\}$ let $n_k = n_k(r)$ be the number of j with $e_j = r + k\mu$. If for some r*

$$n_1 - n_{-1} > \sqrt{3}\, n_{-2} \qquad \text{or} \qquad n_{-2} - n_0 > \sqrt{3}\, n_1,$$

then Y passes.

Proof. By $\sqrt{3}\,\zeta^x = \zeta^{x+\mu} + \zeta^{x-\mu}$ and (7.2), the coordinates of $(a + b\sqrt{3})\Sigma_Y$ at $r - 2\mu, r - \mu, r, r + \mu$ are

$$a\,n_{-2} - b(n_1 - n_{-1}), \quad a\,n_{-1} + b(n_0 + 2n_{-2}), \quad a\,n_0 + b(2n_1 + n_{-1}), \quad a\,n_1 + b(n_0 - n_{-2}).$$

Indeed $\sqrt{3}\zeta^{r-2\mu} = \zeta^{r-\mu} + \zeta^{r-3\mu} = 2\zeta^{r-\mu} - \zeta^{r+\mu}$, $\sqrt{3}\zeta^{r-\mu} = \zeta^r + \zeta^{r-2\mu}$, $\sqrt{3}\zeta^r = \zeta^{r+\mu} + \zeta^{r-\mu}$ and $\sqrt{3}\zeta^{r+\mu} = \zeta^{r+2\mu} + \zeta^r = 2\zeta^r - \zeta^{r-2\mu}$. If $n_1 - n_{-1} > \sqrt{3}n_{-2}$, $b > 0$ and $a < b\sqrt{3}$, the

first coordinate is less than $(a-b\sqrt{3})n_{-2} \le 0$; if $n_{-2}-n_0 > \sqrt{3}n_1$, the last one is less than $(a-b\sqrt{3})n_1 \le 0$. Since the ζ^x, $x \in \mathcal{X}$, are a basis, no $m \ge 0$ has $\sum m(x)\zeta^x = (a+b\sqrt{3})\Sigma_Y$. □

We say that Y *passes the block test* when the hypothesis of Proposition 7.8 holds.

When a prime $q \ge 5$ divides N, the numbers ζ^x, $x \in \mathcal{X}$, are not linearly independent over $\mathbb{Q}$, and Proposition 7.8 is not available. One test serves every N. Let $\mathfrak{d}$ be the product of the primes $q \ge 5$ that divide N ($\mathfrak{d} = 1$ is allowed) and $\mathfrak{s} = N/(6\mathfrak{d})$. As $\mathfrak{d}$ is prime to 6, $\mathfrak{d} \mid \mu$; so $2\mu = \mathfrak{d}\mathfrak{s}$, $\mathfrak{s}$ is even, and p is prime to $\mathfrak{d}$ and to $\mathfrak{s}$.

Proposition 7.9. *Let Y be a cylinder of the direction of AC with exponents $x_1, \dots, x_n$, and let E be an integer with $\mu \le E \le 2\mu - 1$. Let n_1, n_0, n_{-1}, n_{-2} be the numbers of j with $x_j = E$, $E-\mu$, $E-2\mu$, $E-3\mu$ respectively, and let $\mathcal{R}$ be the set of the residues modulo $\mathfrak{d}$ of the integers $r_j = 2(x_j - E)/\mathfrak{s}$, over the j with $\mathfrak{s} \mid 2(x_j - E)$ and $\mathfrak{d} \nmid r_j$. If*

$$n_1 - n_{-1} > \sqrt{3}\, n_{-2} \qquad \text{and} \qquad \sum_{r \in \mathcal{R}} \prod_{q \mid \mathfrak{d},\ q \nmid r} \frac{2}{q-1} < 1,$$

then Y passes. The same holds with the list $(-1-x_j)_j$ in place of $(x_j)_j$.

We then say that the list *passes the test at E*. The proof, in §S5 of the supplement, applies Proposition 7.7 with an explicit function supported on the residue class of $E+\mu$ modulo $\mathfrak{s}$, multiplied at each prime $q \mid \mathfrak{d}$ by a measure on $\mathbb{Z}/q$ supported on three points; when the sum in the hypothesis is less than 1, a count shows that these measures can be chosen so that the exponents not counted by the n_k contribute nothing. For a cylinder of the direction of AB, whose exponents lie in $\mathcal{X} \setminus \{-2\mu\}$, the supplement proves the same with $(-x_j)_j$ in place of $(-1-x_j)_j$, for the reading of Definition 7.5 with $\mathcal{X} \setminus \{-2\mu\}$ in place of $\mathcal{X}$; Proposition 7.6 holds with that reading, by its proof.

If $\mathfrak{d} = 1$, then $\mathcal{R} = \emptyset$, and for the direction of AC the test is the block test: with $r = E - \mu$ the numbers n_k are the $n_k(r)$ of Proposition 7.8, and $x \mapsto -1-x$ maps the block $\{r-2\mu, r-\mu, r, r+\mu\}$ onto the block of $\mu-1-r$, in the reverse order, so that the test for $(-1-x_j)_j$ at $2\mu-1-r$ is the inequality $n_{-2}-n_0 > \sqrt{3}\,n_1$ at r. If $x_j - E \equiv J_j p \pmod{2\mu}$ with an integer J_j, then, as $\mathfrak{s} \mid 4\mu$ and p is prime to $\mathfrak{s}$ and $\mathfrak{d}$, $\mathfrak{s} \mid 2(x_j - E)$ if and only if $\mathfrak{s} \mid 2J_j$, and then $r_j \equiv (2J_j/\mathfrak{s})\, p \pmod{\mathfrak{d}}$, so that a prime $q \mid \mathfrak{d}$ divides r_j if and only if it divides $2J_j/\mathfrak{s}$.

7.3. **The units congruent to ±1 modulo 12.** In this subsection $S' \subset F$ is a closed set containing 1 (Section 1.1) and $H = S' \cap G$, a subgroup of G containing -1 (Lemma 2.6). Every element of F is prime to 6 (proof of Proposition 2.8).

Relabel the vertices if needed so that the numerator at the first vertex is a unit: put $\tilde{p} = p$ if $3 \nmid p$ and $\tilde{p} = 8\mu - p$ if $3 \mid p$. Then $\Delta = (\tilde{p}, 4\mu, 8\mu - \tilde{p})/N$ up to the order of the numerators, $0 < \tilde{p} < 8\mu$, and $\tilde{p}$ is a unit: it is odd, prime to 3 (if $3 \mid p$ then $3 \nmid 4\mu$, so $3 \nmid 8\mu - p$), and $\gcd(\tilde{p}, 4\mu) = \gcd(p, 4\mu) = 1$. The set S does not depend on the labeling, so we may work with $\tilde{p}$. Let

$$\Omega = \max(\tilde{p},\, 2\mu - \tilde{p}) \ \text{ if } \tilde{p} < 4\mu, \qquad \Omega = \max(8\mu - \tilde{p},\, \tilde{p} - 6\mu) \ \text{ if } \tilde{p} > 4\mu.$$

Then $\Omega > \mu$: $\Omega \ge \mu$, with equality only if $\tilde{p} \in \{\mu, 7\mu\}$, which is excluded as $\gcd(\tilde{p}, 4\mu) = 1$ and $\mu > 1$ for $N > 12$.

Lemma 7.10. *Let P be an integer with $P \equiv \tilde{p} \pmod 3$ and $a = P\tilde{p}^{-1} \bmod N$. Then a is holomorphic if and only if $0 < [P] < 8\mu$.*

Proof. This is Lemma 2.17(b) with $p_i = \tilde{p}$, $p_k = N/3$ and $y = P$, as $2N/3 = 8\mu$. □

Lemma 7.11. *Let $s \equiv 0 \pmod 6$ with $0 < |s| < \Omega$ and $\gcd(\tilde{p}+s, N) = 1$. Then $e_s = (\tilde{p}-s)/(\tilde{p}+s) \bmod N$ lies in S'. If $\tilde{p}-s$ is a unit, then $e_s \in H$ and $e_s \equiv 1 \pmod{12}$. If $d = \gcd(\tilde{p}-s, N) > 1$, then d is prime to 6 and $K_{N/d} \subset H$; in particular $K_{N/q} \subset H$ for every prime $q \mid d$.*

Proof. Choose (c, r) among $(\tilde{p}, \tilde{p})$ if $\tilde{p} < 4\mu$; $(\tilde{p}+6\mu, 2\mu-\tilde{p})$ if $\tilde{p} < 2\mu$; $(\tilde{p}, 8\mu-\tilde{p})$ if $\tilde{p} > 4\mu$; $(\tilde{p}-6\mu, \tilde{p}-6\mu)$ if $\tilde{p} > 6\mu$, so that $r = \Omega$. In each case $c \equiv \tilde{p} \pmod{N/2}$ and the interval $(c-r, c+r)$ is $(0, 2\tilde{p})$, $(4\mu+2\tilde{p}, 8\mu)$, $(2\tilde{p}-8\mu, 8\mu)$ or $(0, 2\tilde{p}-12\mu)$, contained in $(0, 8\mu)$. Put $P = c+s$ and $P' = c-s$; both lie in $(0, 8\mu)$ and are $\equiv \tilde{p} \pmod 6$, as $6 \mid N/2$. They are odd and congruent modulo $N/2$ to $\tilde{p}+s$ and $\tilde{p}-s$, and every odd prime power dividing N divides $N/2$; so $\gcd(P, N) = 1$ and $\gcd(P', N) = \gcd(\tilde{p}-s, N)$. By Lemma 7.10, $x = P/\tilde{p}$ is a holomorphic unit and $b = P'/\tilde{p}$ is holomorphic; and $x + b = 2c/\tilde{p} \equiv 2 \pmod N$, so $b = 1 - x - (-1)$. Rule (iii) with the unit $u = x$ (note $x = x \cdot 1 \in xS'$) and $a' = -1 \in S'$ gives $b \in xS'$, that is $P'/P \in S'$. Finally $P'/P \equiv (\tilde{p}-s)/(\tilde{p}+s)$, because $(c-s)(\tilde{p}+s) - (\tilde{p}-s)(c+s) = 2s(c-\tilde{p}) \equiv 0 \pmod N$. If $\tilde{p}-s$ is a unit, e_s is a unit, and $e_s \equiv 1$ modulo 3 and modulo 4, as $\tilde{p}-s \equiv \tilde{p}+s$ modulo 3 and modulo 4. If $d > 1$, d is prime to 6 as $\tilde{p}-s$ is; for $u \in K_{N/d}$, $(u-1)e_s \equiv 0 \pmod N$, so $e_s \in S' \cap uS'$, hence $uS' = S'$ by (ii) and $u = u \cdot 1 \in H$. □

Proposition 7.12. *Each of the following implies $H_{12} \subset H$; in each case, therefore, $H_{12} \subset S$.*

(a) *Setting (I), $N \geq 72$.*
(b) *Setting (II), $p \geq 9$.*
(c) *Setting (III) or (IV), $N \geq 60$.*

The last assertion follows from the first as S is closed and contains 1 (Section 2.1). Parts (a) and (b) are proved now; part (c) after Lemma 7.16.

Proof of (a) and (b). (a) Here $\tilde{p} = p$ and $N = 2^{a+2}3^{b+1}$. Take $s = 6$: $\Omega > \mu \geq 6$ as $N \geq 72$, and $p \pm 6$ are odd and prime to 3, so units. By Lemma 7.11, $v = (p-6)/(p+6)$ lies in H, and $v \equiv 1 \pmod{12}$. Moreover $v = 1 - 12/(p+6)$, so $v \equiv 5 \pmod 8$ and $v \not\equiv 1 \pmod 9$. The units $\equiv 1 \pmod{12}$ form, by the Chinese remainder theorem, the product of the units $\equiv 1 \pmod 4$ modulo 2^{a+2}, a cyclic group of order 2^a generated by any element $\equiv 5 \pmod 8$, and the units $\equiv 1 \pmod 3$ modulo 3^{b+1}, a cyclic group of order 3^b generated by any element $\not\equiv 1 \pmod 9$. So v generates them, and with $-1 \in H$ we get $H_{12} \subset H$.

(b) Here $N = 12 \cdot 2^a$, $p = 3p'$ with $p' \geq 3$ odd, and $p < 4\mu$, so $4\mu \geq 16$. Let x be the unit with $x \equiv 1 \pmod 3$ and $x \equiv (p'+2)/p' \pmod{4\mu}$ (p' is odd and 4μ a power of 2). Then $[x \cdot 4\mu] = 4\mu$, and $xp' \equiv p'+2 \pmod{4\mu}$ gives $[xp] = 3(p'+2) = p+6 < 8\mu$, so $[x(8\mu-p)] = 8\mu - p - 6$; the sum is N, and x is holomorphic. Likewise $2 - x \equiv 1 \pmod 3$ and $(2-x)p' \equiv p' - 2 \pmod{4\mu}$, which is odd, so $2-x$ is a unit, and its residues are $p - 6 \in (0, 8\mu)$, 4μ and $8\mu - p + 6$, with sum N: $2 - x$ is holomorphic. Rule (iii) with $u = x$ and $a' = -1$ gives $2 - x \in xS'$, so $v = (2-x)/x \in H$. Now $v \equiv 1 \pmod 3$ and $v \equiv (p'-2)/(p'+2) = 1 - 4/(p'+2) \pmod{4\mu}$, and $4/(p'+2) \equiv 4 \pmod 8$, so $v \equiv 5 \pmod 8$. The units $\equiv 1 \pmod{12}$ modulo N form a cyclic group of order 2^a generated by any element $\equiv 5 \pmod 8$ that is $\equiv 1 \pmod 3$; so they lie in H, and with -1, $H_{12} \subset H$. □

For part (c) let some prime $q \geq 5$ divide N; then $\tilde{p}$ is a unit in both settings (III) and (IV). The first step finds a non-unit in S', the second spreads it.

Lemma 7.13. *Let $q \geq 5$ be a prime dividing N with $K_{N/q} \subset H$. Then $H_{12} \subset H$.*

Proof. Put $M = N/q$, so $12 \mid M$ and $8\mu = 2qM/3 > 3M$.

(1) Let $z, w \in [1, 8\mu)$ be prime to N, with $z \equiv w \equiv \tilde{p} \pmod 3$, $z + w \equiv 2\tilde{p} \pmod M$, and $\tilde{p} - z - w$ prime to N. By Lemma 7.10, $x = z/\tilde{p}$ and $b = w/\tilde{p}$ are holomorphic units, and $a' = 1 - x - b = (\tilde{p} - z - w)/\tilde{p}$ is a unit $\equiv -1 \pmod M$, so $a' \in -K_M \subset H \subset S'$. Rule (iii) with $u = x$ gives $b \in xS'$, so $w/z \in H$.

(2) Let $\bar{z}, \bar{w}$ be units modulo M with $\bar{z} \equiv \tilde{p} \pmod 3$ and $\bar{z} + \bar{w} \equiv 2\tilde{p} \pmod M$. Let $z_0, w_0 \in [1, M)$ represent them. The lifts $z_0 + iM$, $w_0 + jM$ $(i, j \in \{0, 1, 2\})$ lie in $[1, 3M) \subset [1, 8\mu)$, are odd and $\equiv \tilde{p} \pmod 3$, and $\tilde{p} - z - w \equiv -\tilde{p} \pmod M$ is a unit modulo M. If $q \mid M$, every lift and every $\tilde{p} - z - w$ is prime to N. If $q \nmid M$, the three lifts of $\bar{z}$ are distinct modulo q; choose one with $q \nmid z$; the three lifts of $\bar{w}$ are distinct modulo q, at most one has $q \mid w$ and at most one has $q \mid \tilde{p} - z - w$, so a third one satisfies (1). Hence H contains an element $\equiv \bar{w}/\bar{z} \pmod M$.

(3) The ratios $\bar{w}/\bar{z}$ of (2) are the numbers $(2 - y)/y$ for the units $y = \bar{z}/\tilde{p}$ modulo M with $y \equiv 1 \pmod 3$ and $2 - y$ a unit. Prime power by prime power: modulo $2^c \parallel M$ $(c \geq 2)$ they run over all of $1 + 4\mathbb{Z}$; modulo $3^c \parallel M$ over all of $1 + 3\mathbb{Z}$; modulo $q'^c \parallel M$ with $q' \geq 5$ over the set $R_{q'}$ of residues $\not\equiv 0, -1 \pmod{q'}$, which has $q'^{c-1}(q' - 2) > \varphi(q'^c)/2$ elements, so that $R_{q'} R_{q'}^{-1}$ is the whole unit group modulo q'^c. By the Chinese remainder theorem the set of ratios is the product of these sets, each of which contains 1, so the group it generates contains every unit modulo M that is $\equiv 1 \pmod{12}$.

(4) For a unit $u \equiv 1 \pmod{12}$ modulo N, (2) and (3) give $h \in H$ with $h \equiv u \pmod M$; then $uh^{-1} \in K_M \subset H$, so $u \in H$. With $-1 \in H$, $H_{12} \subset H$. □

Let $j(n)$ be Jacobsthal's function, as in Section 6.1.

Lemma 7.14. *Let $q \geq 5$ be a prime dividing N, and N_q the product of the primes ≥ 5 of N other than q. If $\lfloor N/(36q) \rfloor \geq j(N_q)$, there is $s \equiv 0 \pmod 6$ with $0 < |s| < \Omega$, $q \mid \tilde{p} - s$ and $\gcd(\tilde{p} + s, N) = 1$; hence $K_{N/q} \subset H$ by Lemma 7.11. Such a q exists unless $N = 12q$ or $N = 24q$ with q prime.*

Proof. The number $n = \tilde{p} - s$ runs over the integers $\equiv \tilde{p} \pmod 6$ of the open interval $(\tilde{p} - \Omega, \tilde{p} + \Omega)$, of length $2\Omega > 2\mu = N/6$, other than $\tilde{p}$. Those divisible by q form an arithmetic progression of difference $6q$, none equal to $\tilde{p}$ (a unit), and the interval contains at least $\lfloor N/(36q) \rfloor$ consecutive terms $n_t = n_1 + 6qt$ of it. For such n, $\tilde{p} + s = 2\tilde{p} - n$ is odd, $\equiv \tilde{p} \pmod 3$ and $\equiv 2\tilde{p} \not\equiv 0 \pmod q$; for a prime $q' \mid N_q$ it is divisible by q' for t in exactly one class modulo q'. By the Chinese remainder theorem there is t^* such that $2\tilde{p} - n_t$ is prime to N_q if and only if $t - t^*$ is, and among $j(N_q)$ consecutive values of t one has this property.

For the second statement write $N = QM$ with $Q = 2^a 3^b \geq 12$ and M prime to 6. If $M = q^e$ is a prime power, $N_q = 1$, $j(1) = 1$, and $N/(36q) = Qq^{e-1}/36 \geq 1$ unless $e = 1$ and $Q \in \{12, 24\}$. Otherwise let q be the least prime ≥ 5 of N and $n = N_q$, a squarefree number with $k \geq 1$ prime factors, all ≥ 7; then $N \geq 12qn$ and $\lfloor N/(36q) \rfloor \geq \lfloor n/3 \rfloor$. If $k = 1$, $j(n) = 2 \leq \lfloor n/3 \rfloor$. If $k \geq 2$, by inclusion and exclusion over the 2^k divisors of n, the number of integers prime to n among J consecutive integers differs from $J\varphi(n)/n$ by less than 2^k; so $j(n) \leq 2^k n/\varphi(n) + 1$. As $n \geq 77$ and $\varphi(n) \geq 6^k$, $\varphi(n)(\frac{1}{3} - \frac{2}{n}) \geq 6^k(\frac{1}{3} - \frac{2}{77}) > 2^k$, which gives $2^k n/\varphi(n) + 1 \leq n/3 - 1 < \lfloor n/3 \rfloor$. □

It remains to treat $N = Qq$ with $Q \in \{12, 24\}$ and $q \geq 5$ prime. There $K_Q = K_{N/q}$, reduction modulo q is an isomorphism from K_Q onto $\mathbb{F}_q^\times$, and we let $W \subset \mathbb{F}_q^\times$ be the image of $H \cap K_Q$ and r' its index.

Lemma 7.15. *Let $h \in H$ and let z, w be integers with $0 < z, w < 8\mu$, $z \equiv w \equiv \tilde{p} \pmod 3$, $z + w \equiv (1+h)\tilde{p} \pmod N$ and $\gcd(z, N) = 1$. Then $w/z \in S'$, and if $d = \gcd(w, N) > 1$ then $K_{N/d} \subset H$.*

Proof. By Lemma 7.10, $x = z/\tilde{p}$ is a holomorphic unit and $b = w/\tilde{p}$ is holomorphic, and $1 - x - b \equiv -h \in S'$. Rule (iii) with $u = x$ and $a' = -h$ gives $b \in xS'$, so $w/z \in S'$; the last statement follows as at the end of the proof of Lemma 7.11. □

Lemma 7.16. *Let $q \equiv 1 \pmod 3$ be prime, $W_3 \subset \mathbb{F}_q^\times$ the subgroup of cubes, and $\delta \in \mathbb{F}_q^\times$. Then $\#\{x \in W_3 : \ x + \delta \in W_3\} \le (q + 4 + 2\sqrt{q})/9$.*

Proof. Let χ be a character of $\mathbb{F}_q^\times$ of order 3, extended by $\chi(0) = 0$. On $\mathbb{F}_q^\times$ the indicator of W_3 is $(1 + \chi + \chi^2)/3$, so the number is $\frac{1}{9}\sum_{i,j\in\{0,1,2\}}\sum_{x\ne 0,-\delta}\chi^i(x)\chi^j(x+\delta)$. The term $(i,j) = (0,0)$ is $q-2$. The four terms with exactly one of i, j zero are $-\chi^i(-\delta)$ and $-\chi^j(\delta)$, of absolute value 1. The terms $(1,2)$ and $(2,1)$ are $\sum_x \chi^{\pm 1}(x/(x+\delta)) = -1$, as $x/(x+\delta)$ runs over $\mathbb{F}_q \setminus \{0,1\}$. The terms $(1,1)$ and $(2,2)$ become, after $x = -\delta y$, $\chi^i(-\delta^2)\sum_y \chi^i(y)\chi^i(1-y) = \chi^i(-\delta^2)J(\chi^i,\chi^i)$, a Jacobi sum with χ^i, χ^i and χ^{2i} all non-trivial, so of absolute value $\sqrt{q}$ [5, Corollary 2.5]. The sum is at most $q-2+4+2+2\sqrt{q}$. □

Proof of Proposition 7.12(c). By Lemma 7.13 it suffices to find a prime $q \ge 5$ of N with $K_{N/q} \subset H$. If N is not $12q$ or $24q$ with q prime, Lemma 7.14 gives one. Let $N = Qq$ with $Q \in \{12, 24\}$, and suppose first that $Q = 24$ and $q \ge 11$, or $Q = 12$ and $q \ge 17$, $q \ne 19$. Let $\varepsilon = \pm 1$ with $\tilde{p} \equiv \varepsilon q \pmod 6$.

(i) $\varepsilon = 1$. Apply Lemma 7.15 with $h = 1$, $w = mq$ and $z \equiv 2\tilde{p} - mq \pmod N$, for $m \in \{1, 7\}$ ($Q = 12$) or $m \in \{1, 7, 13\}$ ($Q = 24$). Then $mq \equiv \tilde{p} \pmod 6$, $0 < mq < 8\mu$, and z is a unit ($\equiv \tilde{p} \pmod 6$ and $\equiv 2\tilde{p} \not\equiv 0 \pmod q$). We need $[z] \in (0, 8\mu)$, that is $[2\tilde{p}] \in (mq, mq + 8\mu)$ modulo N; the intervals $(q, 9q) \cup (7q, 15q)$ modulo $12q$, respectively $(q, 17q) \cup (7q, 23q) \cup (13q, 29q)$ modulo $24q$, cover every even residue. So some m applies, $\gcd(w, N) = q$, and $K_{N/q} \subset H$.

(ii) If W has index $r' \ge 4$, there is a hit. For each integer t with $|t| < q/6$ put $s = (Q/2)t$; then $s \equiv 0 \pmod 6$ and $|s| < Qq/12 = \mu < \Omega$, and $\tilde{p} \pm s$ are odd and prime to 3. If q divides $\tilde{p} - s$ or $\tilde{p} + s$ for one such t (not both, as $q \nmid 2\tilde{p}$), then s or $-s$ satisfies Lemma 7.11 with $q \mid d$, and $K_{N/q} \subset H$. Otherwise all the e_s are units of H, $\equiv 1 \pmod Q$ as $2s \equiv 0 \pmod Q$, and pairwise distinct modulo q ($e_s \equiv e_{s'}$ means $2\tilde{p}(s - s') \equiv 0$, so $q \mid t - t'$, while $|t - t'| < q/3$). So $|W| \ge 2\lfloor q/6 \rfloor + 1 \ge (q-2)/3 > (q-1)/4$ (as $q > 5$), and $r' \le 3$.

(iii) $\varepsilon = -1$. Now $mq \equiv \tilde{p} \pmod 6$ with $0 < mq < 8\mu$ means $m = 5$ ($Q = 12$) or $m \in \{5, 11\}$ ($Q = 24$). For $h \in H \cap K_Q$ with $h \not\equiv -1 \pmod q$ put $c_h = (1+h)\tilde{p} \bmod N$. With $w = mq$ and $z \equiv c_h - mq$, z is a unit ($\equiv \tilde{p} \pmod 6$ as $c_h \equiv 2\tilde{p} \pmod Q$, and $\not\equiv 0 \pmod q$), and Lemma 7.15 gives $K_{N/q} \subset H$ as soon as $[c_h - mq] \in (0, 8\mu)$ for an admissible m, that is $c_h \in (5q, 13q)$ modulo $12q$, respectively $c_h \in (5q, 27q)$ modulo $24q$. So if no such h gives a hit, then $c_h \in [aq, 5q]$ modulo N for every such h, with $a = 1$ ($Q = 12$) or $a = 3$ ($Q = 24$). Write $c_h \equiv 2\tilde{p} + Q\kappa_h \pmod N$ with $\kappa_h \equiv \gamma(h-1) \pmod q$, $\gamma = \tilde{p}/Q \bmod q$; so $h \mapsto \kappa_h$ is injective modulo q, and $c_h \in [aq, 5q]$ modulo N if and only if $\kappa_h \equiv k \pmod q$ for some k in the set B of integers k with $aq \le 2\tilde{p} + Qk \le 5q$ (taking $2\tilde{p} \in [0, N)$), a set of at most $\lfloor (5-a)q/Q \rfloor + 1 \le q$ consecutive integers. Hence $|W \setminus \{-1\}| \le |B|$.

(iv) Combine, when $\varepsilon = -1$ and there is no hit, so that $r' \le 3$ by (ii). If $Q = 24$: $|B| \le \lfloor q/12 \rfloor + 1 < (q-4)/3 \le |W| - 1$ for $q \ge 11$, a contradiction. If $Q = 12$ and $r' \le 2$: $|B| \le \lfloor q/3 \rfloor + 1 < (q-3)/2 \le |W| - 1$ for $q \ge 17$, a contradiction. If $Q = 12$ and $r' = 3$, then $q \equiv 1 \pmod 3$, so $q \ge 31$, and $W = W_3 \ni -1$. The set $X = \{\gamma h : \ h \in W \setminus \{-1\}\}$

lies in a set $\gamma + B$ of at most $(q+2)/3$ consecutive residues, so $|X \cup (X+1)| \le (q+5)/3$ and $|X \cap (X+1)| \ge 2(q-4)/3 - (q+5)/3 = (q-13)/3$. But $X \cap (X+1)$ has at most $\#\{h \in W_3 : \ h + \gamma^{-1} \in W_3\} \le (q+4+2\sqrt{q})/9$ elements by Lemma 7.16; this gives $2q - 2\sqrt{q} - 43 \le 0$, false for $q \ge 29$. So there is a hit, and $K_{N/q} \subset H$.

There remain $N = 60, 84, 132, 156, 228$ ($Q = 12$, $q = 5, 7, 11, 13, 19$) and $N = 120, 168$ ($Q = 24$, $q = 5, 7$). For each of these seven N and each of the 140 triangles $(p, 4\mu, 8\mu - p)/N$ with $1 \le p < 4\mu$ and $\gcd(p, 4\mu) = 1$ we find that the closure of $\{1\}$, which lies in every closed set containing 1, contains H_{12}. □

7.4. **Explicit cylinders of the direction of AC.** In this subsection $g \in \{1, 3\}$ and we work in the direction of AC, so indices of bases and passages are half-integers; we write $\lambda = \sqrt{3}/2 = |CA|$ for short. We use three facts.

(F1) Side 1 at a right base. At a right base y, with $\theta = 2y\vartheta$, the window has length $\sqrt{3}s\cos\theta$, and the leaves that take side 1 are those of its bottom part, of length $\sqrt{3}s\sin(\theta + \pi/6)$ when this lies between 0 and $\sqrt{3}s\cos\theta$. Indeed $\ell + s = \sqrt{3}\sin(\alpha + \pi/6)$ and $(\ell + s)\sin\theta - \lambda\sin(\theta - \alpha) = \sqrt{3}s\sin(\theta + \pi/6)$. So no leaf takes side 1 at $y \le -\mu$, and the whole window takes side 1 at $y \ge \mu$.

(F2) Crossing a vertical leg. The leg shared by the corners of the bases $3\mu - p/2$ and $3\mu + p/2$ has direction $\pi/2$ in the frame of the flow: it is a copy of AC pointing straight up from a point over A. Likewise the leg shared by the bases $-3\mu \mp p/2$ points straight down. By the proof of Lemma 7.3(b), a crossing of the star above the apex that enters by the base x crosses the leg pointing up if and only if $x \equiv 3\mu + p/2 \pmod p$, and a crossing below the apex crosses the leg pointing down if and only if $x - N \equiv -3\mu + p/2 \pmod p$; it crosses it at a right angle.

(F3) A reflection. Each copy of a side of Δ in X is fixed pointwise by the isometry of X that exchanges the two images of Δ adjacent along it; its linear part is the reflection in the direction of that copy. Two isometries of X with the same linear part differ by an automorphism that preserves ω, which is the identity by [19, Theorem 6.2]. So one isometry ρ_0 fixes every vertical copy of a side pointwise. It maps horizontal leaves to horizontal leaves with the direction reversed. If a horizontal leaf crosses vertical copies of sides at right angles at points P_1 and then P_2, then ρ_0 fixes both points and reverses the leaf, so the leaf runs from P_2 back to P_1 along the mirror image of its path from P_1 to P_2: it is closed, and its crossings after P_2 are those before, in reverse order, each passage w replaced by $-w$: the reflection takes the index x of a base to $6\mu - x$ (modulo N), so a crossing that leaves the star by the base y and enters it by the base x, with passage w, becomes the crossing that leaves by $6\mu - x$ and enters by $6\mu - y$, with passage $-w$ and the same side number.

Proposition 7.17. *Let $2\mu < p < 4\mu$. In the direction of AC every leaf that leaves the star through the right base $y_1 = 4\mu - p/2$ is closed after two crossings, by side 1 at y_1 and by side 2 at $-y_1$, with passages $3\mu - p/2$ and $-(3\mu - p/2)$. These leaves form a cylinder $\mathcal{U}$ whose exponents are*

$$E = 3\mu - \tfrac{p+1}{2} \in [\mu, 2\mu - 1] \qquad \text{and} \qquad -E - 1 \in [-2\mu, -\mu - 1].$$

Proof. $2y_1\vartheta = 2\pi/3 - \alpha$, and $|y_1| < 3\mu$ as $p > 2\mu$, so y_1 is a right base. Its window is $(\lambda\sin(2\pi/3 - 2\alpha),\ 3/4)$. The threshold of Lemma 7.3(a) is $(\ell + s)\sin(2\pi/3 - \alpha) = \sqrt{3}\sin(\alpha + \pi/6)\sin(\alpha + \pi/3) = 3/4 + \lambda\sin 2\alpha > 3/4$, so the whole window takes side 1. The entry is $x = 8\mu - p/2 \in (6\mu, 7\mu)$ and the passage $w = y_1 - \mu = 3\mu - p/2$, with $2w\vartheta = \pi/2 - \alpha$; the new height is $c' = c - \sqrt{3}\ell\cos\alpha = c - \lambda\sin(\pi/3 + 2\alpha) - 3/4$. As $\sin(2\pi/3 - 2\alpha) = \sin(\pi/3 + 2\alpha) > 0$, c' runs over $(-3/4, -\lambda\sin(\pi/3 + 2\alpha))$, below the

apex. So the exit is $\equiv x - N \equiv -4\mu - p/2 \pmod p$, and $(-3/4, -\lambda\sin(\pi/3 + 2\alpha))$ is exactly the window of the base $-y_1 = -4\mu + p/2$ of that class. There the threshold is $-(3/4 + \lambda\sin 2\alpha) < c'$, so the leaf takes side 2, enters by $x = 4\mu + p/2$ with passage $-y_1 + \mu = -(3\mu - p/2)$, and its height is back to $c > 0$; the crossing is above the apex, the exit is $\equiv 4\mu + p/2 \equiv y_1 \pmod p$, and c lies in the window of y_1. The exponents are the passages minus $\frac{1}{2}$, and $2\mu < p < 4\mu$ with p odd gives the ranges. □

Lemma 7.18. *Let $\mu \geq 2$ and $2\mu < p < 4\mu$. Then $\mathcal{U}$ passes the test of Proposition 7.9 at $E = 3\mu - \frac{p+1}{2}$.*

Proof. By Proposition 7.17 the exponents of $\mathcal{U}$ are $E \in [\mu, 2\mu-1]$ and $-E-1$. At E: $n_1 = 1$; $n_{-1} = 0$, since $-E-1 = E-2\mu$ would mean $2E = 2\mu-1$; and $n_{-2} = 0$, since $-E-1 = E-3\mu$ would mean $p = 3\mu$, while $\gcd(p, \mu) = 1$ and $\mu \geq 2$. So $n_1 - n_{-1} = 1 > 0 = \sqrt{3}n_{-2}$. The exponent $-E-1$ has $-E-1-E = p-6\mu \equiv 1 \cdot p \pmod{2\mu}$, so $J = 1$, and $\mathfrak{s} \mid 2(x-E)$ if and only if $\mathfrak{s} \mid 2$, that is $\mathfrak{s} = 2$; the exponent E itself has $r = 0$. So $\mathcal{R} = \emptyset$ unless $\mathfrak{s} = 2$ and $\mathfrak{d} > 1$; then $r \equiv p \pmod{\mathfrak{d}}$, $\mathcal{R} = \{p \bmod \mathfrak{d}\}$, and the sum is $\prod_{q\mid\mathfrak{d}} 2/(q-1) \leq \frac{1}{2}$, as every $q \geq 5$ and p is prime to $\mathfrak{d}$. In each case the sum is less than 1. If $\mathfrak{d} = 1$ this is the block test (the remark after Proposition 7.9). □

The top window. The right base $y_0 = 3\mu - p/2$ has $2y_0\vartheta = \pi/2 - \alpha$ and window $(\lambda\cos 2\alpha, \lambda)$, of length $\Psi = \sqrt{3}\sin^2\alpha$. A leaf through it, followed backwards, crosses the leg pointing up at a right angle at the same height. This window is the *top window*; we write the height of a leaf in it as $\lambda\cos 2\alpha + \eta$, $0 < \eta < \Psi$. The threshold $(\ell + s)\cos\alpha = \lambda(\sin(2\alpha + \pi/6) + \frac{1}{2})$ exceeds λ, so the whole top window takes side 1, with passage

$$x_0 = y_0 - \mu = 2\mu - p/2, \qquad 2x_0\vartheta = \pi/3 - \alpha,$$

and new height $\eta - \lambda/2$ (as $\sqrt{3}\ell\sin(\pi/3 - \alpha) = \lambda/2 + \lambda\cos 2\alpha$); it enters the star by $7\mu - p/2$. When $p < 2\mu$ the exponent $E_0 = x_0 - \frac{1}{2} = 2\mu - \frac{p+1}{2}$ lies in $[\mu, 2\mu - 1]$.

The top window when $N \geq 5p^4$. Let $p \geq 5$ and $N \geq 5p^4$; then $p^4\vartheta \leq \pi/5$, so $p^3\vartheta \leq 0.126$, $p^2\vartheta \leq 0.0252$, $p\vartheta \leq 0.00503$, and $2\mu = N/6 > 0.83p^4 > p^2 + p$. Let $\kappa \equiv 4\mu \pmod p$, a residue prime to p, and $k^* = (p-3)/2$. We use two more facts.

(F4) Write a height as $c = \lambda\sin(q\vartheta - \pi/6)$ with $|q\vartheta| < \pi/3$. The window of the base $-\mu + w$ is then exactly $2w - p < q < 2w + p$. If a leaf at q in that window takes side 2 and arrives at q', then

$$\sin(q'\vartheta - \tfrac{\pi}{6}) - \sin((q-4w)\vartheta - \tfrac{\pi}{6}) = 2\sin(2w\vartheta)\left[\cos((q-2w)\vartheta - \tfrac{\pi}{6}) - \cos(p\vartheta - \tfrac{\pi}{6})\right],$$

since $\sin(q'\vartheta - \frac{\pi}{6}) = \sin(q\vartheta - \frac{\pi}{6}) - 2\ell\sin 2w\vartheta$ and $2\ell = 2\cos(p\vartheta - \frac{\pi}{6})$; the bracket is $-2\sin(\frac{(q-2w+p)\vartheta}{2} - \frac{\pi}{6})\sin(\frac{(q-2w-p)\vartheta}{2})$, of absolute value at most $p\vartheta$ when $|q - 2w| \leq p$.

(F5) The excursion. Let $0 < w < 2\mu$, $\theta = 2w\vartheta$, and let a leaf in the side-1 part of the window of the base $-\mu + w$ take side 1. Its passage is $w - 2\mu$, it enters the star by the base $3\mu + w$, and the side-1 part (F1) is carried exactly onto $(\lambda\cos(\theta + \alpha), \lambda\cos(\theta - \alpha))$: the bottom goes to $\lambda\sin(\theta - \alpha - \frac{\pi}{6}) + \sqrt{3}\cos(\frac{\pi}{6} - \alpha)\sin(\frac{\pi}{3} - \theta) = \lambda\cos(\theta + \alpha)$, and the part has length $\sqrt{3}s\sin\theta = \lambda\cos(\theta - \alpha) - \lambda\cos(\theta + \alpha)$. If $\theta + \alpha < \pi/2$ the new height is positive, so the leaf crosses the star above the apex and leaves by a right base $3\mu - v$ with $v \equiv -w \pmod p$ and $v > 0$, whose window $(\lambda\cos((2v+p)\vartheta), \lambda\cos((2v-p)\vartheta))$ contains the height; hence $0 < v < w + p$. If $v < 2\mu$, that base takes side 1 on its whole window (F1), with passage $2\mu - v$, and the height $\lambda\cos\beta$ becomes $\lambda\sin((2v-p)\vartheta - \frac{\pi}{6}) + \lambda[\cos\beta - \cos((2v+p)\vartheta)]$, where $0 < \cos\beta - \cos((2v+p)\vartheta) < 2\sin(2v\vartheta)\sin(p\vartheta)$.

A *state* is a triple (k, Q, ε) with $0 \le k \le k^*$, Q an even integer and $|\varepsilon| < 1$; it means that the leaf, coming from a crossing of the star below the apex, is about to leave the star by a base $-\mu + w$ with $2w \equiv p - 2(k+1)\kappa \pmod{2p}$, at the height $\lambda \sin(q\vartheta - \pi/6)$, $q = Q + \varepsilon$. Put $D \in \{0, \dots, p-1\}$, $D \equiv Q/2 + (k+1)\kappa \pmod{p}$; the windows of that class of bases are the intervals $(Q - 2D + 2pj,\ Q - 2D + 2p(j+1))$ of q.

Proposition 7.19. *Let $p \ge 5$, $N \ge 5p^4$, and let a leaf of the top window, $0 < \eta < \Psi$, meet no point over A or C. Then:*

(a) *it leaves by y_0 with passage $x_0 = 2\mu - p/2$ and reaches the state $(0, 0, \varepsilon_0)$ with $0 < \varepsilon_0 < 0.06$;*

(b) *for $k = 0, 1, \dots, k^*$ it goes from a state (k, Q_k, ε_k) to a state $(k+1, Q_{k+1}, \varepsilon_{k+1})$ (for $k = k^*$, to the crossing of (c)), with $D_k \equiv \kappa(k+1)^2 \pmod{p}$, $|Q_k| \le 2kp$ and $|\varepsilon_k| < 0.68$, in exactly one of three ways:*

- *(N) $D_k \ge 1$, or $D_k = 0$ and ε_k is above the side-1 part of its window: side 2 at the base $-\mu + w_k$, $2w_k = Q_k + p - 2D_k$, one passage w_k, and $Q_{k+1} = Q_k - 4w_k$;*
- *(B) $D_k = 0$ and $\varepsilon_k < 0$: side 2 at the base $-\mu + w_k - p$, $2w_k = Q_k + p$, one passage $w_k - p$, and $Q_{k+1} = Q_k - 4(w_k - p)$;*
- *(X) $D_k = 0$, $Q_k + p > 0$, and ε_k inside the side-1 part of the window of $-\mu + w_k$, $2w_k = Q_k + p$: an excursion (F5) with two passages $w_k - 2\mu$ and $2\mu - v_k$, where $v_k \equiv -w_k \pmod{p}$ and $0 < v_k < w_k + p$; then $Q_{k+1} = 2v_k - p$ and $0 < \varepsilon_{k+1} < 0.30$.*

$D_k = 0$ happens if and only if $p \mid (k+1)^2$.

(c) *The crossing of the star after step k^* meets the leg pointing down at a right angle, so the leaf is closed, with $p + 1 + 2e$ crossings, e being the number of excursions in (b); its passages are x_0, the passages of the steps $0, \dots, k^*$, their negatives in reverse order, and $-x_0$.*

(d) *Every passage of a step (N) or (B) is a half-integer w with $|w| \le (2k+1)p/2 < p^2/2$ and $w \not\equiv p/2 \pmod{p}$; every passage of an excursion is $w_k - 2\mu \in (-2\mu, -2\mu + p^2/2)$ or $2\mu - v_k \in (2\mu - p^2/2, 2\mu)$, with $w_k, v_k \not\equiv p/2 \pmod{p}$.*

Proof. All q that occur below satisfy $|q| \le p^2 + 1$, so $|q\vartheta| \le 0.0262$ and $\cos(q\vartheta - \pi/6) \ge 0.85$; by the mean value theorem, for two such heights

$$|q - q'| \le |\sin(q\vartheta - \tfrac{\pi}{6}) - \sin(q'\vartheta - \tfrac{\pi}{6})|/(0.85\,\vartheta). \tag{MV}$$

(a) The whole top window takes side 1 at y_0, and the height becomes $c_0 = \eta - \lambda/2 = \lambda \sin(\varepsilon_0\vartheta - \pi/6)$ with $\varepsilon_0 > 0$; from $\lambda\frac{\sqrt3}{2}\sin\varepsilon_0\vartheta \le \lambda(\sin(\varepsilon_0\vartheta - \frac{\pi}{6}) + \frac12) = \eta < \sqrt3 \sin^2\alpha$ we get $\sin\varepsilon_0\vartheta < \frac{4}{\sqrt3}p^2\vartheta^2$, so $\varepsilon_0 < 2.32p^2\vartheta < 0.06$. The entry is $7\mu - p/2$ and $c_0 < 0$, so the next base is $\equiv -5\mu - p/2 \pmod{p}$, that is $-\mu + w$ with $2w \equiv -8\mu - p \equiv p - 2\kappa \pmod{2p}$: this is the state $(0, 0, \varepsilon_0)$, with $D_0 \equiv \kappa$.

(b) Let the leaf be in a state (k, Q, ε) with $|Q| \le 2kp$, $|\varepsilon| < 0.68$ and $D \equiv \kappa(k+1)^2$; $q = Q + \varepsilon$. If $D \ge 1$: $q - (Q - 2D) = 2D + \varepsilon \in (1.32,\ 2p - 1.32)$, so the base is $-\mu + w$ with $2w = Q + p - 2D$, and the leaf is more than 1.32 above the bottom of its window; $|w| \le (|Q| + p)/2 \le (2k+1)p/2 \le (p-2)p/2$. The side-1 part of that window is empty if $w < 0$, and otherwise has length $\sqrt3 s \sin 2w\vartheta \le 2\sqrt3 pw\vartheta^2$ in c, so by (MV) at most $4.71\,pw\vartheta \le 2.36p^3\vartheta \le 0.2966$ in q. So the leaf takes side 2: type (N). If $D = 0$ and $\varepsilon < 0$: q lies in the window just below the common end Q, that of $-\mu + w - p$ with $2w = Q + p$, within 0.68 of its top; the side-1 part of that window is at its bottom and at most 0.30 long, and the window has length $2p \ge 10$: side 2, type (B), and $|w - p| = |Q - p|/2 \le (2k+1)p/2$.

If $D = 0$ and $\varepsilon > 0$: q lies in the window of $-\mu + w$, $2w = Q + p$, at ε above its bottom. Either it is above the side-1 part (always so if $w < 0$): side 2, type (N); or it is inside it: side 1, type (X), and $w > 0$. ($\varepsilon = 0$, or ε at the top of the side-1 part, is a leaf through a singular point.)

Side 2, from the base $-\mu + w'$ ($w' = w$ or $w - p$). By (F4) with $|q - 2w'| < p$, the difference $\sin(q'\vartheta - \frac{\pi}{6}) - \sin((q - 4w')\vartheta - \frac{\pi}{6})$ has absolute value at most $4|w'|p\vartheta^2$, so by (MV) $q' = q - 4w' + \theta$ with $|\theta| \le 4.71|w'|p\vartheta$ (and $|q - 4w'| \le |Q| + 2p + 0.68 \le p^2$). The new height is negative, the entry is $7\mu + w'$, and the next base is $\equiv -5\mu + w'$, the class $2w'' \equiv 2w' - 2\kappa \equiv p - 2(k+2)\kappa$. Put $Q^+ = Q - 4w'$ (even, as $2w'$ is odd) and $\varepsilon^+ = \varepsilon + \theta$. Then $|Q^+| \le |Q| + 2p$, since $Q^+ = -Q - 2p + 4D$ in (N) and $-Q + 2p$ in (B), and, using $Q/2 \equiv D - (k+1)\kappa$,

$$D^+ \equiv Q^+/2 + (k+2)\kappa \equiv -Q/2 + 2D + (k+2)\kappa \equiv D + (2k+3)\kappa \equiv \kappa(k+2)^2 \pmod p.$$

Side 1, type (X), from $-\mu + w$ with $2w = Q + p > 0$. (F5) applies, as $\theta + \alpha \le p^2\vartheta + p\vartheta < \pi/2$ and $w + p \le (2k+1)p/2 + p \le p^2/2 < 2\mu$: the passages are $w - 2\mu$ and $2\mu - v$ with $v \equiv -w \pmod p$, $0 < v < w + p \le p^2/2$, and the new height is $\lambda \sin(q''\vartheta - \frac{\pi}{6})$ with $0 < \sin(q''\vartheta - \frac{\pi}{6}) - \sin((2v - p)\vartheta - \frac{\pi}{6}) < 2\sin(2v\vartheta)\sin(p\vartheta) \le 4vp\vartheta^2$; by (MV), $q'' = 2v - p + \delta$ with $0 < \delta < 4.71\, vp\vartheta \le 2.36p^3\vartheta \le 0.2966$. The height is negative, the entry is $7\mu - v$, and the next base is $\equiv -5\mu - v \equiv -5\mu + w$, the same class as after a side-2 passage w. Put $Q^+ = 2v - p$ (even) and $\varepsilon^+ = \delta$. Then $-p < Q^+ < 2w + p = Q + 2p$, so $|Q^+| \le |Q| + 2p$; and $Q^+ \equiv -2w - p \equiv -Q \pmod{2p}$, so $D^+ \equiv -Q/2 + (k+2)\kappa \equiv (2k+3)\kappa \equiv \kappa(k+2)^2$, as $D = 0$ means $Q/2 \equiv -(k+1)\kappa$ and $\kappa(k+1)^2 \equiv 0$.

Induction. The bounds $|Q_k| \le 2kp$ and $D_k \equiv \kappa(k+1)^2$ follow. ε_k is ε_0 or the δ of the last excursion, plus the θ of the side-2 steps since then, so

$$|\varepsilon_k| \le 0.2966 + 4.71\, p\vartheta \sum_{j \le k^*} \tfrac{(2j+1)p}{2} = 0.2966 + 4.71\, p^2\vartheta\, \tfrac{(p-1)^2}{8}$$
$$\le 0.2966 + 0.589\, p^4\vartheta \le 0.2966 + 0.3701 < 0.68.$$

Finally $D_k = 0$ if and only if $p \mid \kappa(k+1)^2$, if and only if $p \mid (k+1)^2$.

(c) After the last passage of step k the leaf crosses the star below the apex, entering by $7\mu + w'$ or $7\mu - v$, both $\equiv 7\mu + w_k \pmod p$, where $2w_k \equiv p - 2(k+1)\kappa$. By (F2) it crosses the leg pointing down if and only if $-5\mu + w_k \equiv -3\mu + p/2$, that is $-(k+1) \cdot 4\mu \equiv 2\mu$, that is $p \mid 2\mu(2k+3)$, that is $p \mid 2k+3$ (as $\gcd(p, 2\mu) = 1$): for $0 \le k \le k^*$ exactly at $k = k^*$. The crossing of the star above the apex inside an excursion does not meet the leg pointing up: by (F2) that would need $3\mu + w_k \equiv 3\mu + p/2$, that is $w_k \equiv p/2 \pmod p$, which by (d) needs $p \mid k+1$. The leaf crossed the leg pointing up at a right angle before y_0; by (F3) it is closed, with the passages stated. Up to the second right angle it has $1 + (k^* + 1) + e = (p+1)/2 + e$ crossings, so $p + 1 + 2e$ in all.

(d) The sizes are in the proof of (b). $2w_k \equiv p - 2(k+1)\kappa \equiv p \pmod{2p}$ would need $p \mid k+1$, while $k + 1 \le (p-1)/2$; and $v_k \equiv -w_k$. □

Corollary 7.20. *Let $p \ge 5$ and $N \ge 5p^4$. Every cylinder Y through the top window has the exponent $E_0 = 2\mu - \frac{p+1}{2}$ exactly once and no exponent $E_0 - 2\mu$ or $E_0 - 3\mu$ (passages $-p/2$ and $-\mu - p/2$). If moreover $N = 12 \cdot 2^a 3^b$, Y passes the block test.*

Proof. By Proposition 7.19(c), (d), the passages are $\pm x_0$ once each; half-integers of absolute value below $p^2/2$ that are $\not\equiv p/2 \pmod p$; and half-integers within $p^2/2$ of $\pm 2\mu$ of the forms $\pm(2\mu - w_k)$, $\pm(2\mu - v_k)$ with $w_k, v_k \not\equiv p/2 \pmod p$. Now $x_0 = 2\mu - p/2$ is none of

the latter; $-p/2 \equiv p/2 \pmod p$ is not of the second kind and is not within $p^2/2$ of $\pm 2\mu$, as $2\mu > 0.83p^4$; and $-\mu - p/2$ has absolute value above $p^2/2$ and lies farther than $p^2/2$ from -2μ, as $\mu > 0.41p^4$. With $r = E_0 - \mu \in [0, \mu)$ this gives $n_1 = 1$, $n_{-1} = n_{-2} = 0$ in Proposition 7.8. □

The case $p = 1$. We carry this case through in full; it uses the top window, the test of Proposition 7.9 and nothing from the supplement but the proof of that test. Figure 1 shows it at $N = 24$.

Proposition 7.21. *Let $p = 1$ and $\mu \geq 2$. In the direction of AC every leaf of the top window is closed after two crossings, both by side 1: at $y_0 = 3\mu - \frac{1}{2}$, with passage $x_0 = 2\mu - \frac{1}{2}$, and at $y_1 = -\mu + \frac{1}{2}$, with passage $-x_0$. These leaves form a cylinder $\mathcal{Z}$ of height $\sqrt{3}\sin^2\alpha$ and circumference $2\sqrt{3}\,\ell\cos(\frac{\pi}{3} - \alpha)$, with the exponents $2\mu - 1$ and -2μ, and $\mathcal{Z}$ passes the test at $E = 2\mu - 1$.*

Proof. Here $\alpha = \vartheta \leq \pi/24$. By the paragraph on the top window, a leaf of it at the height $\lambda\cos 2\alpha + \eta$, $0 < \eta < \Psi = \sqrt{3}\sin^2\alpha$, takes side 1 at y_0 with passage x_0, enters the star by the base $7\mu - \frac{1}{2}$, and has the new height $c_1 = \eta - \lambda/2$. As $\sin\alpha < \frac{1}{2}$, $\Psi < \sqrt{3}/4 = \lambda/2$, so $c_1 < 0$, and by Lemma 7.3(b) the leaf leaves the star by the unique right base whose window contains c_1 (with $p = 1$ the congruence there is no condition). By (7.1) and $2\mu\vartheta = \pi/6$, the window of y_1 is $(-\lambda/2, \lambda\sin(2\alpha - \frac{\pi}{6}))$, of length $\lambda(\sin(2\alpha - \frac{\pi}{6}) + \frac{1}{2}) = \sqrt{3}\sin\alpha\cos(\frac{\pi}{6} - \alpha)$, which exceeds Ψ as $\sin\alpha < \frac{1}{2} < \cos(\frac{\pi}{6} - \alpha)$. The heights c_1 fill $(-\lambda/2, -\lambda/2 + \Psi)$, so they lie in the window of y_1, and the leaf leaves by y_1.

By (F1) at $\theta = 2y_1\vartheta = \alpha - \frac{\pi}{6}$, the leaves that take side 1 at y_1 are those of the bottom part of its window of length $\sqrt{3}s\sin(\theta + \frac{\pi}{6}) = \sqrt{3}\sin^2\alpha = \Psi$, which lies between 0 and the length of the window; this is exactly the set of the heights c_1. So every leaf takes side 1 at y_1, with passage $w = y_1 - \mu = -x_0$, and enters the star by $y_1 + 4\mu = 3\mu + \frac{1}{2}$. As $2w\vartheta = \alpha - \frac{\pi}{3}$, Lemma 7.3(a) and the identity $\sqrt{3}\ell\sin(\frac{\pi}{3} - \alpha) = \frac{\lambda}{2} + \lambda\cos 2\alpha$ give the new height

$$c_1 + \sqrt{3}\,\ell\sin(\tfrac{\pi}{3} - \alpha) = \eta - \tfrac{\lambda}{2} + \tfrac{\lambda}{2} + \lambda\cos 2\alpha = \lambda\cos 2\alpha + \eta.$$

This is positive, so the leaf leaves the star by the right base whose window contains it, which is y_0, at its first height: it is closed. Every inequality used is strict for $0 < \eta < \Psi$, so no leaf of the open top window meets a point over A or C; the leaves through the ends of the window pass through the ends of the base y_0, which lie over C. So these leaves form a cylinder whose height is the length Ψ of the top window. Its exponents are the passages minus $\frac{1}{2}$, and its circumference is $\sqrt{3}\ell(\cos 2x_0\vartheta + \cos 2w\vartheta) = 2\sqrt{3}\ell\cos(\frac{\pi}{3} - \alpha)$ by Lemma 7.3.

At $E = 2\mu - 1$: $n_1 = 1$, and $E - \mu = \mu - 1$, $E - 2\mu = -1$ and $E - 3\mu = -\mu - 1$ differ from -2μ as $\mu \geq 2$, so $n_0 = n_{-1} = n_{-2} = 0$ and $n_1 - n_{-1} = 1 > 0 = \sqrt{3}n_{-2}$. The exponent -2μ has $-2\mu - E = -4\mu + 1 \equiv 1 \cdot p \pmod{2\mu}$, so $J = 1$, and $\mathfrak{s} \mid 2(x - E)$ if and only if $\mathfrak{s} \mid 2$, that is $\mathfrak{s} = 2$; the exponent E itself has $r = 0$. So $\mathcal{R} = \emptyset$ unless $\mathfrak{s} = 2$ and $\mathfrak{d} > 1$; then $r \equiv p = 1 \pmod{\mathfrak{d}}$, $\mathcal{R} = \{1\}$, and the sum is $\prod_{q|\mathfrak{d}} 2/(q-1) \leq \frac{1}{2}$, as every $q \geq 5$. In each case the sum is less than 1. □

At $N = 12$ the same two crossings give the exponents 1 and -2, and neither inequality of the block test holds.

Corollary 7.22. *Theorem 7.1 holds for $p = 1$.*

Proof. Let $N > 58$ and $p = 1$. As $3 \nmid p$, Δ is in (I), where $N \geq 72$, or in (III), where $N \geq 60$. So $H_{12} \subset S$ by Proposition 7.12(a) or (c). By Propositions 7.21 and 7.9 the cylinder $\mathcal{Z}$ passes, so every unit lies in S by Proposition 7.6, and the rest of Theorem 7.1 follows. □

7.5. **The plan in the four settings.** Let $N > 58$. By Proposition 7.12, $H_{12} \subset S$ in every setting, except in (II) with $p = 3$, where Proposition 7.12(b) needs $p \geq 9$; there $N = 3 \cdot 2^{a+2} \geq 96$, and rule (iii), applied to another pair of holomorphic units, gives a unit $v \equiv 5 \pmod 8$, $v \equiv 1 \pmod 3$ in S, which generates the units $\equiv 1 \pmod{12}$; so again $H_{12} \subset S$ (supplement, §S5). By Proposition 7.6 it is then enough to find, at each (p, N), one cylinder of the direction of AB or AC that passes. At one pair, $(9, 60)$, there is none, and we bound the rank instead (Proposition 7.28). As $\gcd(p, \mu) = 1$, $\rho = c/e$ in lowest terms means $p = c$ and $\mu = e$; so ρ is not 1, $\frac{8}{7}$, $\frac{4}{3}$, $\frac{8}{5}$, $\frac{12}{7}$ or 2, as $\mu \geq 5$ and p is odd. Table 3 lists the cylinders used, by range of ρ.

range	cylinder	it passes
$p = 1$	$\mathcal{Z}$ of AC, two crossings (Proposition 7.21)	the test at $2\mu - 1$
$p = 3$	$\mathcal{Z}_3$ of AC, four crossings (Proposition 7.23)	the test at $2\mu - 2$; at $N = 60$, 84 by an explicit function
$2 < \rho < 4$	$\mathcal{U}$ of AC, two crossings (Proposition 7.17)	the test at $3\mu - \frac{p+1}{2}$ (Lemma 7.18)
$(1, \frac{13}{10}] \cup (\frac{4}{3}, 2)$	one of 17 types with intervals (Proposition 7.26)	the test, outside 35 pairs
$\frac{13}{10} < \rho < \frac{4}{3}$	$\mathcal{V}$ of AB, four crossings (Proposition 7.24)	the test at $5\mu - 3p$
$\rho < 1$, $N \geq 5p^4$	through the top window (Proposition 7.19)	by Corollary 7.20 and supplement, §S5
$\rho < 1$, $N < 5p^4$, $\frac{1}{2} < f < \frac{33}{64}$	$\mathcal{V}_K$ of AB, four crossings (Proposition 7.25)	the test at $\mu + \delta_K$
$\rho < 1$, $N < 5p^4$, otherwise	members of families of types (Proposition 7.27)	supplement, §S5
$(p, N) = (9, 60)$	none	Proposition 7.28

TABLE 3. The cylinders that prove Theorem 7.1 for $N > 58$, by range of $\rho = p/\mu$; $t = 2\mu/p$, $K = \lfloor t \rfloor$, $f = t - K$, and $\delta_K = 4\mu - (2K + 1)p$.

The statements follow; their proofs are in the supplement (§S5). The first three are statements about the star at the real number ρ (that a sequence of crossings is followed by an interval of heights) together with a count of exponents, as in Proposition 7.21.

Proposition 7.23. *Let $p = 3$, so that $9 \nmid N$, and let $\mu \geq 5$. In the direction of AC the leaves of the top window form one cylinder $\mathcal{Z}_3$ with four crossings, by the sides 1, 2, 2, 1, with the exponents $2\mu - 2$, 0, -1 and $-2\mu + 1$. It passes the test at $E = 2\mu - 2$ unless $N \in \{60, 84\}$, and at $N = 60$ and $N = 84$ it passes.*

Proposition 7.24. *Let $\frac{13}{10} < \rho < \frac{4}{3}$, $\delta = 4\mu - 3p$ and $\lambda = \sqrt{3}/2$. In the direction of AB the leaves that leave the star through the right base p at a height c with*

$$\lambda \sin 7\alpha < c < \lambda\big[\sin\alpha + \sin(3\alpha - \tfrac{\pi}{3}) + \sin(\tfrac{2\pi}{3} - 5\alpha)\big]$$

form a cylinder $\mathcal{V}$ with four crossings: they leave the star by the bases p, δ, $-p$, $-\delta$, with the sides 1, 2, 2, 1. Its exponents are $p - \mu$, $5\mu - 3p$, $\mu - p$, $3p - 5\mu$, and it passes the test at $E = 5\mu - 3p$.

Proposition 7.25. *Let $K \geq 2$ be an integer with $\frac{128\mu}{64K+33} < p < \frac{4\mu}{2K+1}$, and $\delta_K = 4\mu - (2K+1)p$. In the direction of AB the leaves that leave the star through the right base Kp at the heights of an explicit interval form a cylinder $\mathcal{V}_K$ with four crossings: they leave the star by the bases Kp, δ_K, $-Kp$, $-\delta_K$, with the sides 1, 2, 2, 1. Its exponents are $Kp - \mu$, $\mu + \delta_K$, $\mu - Kp$, $-\mu - \delta_K$, and it passes the test at $E = \mu + \delta_K$.*

In the middle range the cylinders are found by computation. A *type* is a closed itinerary through the star: the bases $A_j\mu + B_jp/2$ by which a leaf leaves it, with fixed integers A_j, B_j, the sides it takes there, and the side of the apex on which it crosses the star next. Whether a leaf follows a type is a set of inequalities between trigonometric polynomials in α, so it depends on ρ and not on N; the passages, doubled, are $a_j\mu + b_jp$ with integers a_j, b_j fixed by the type. For a type τ there is a finite set $X(\tau)$ of values of N, given by the differences of the b_j and the primes of $\mathfrak{d}$, such that at every $N \notin X(\tau)$ whose ρ lies in the interval of τ the cylinder of τ passes the test; the proof rests on the last remark after Proposition 7.9.

Proposition 7.26. *There are 18 types, each with an interval on which it is realised, whose intervals have union $(1, \frac{13}{10}] \cup (\frac{4}{3}, 4)$ minus the points $\frac{8}{7}$, $\frac{8}{5}$, $\frac{12}{7}$ and 2; one of them is the type of $\mathcal{U}$ on $(2, 4)$. Let $N > 58$ and $\rho \in (1, \frac{13}{10}] \cup (\frac{4}{3}, 4)$. Then some cylinder of the direction of AB or AC passes, unless $(p, N) = (9, 60)$. More precisely, the cylinder of some type whose interval contains ρ passes the test, unless (p, N) is one of the following 35 pairs:*

- *in (I):* $(7, 72)$, $(13, 96)$*; in (II):* $(9, 96)$*;*
- *in (III):* $(7, 60)$, $(11, 84)$, $(13, 84)$, $(11, 120)$, $(13, 120)$, $(17, 120)$, $(19, 120)$, $(17, 132)$, $(19, 132)$, $(17, 168)$, $(19, 180)$, $(23, 240)$, $(37, 252)$, $(25, 264)$, $(37, 276)$, $(29, 312)$, $(37, 420)$, $(59, 420)$, $(61, 420)$, $(71, 660)$, $(97, 660)$, $(113, 780)$, $(79, 840)$*;*
- *in (IV):* $(9, 60)$, $(9, 84)$, $(15, 132)$, $(21, 132)$, $(33, 228)$, $(45, 336)$, $(39, 420)$, $(57, 420)$, $(87, 660)$.

At 31 of these pairs we find that the cylinder of a type passes. At the following three we find another cylinder that passes, with the exponents

- $(13, 96)$*, of AC, 16 crossings:* $-13, -10, -7, -7, -6, -6, -1, -1, 0, 0, 5, 5, 6, 6, 9, 12$*; the test at $E = 12$;*
- $(13, 120)$*, of AC, 8 crossings:* $-19, -9, -4, -3, 2, 3, 8, 18$*; at $E = 18$, with a choice of the measure at $q = 5$;*
- $(23, 240)$*, of AB, 9 crossings:* $-34, -23, -22, -12, 0, 12, 22, 23, 34$*; the test at $E = 23$, with $\mathcal{R} = \emptyset$.*

At $(9, 60)$ no cylinder of AB or AC passes.

The point $\rho = \frac{13}{10}$ is attained only at $(13, 120)$, and there the cylinder $\mathcal{V}$, which still exists, gives the sum $\frac{3}{2}$ in Proposition 7.9; so Proposition 7.24 is stated on the open interval, and Proposition 7.26 on the closed one.

Proposition 7.27. *Let $p \geq 5$, $\rho < 1$ and $N < 5p^4$, and let $t = 2\mu/p$, $K = \lfloor t \rfloor$ and $f = t - K$. If $f \notin [\frac{1}{2}, \frac{33}{64})$, then some cylinder of the direction of AB or AC passes.*

Here $K \geq 2$, and the cylinders belong to families of types whose itineraries depend linearly on K, so that whether a leaf follows one is a statement about (α, f) alone.

Proposition 7.28. *Theorem 7.1 holds for $\Delta = (9, 20, 31)/60$.*

Proof. The zeros of ω are the three points over A, of cone angle 6π, and the point over C; the points over B are regular. So the relative characters are 20 and 40, both even, and

$V \cap Z = 0$, as $V \subset E^-$ and by (2.1). We find that the closure of $\{1\}$ is the set S_+ of Proposition 2.8, and that among the 20 cylinders of the direction of AC there are ten, no two of them S_+-equivalent. As $S_+ \subset S$, Lemma 2.16(d) shows that no two of them are $\mathcal{M}$-parallel, and Lemma 2.16(g) gives $\operatorname{rank}\mathcal{M} \geq 10$, so $|S| \geq 20$ by (1.2). An odd a lies in F if and only if $3 \nmid a$ ($9a \equiv 0$ needs $20 \mid a$, $20a \equiv 0$ needs $3 \mid a$, and $31a \equiv 0$ needs $60 \mid a$), so F is the set of the 20 residues prime to 6, and $S = F$. □

Proof of Theorem 7.1. By the remarks after the statement it is enough that every unit lies in S. The case $(p, N) = (9, 60)$ is Proposition 7.28; in every other case $H_{12} \subset S$, as said at the start of this subsection, and by Proposition 7.6 it is enough that one cylinder of the direction of AB or AC passes. If $p = 1$, this is Proposition 7.21, and if $p = 3$, Proposition 7.23. Let $p \geq 5$. If $\rho \in (1, \frac{13}{10}] \cup (\frac{4}{3}, 4)$, apply Proposition 7.26, and if $\frac{13}{10} < \rho < \frac{4}{3}$, Proposition 7.24; as $\rho \neq 1, \frac{4}{3}$, it remains that $\rho < 1$, and then $K \geq 2$, as $t = 2/\rho > 2$. If $N \geq 5p^4$, some leaf of the top window meets no point over A or C, as these points are the ends of countably many leaves, each of which meets the top window in a countable set; its cylinder passes through the top window, and it passes by Corollary 7.20 in (I) and by §S5 of the supplement in the other settings. Let $N < 5p^4$. As $p \geq 5$ and $\gcd(p, 4\mu) = 1$, $f \neq \frac{1}{2}$; if $\frac{1}{2} < f < \frac{33}{64}$, that is $\frac{128\mu}{64K+33} < p < \frac{4\mu}{2K+1}$, apply Proposition 7.25, and otherwise Proposition 7.27. □

8. Small denominators and the proof of the main theorem

This section treats the denominators $N \leq 58$ and $58 < N \leq 400$, where the proofs are computations on finitely many triangles, and sixteen triangles with $490 \leq N \leq 2{,}000$ that no theorem of Section 6 covers. Then it proves Theorems 1.2 and 1.1.

8.1. **Denominators up to 58.**

Theorem 8.1. *Let Δ be a scalene rational triangle with $N \leq 58$ that is not in (1.1). Then $S = F$, and the orbit closure of its unfolding is its ambient locus.*

This is the conclusion of Delecroix and Rüth's theorem [10, Theorem 4.1] for these triangles. The proof, in §S6 of the supplement, does not use their theorem, and runs as follows. There are 4,093 scalene triangles with $N \leq 58$, and 74 of them are in (1.1). Among the other 4,019, the unfolding of $(1, 2, 3)/6$ is a flat torus, and we treat it directly. For the others, a pair $(C, \mathcal{D})$ with $C \subset F$ and $\mathcal{D} \subset R$ is closed under the five rules if C satisfies rules (i)–(iii) and the pair satisfies rules (iv) and (v) with $(C, \mathcal{D})$ in place of $(S, \mathcal{C})$. The pair $(S, \mathcal{C})$ is one of them, so it is also closed in the weaker sense in which rule (iv) is required only at $u = 1$, and an intersection of pairs closed in this weaker sense is again one. So S contains the first member of the smallest pair closed in this weaker sense whose first member contains a given subset of S. We find that this first member is F for the subset $\{1\}$ on 3,740 of the triangles, and for every subset $\{1, t\}$ with $t \in F \setminus \{\pm 1\}$ on 156 more; on these, $|S| \geq 4$, as the scalene triangles of rank one other than $(1, 2, 3)/6$ are in (1.1) [19, Theorem 1.1], so $S = F$. On 120 triangles one or two completely periodic directions of the unfolding, computed exactly in the number field of the surface, put into S, through the twists of [35, Corollary 3.4] (supplement, Theorem S6.2) and the test of Lemma 2.16(e), a character from which these rules reach F. This lower bound follows Delecroix and Rüth's procedure [10, §3]; the twists of the cylinders of one direction, which lie in V by Wright's theorem [35, Corollary 3.4], are the step of their algorithm, and the test of Lemma 2.16(e) is added to it. The last two triangles, $(1, 6, 41)/48$ and $(1, 7, 48)/56$, lie in families of cyclic covers of the sphere; there we use that orbit closures are affine invariant submanifolds [12, 13] and algebraic [14, Theorem 1.1], and Mirzakhani

and Wright's theorems on their boundary [27, Theorem 2.9 and Corollary 2.14], with the unfolding of $(7, 8, 41)/56$, one of the 120, in the family of the first and on the boundary of the family of the second. By Corollary 2.4, $S = F$ gives the second assertion.

8.2. **Denominators from 59 to 400.**

Proposition 8.2. *Let N be composite with $58 < N \le 400$, not a power of 2 and not $2P$ or $3P$ with P prime. Let Δ be scalene and not in (1.1), with no numerator $2N/3$, other than Γ_1 with $4 \mid N$, Γ_2 with $8 \mid N$ and Γ_4 with $N \equiv 4 \pmod 8$, and with no numerator $N/3$ if $12 \mid N$. Then every closed set $C \ni 1$ with $|C| \ge 4$ is F.*

Proof. We find, at every such N and on every such Δ:

(a) if Δ has a witness, the closure of $\{1\}$ is F;
(b) if Δ has no witness, every closed set $C \ni 1$ other than F is H_m for some $m \mid N$;
(c) on the 911 triangles without a witness, at 217 values of N, no H_m with $\{\pm 1\} \ne H_m \ne G$ is closed.

Let $C \ni 1$ be closed with $|C| \ge 4$. If Δ has a witness, C contains the closure of $\{1\}$, which is F by (a). If not, and $C \ne F$, then $C = H_m$ for some m by (b), $H_m \ne \{\pm 1\}$ as $|C| \ge 4$, and $H_m = G$ by (c). Then $G = C$ satisfies the rules, and Theorem 1.5 gives $C = F$, as $N > 30$, a contradiction. □

We find (a) by iterating the three rules from $\{1\}$ until nothing is added. For (b) the closed sets containing 1 are listed by closure: starting from the closure of $\{1\}$, each closed set other than F found so far is enlarged by one element outside it and closed again; every closed $C \ni 1$ is reached, since adding the elements of C one at a time never leaves C. For (c) each H_m is tested against Lemma 3.3. The exclusions of Γ_1, Γ_2, Γ_4 and of a numerator $2N/3$ are needed: some H_m with $\{\pm 1\} \ne H_m \ne G$ is closed on each of the 172 triangles Γ_1, Γ_2, Γ_4 in this range, where it is $H_{N/2}$, and on 95 triangles with a numerator $2N/3$.

8.3. **Sixteen triangles with $N \le 2{,}000$.**

Proposition 8.3. *The sixteen triangles $\mathcal{B}_3 = (3, 2N/5 - 3, 3N/5)/N$ with*

$$N \in \{490, 500, 640, 770, 800, 910, 1000, 1190, 1250, 1280, 1330, 1430, 1600, 1870, 2000\}$$

and $\mathcal{B}_5 = (5, 219, 280)/504$ satisfy (N′).

Proof. Let Δ be one of them, and suppose that a closed set $C \ni 1$ has a unit part $H \ne \{\pm 1\}$ of conductor N'. Then $C = H$ by Lemma 2.7, H satisfies (P) by Lemma 3.3, and H contains $U_0 = \langle -1, h\rangle$ for a unit $h \in H \setminus \{\pm 1\}$. For each unit $h \ne \pm 1$ we list, for every $a' \in U_0 = \langle -1, h\rangle$, the pairs on the diagonal $1 - a'$ with a unit member. If one of them has exactly one unit member, (P) fails for every $H \supset U_0$. Otherwise (P) puts the ratios b/x of these pairs into H, and with U_0 they generate a group $U_1 \subset H$; the conductor of H divides that of U_1, which divides N', so if the conductor of U_1 is not N', neither is that of H. We find that every h is settled in this way: at $N = 504$ and at the seven $N \equiv 2 \pmod 4$ other than 1,250 by a pair with one unit member, and at the other eight N by the conductor of U_1. So no such C exists. □

8.4. **Proof of the main theorem.**

Proof of Theorem 1.2. Let $N > 58$ and let Δ be scalene and not in (1.1). Then $\operatorname{rank} \mathcal{M} \ge 2$ [19, Theorem 1.1], so $|S| \ge 4$, and S is a closed set containing 1 (Section 2.1). We take the cases of Section 1.3 in turn; in each, Δ meets none of the earlier hypotheses.

(1) N is prime. The orbit closure is the ambient locus [19, Theorem 1.2], a connected component of a stratum, whose tangent space is $H^1(X, \Sigma; \mathbb{C})$. So $p(V) = H^1(X; \mathbb{C})$, and $S = F$ by (1.2).

(2) A numerator $2N/3$. Theorem 6.3, as $N > 48$.

(3) $12 \mid N$ *and a numerator* $N/3$. The other two numerators add up to $2N/3$; let p be the smaller. Then $\Delta = (p, N/3, 2N/3 - p)/N$ with $1 \le p < N/3$, and $\gcd(p, N/3) = 1$, since it divides all three numerators. Theorem 7.1 gives $S = F$.

(4) Γ_1 *with* $4 \mid N$, Γ_2 *with* $8 \mid N$, Γ_4 *with* $N \equiv 4 \pmod 8$. Theorems 6.11, 6.12 and 6.13, as $N \ge 60$.

(5) $N = 2^j$, $2P$ *or* $3P$ *with* P *prime.* If $N = 2^j$, then $N \ge 64$ and Δ is neither Γ_1 nor Γ_2, and Proposition 5.8 applies. If $N = 2P$, then $P \ge 31$, and by Proposition 5.9 the unit part of S is $\{\pm 1\}$ or G; it is not $\{\pm 1\}$ by Lemma 2.7, as $|S| \ge 4$, so $G \subset S$, and $S = F$ by Theorem 1.5. If $N = 3P$, then $P \ge 23$, and Proposition 5.10 applies: its exception $(3, P - 3, 2P)/3P$ has the numerator $2N/3$.

(6) $N \le 400$. Now N is composite, not 2^j, $2P$ or $3P$, and Δ satisfies the hypotheses of Proposition 8.2, which gives $S = F$.

(7) $N > 400$. Now N is composite and not 2^j, $2P$ or $3P$, and Δ has no numerator $2N/3$, is not one of the three triangles of case (4), and has no numerator $N/3$ if $12 \mid N$. We check the three conditions of Corollary 3.2.

(N′): if Δ has a witness, Theorem 1.4 gives (N′). If not, Δ is one of the triangles of Proposition 4.1, and as it has no numerator $2N/3$ and is not Γ_1, Γ_2 or Γ_4, it is one of the following.

- $\mathcal{A}_d$ with $n = N/d \ge 5$ odd, so that d and N have the same power of 2. If $d = 1$, N is odd, and $S = F$ by Theorem 6.20. If N is odd and $d \ge 3$, or $4 \mid N$, or $N \equiv 2 \pmod 4$ and $d \ge 6$, then $S = F$ by Theorem 6.19. If $d = 2$, then $N \equiv 2 \pmod 4$, $\nu = N/2$ is odd and composite, as $N \ne 2P$, and Theorem 6.17 gives (N′), as remarked after it.
- Λ, with ν odd and composite: Theorem 6.15.
- Θ_0 with $4 \mid N$: Theorem 6.16 if $3 \nmid N$, and Theorem 6.18(a) if $3 \mid N$, as then $12 \mid N$.
- Θ_1, Θ_2 or Θ_3 with $N \equiv 4 \pmod 8$: Theorem 6.18(b) and (c), as $N/4 > 100$.
- $\mathcal{B}_{k,d}$: Theorem 6.21, and Proposition 8.3 on the sixteen triangles named there.

In each case (N′) holds or $S = F$.

(D): if $4 \mid N$, then Δ has no numerator $N/3$, since such a numerator needs $3 \mid N$ and so $12 \mid N$; and N is not a power of 2; so Theorem 5.3 applies. By Lemma 5.1, a conductor c with $1 < c < N'$ of the unit part of a closed set has a step with $e \ge 2$, and $e = 2$ only if $4 \mid N$ and c is the conductor named in Theorem 5.3, which no closed set containing 1 has. Theorem 5.7, as $N > 60$ is composite, gives (D) at the others.

(12): if $12 \mid N$, Δ has no numerator $N/3$ or $2N/3$, and Proposition 4.2 gives (12); otherwise (12) holds by definition.

So $S = F$ by Corollary 3.2. □

Proof of Theorem 1.1. For $N \le 58$ this is Theorem 8.1. For $N > 58$, $\Delta \ne (1, 2, 3)/6$, and Theorem 1.2 with Corollary 2.4 gives $\mathcal{M} = \mathcal{L}$. □

9. Billiards in the triangle

Two points p and p' of Δ, not necessarily distinct, are *finitely blocked* if a finite set of points other than p and p' meets every billiard path from p to p', a path being allowed to run along a side but not through a vertex [3, §1 and Remark 3.14]. They are finitely blocked

only if every point of X over p is finitely blocked from every point of X over p', with straight segments in place of billiard paths (the blocking set on X is the preimage of the one on Δ together with the points over vertices other than p and p') [3, proof of Theorem 3.10], [2, §9]. A point of X other than a zero is *periodic* if marking it does not raise the dimension of the orbit closure of (X, ω) [1, §1].

Corollary 9.1. *Let Δ be a scalene rational triangle that is not in (1.1), $\Delta \neq (1, 2, 3)/6$. If N is odd, X has no periodic points; if N is even, its periodic points are the fixed points of ι off Σ, which lie over vertices. If two points of Δ, not necessarily distinct, are finitely blocked, they are the same vertex.*

For the right triangles among these Apisa proves more: no two points, equal or not, are finitely blocked [2, Theorem 1.3]. For prime N and $\Delta \neq (1, 2, 4)/7$ the last assertion is Apisa and Wright's [3, Theorem 3.12 and Remark 3.14], and for every rational polygon that is not Gaussian, Eisenstein or rectangle-tiled and has an angle that is not a multiple of $\pi/2$ they show that only finitely many pairs of points are finitely blocked [3, Theorem 1.1(3)].

Proof. As Δ is scalene and $\Delta \neq (1, 2, 3)/6$, $N \geq 7$; so X is not a translation cover of a torus [3, proof of Proposition 3.11], and $\mathcal{M} = \mathcal{L}$ by Theorem 1.1. Let $(Y, q) = (X, \omega)$ and $\mathcal{S} = \mathcal{L}$ if N is odd, and $(Y, q) = (X/\iota, q)$ and $\mathcal{S} = \mathcal{Q}$ (Section 2.2) if N is even. As ι is a power of T, the map from X to Δ factors through Y; and T acts freely on the points of X that are not over a vertex [19, §2.1].

The component $\mathcal{S}$ is not hyperelliptic. For odd N, Mirzakhani and Wright's Lemma 6.7 [28] excludes it, as after Theorem 1.2. For even N, an automorphism α of Y with $\alpha^* q = q$ lifts to an automorphism $\tilde{\alpha}$ of X with $\tilde{\alpha}^* \omega = \pm\omega$, which is 1 or ι [19, Theorem 6.2], so α is the identity; but every surface in a hyperelliptic component has an involution that preserves its quadratic differential [24, Definition 1 and §4.1]. This is the sense of Apisa and Wright, whose hyperelliptic components are those in which every surface covers a surface of genus zero by the quotient by an involution preserving its quadratic differential [3, §1, Lemma 4.5 and §5].

The orbit of (Y, q) is dense in a neighborhood W of (Y, q) in $\mathcal{S}$. For odd N this is Theorem 1.1, with $W = \mathcal{S}$. For even N, Lanneau's chart identifies a neighborhood W of (Y, q), by the double-cover map, with $E^- \cap U$, which is $\mathcal{M} \cap U$ as $\mathcal{M} = \mathcal{L}$ (Section 2.2 and the proof of Lemma 2.2). If $g(X, \omega) \in U$ with $g \in \mathrm{GL}(2, \mathbb{R})$, the point of W over it is its quotient by an involution that negates its form; that involution is affine with derivative $-I$ for the flat structure of ω, as $g(-I)g^{-1} = -I$, so it is ι [19, Theorem 6.2], and the point is $g(Y, q)$. As the orbit of (X, ω) is dense in $\mathcal{M}$, the orbit of (Y, q) is dense in W.

The orbit closure of (Y, q) contains W, so it is $\mathcal{S}$; if (Y, q) had a non-bijective half-translation covering of some degree, every surface of $\mathcal{S}$ would, as surfaces with such a covering form a closed invariant set, contradicting [3, Lemma 4.5]. Hence every half-translation covering of (Y, q) is bijective. The covering $X \to Y$ is a factor of Apisa and Wright's minimal covering $\pi_{Q_{\min}}$ of X onto a half-translation surface [3, Lemma 3.3], so $\pi_{Q_{\min}}$ is $X \to Y$ followed by a bijection, and two points of X have the same image under $\pi_{Q_{\min}}$ if and only if they have the same image in Y.

If N is odd, X has genus at least two (Section 2.1) and dense orbit in the component $\mathcal{S}$, which is not hyperelliptic, so it has no periodic points [1, Theorem 1.1]. If N is even, $\operatorname{rank} \mathcal{L} = |F|/2 \geq \varphi(N)/2 \geq 2$ (Section 2.2), as every unit lies in F (Section 2.1); so $\mathcal{Q}$ is not $\mathcal{Q}(-1^4)$, $\mathcal{Q}(2, -1^2)$ or $\mathcal{Q}(2^2)$ [3, Corollary 4.3], and the periodic points of X are fixed points

of ι off Σ [3, Theorem 1.4], which lie over vertices as $\iota = T^{N/2}$; conversely, a fixed point of ι off Σ is periodic, as its period relative to a zero s is half the period of a path from s to ιs.

Let $p, p' \in \Delta$ be finitely blocked. Suppose that p is not a vertex, and let $x \in X$ lie over p, so that x is neither a zero nor a periodic point. Let $x' = Tx$ if $p' = p$, and let x' be any point over p' otherwise. Then x and x' have different images in Y; for $p' = p$ because $Tx \notin \{x, \iota x\}$, as T acts freely on the points over p and $N \geq 7$. As x and x' are finitely blocked, this contradicts [3, Theorem 3.6]. So p, and likewise p', is a vertex. Suppose that $p \neq p'$, and let x and x' be the ends of a lift to X of the side from p to p'; its interior lies over the interior of the side, so it meets no point over a vertex. As x and x' have different images in Y, they are periodic points or zeros [3, Theorem 3.6], so their positions are locally determined by the unmarked surface, and so are those of the points of a minimal finite set B that blocks them [3, Lemma 3.8]. Marking B therefore does not raise the dimension of the orbit closure, so the points of B are periodic points or zeros, and lie over vertices. The lift avoids B, a contradiction. So $p = p'$ is a vertex. □

Declarations

Use of AI. This paper and its results were produced by an AI research system that the author designed, built and directs, running on Anthropic's Claude Fable 5.2 in Claude Code and OpenAI's GPT-6.2 Astra in Codex. The author chooses the problems and prioritizes the work. Separate AI agents checked each result, and a second program confirmed the computations the proofs use, with any exceptions listed in the public deposit. The system also searched the literature and checked the citations against reliable sources. The author read the paper, reran the computations from the deposit and takes full responsibility for all of the paper's contents.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [20].

References

1. Paul Apisa, $\mathrm{GL}_2\mathbb{R}$*-invariant measures in marked strata: generic marked points, Earle–Kra for strata, and illumination*, Geom. Topol. **24** (2020), no. 1, 373–408, doi:10.2140/gt.2020.24.373.
2. ———, *Billiards in right triangles and orbit closures in genus zero strata*, 2021, Preprint, arXiv:2110.07540v1.
3. Paul Apisa and Alex Wright, *Marked points on translation surfaces*, Geom. Topol. **25** (2021), no. 6, 2913–2961, doi:10.2140/gt.2021.25.2913, arXiv:1708.03411v3.
4. ———, *High rank invariant subvarieties*, Ann. of Math. (2) **198** (2023), no. 2, 657–726, doi:10.4007/annals.2023.198.2.4, arXiv:2102.06567v1.
5. Keith Conrad, *Gauss and Jacobi sums on finite fields and* $\mathbf{Z}/m\mathbf{Z}$, Expository notes, https://kconrad.math.uconn.edu/blurbs/gradnumthy/Gauss-Jacobi-sums.pdf, read November 18, 2026.
6. Vincent Delecroix, *Surfaces: combinatorics, geometry, algorithms and dynamics*, Mémoire d'habilitation, Université de Bordeaux, 2024, HAL tel-05410741v1.
7. ———, *Computing the multiscale boundary of linear subvarieties*, 2025, Slides, joint work with K. Fu and B. Zykoski, JHH80, Toulouse, June 2025, https://indico.math.cnrs.fr/event/12318/.
8. Vincent Delecroix, W. Patrick Hooper, and Julian Rüth, *sage-flatsurf*, 2025, Zenodo, doi:10.5281/zenodo.17650831.
9. Vincent Delecroix and Julian Rüth, *flatsurf*, 2024, Zenodo, doi:10.5281/zenodo.13838321.
10. ———, *A new orbit closure in genus 8?*, Exp. Math. **34** (2025), no. 2, 254–259, doi:10.1080/10586458.2024.2361608, arXiv:2110.05407v2.
11. Alex Eskin, Curtis T. McMullen, Ronen E. Mukamel, and Alex Wright, *Billiards, quadrilaterals and moduli spaces*, J. Amer. Math. Soc. **33** (2020), no. 4, 1039–1086, doi:10.1090/jams/950.

12. Alex Eskin and Maryam Mirzakhani, *Invariant and stationary measures for the* $\mathrm{SL}(2,\mathbb{R})$ *action on moduli space*, Publ. Math. Inst. Hautes Études Sci. **127** (2018), 95–324, doi:10.1007/s10240-018-0099-2, arXiv:1302.3320v6.
13. Alex Eskin, Maryam Mirzakhani, and Amir Mohammadi, *Isolation, equidistribution, and orbit closures for the* $\mathrm{SL}(2,\mathbb{R})$ *action on moduli space*, Ann. of Math. (2) **182** (2015), no. 2, 673–721, doi:10.4007/annals.2015.182.2.7.
14. Simion Filip, *Splitting mixed Hodge structures over affine invariant manifolds*, Ann. of Math. (2) **183** (2016), no. 2, 681–713, doi:10.4007/annals.2016.183.2.5, arXiv:1311.2350v3.
15. W. Patrick Hooper, *Another Veech triangle*, Proc. Amer. Math. Soc. **141** (2013), no. 3, 857–865, doi:10.1090/S0002-9939-2012-11379-6, arXiv:1107.5054v1.
16. Manvir Jaswal, *Obtuse rational lattice triangles*, 2026, Zenodo, doi:10.5281/zenodo.24223593.
17. ———, *Orbit closures of generic rational polygons with at least five sides*, 2026, Zenodo, doi:10.5281/zenodo.24452738.
18. ———, *Orbit closures of generic rational quadrilaterals*, 2026, Zenodo, doi:10.5281/zenodo.24434365.
19. ———, *Orbit closures of scalene rational triangles: rank one and prime denominators*, 2026, Zenodo, doi:10.5281/zenodo.24434354.
20. ———, *Programs and data for "Orbit closures of scalene rational triangles: every denominator"*, 2026, Zenodo, doi:10.5281/zenodo.24434356.
21. Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292, doi:10.1109/TC.2017.2690633.
22. Jeremy Kahn and Alex Wright, *Hodge and Teichmüller*, J. Mod. Dyn. **18** (2022), 149–160, doi:10.3934/jmd.2022007, arXiv:2106.04665v1.
23. Richard Kenyon and John Smillie, *Billiards on rational-angled triangles*, Comment. Math. Helv. **75** (2000), no. 1, 65–108, doi:10.1007/s000140050113.
24. Erwan Lanneau, *Hyperelliptic components of the moduli spaces of quadratic differentials with prescribed singularities*, Comment. Math. Helv. **79** (2004), 471–501, doi:10.1007/s00014-004-0806-0, arXiv:math/0210099v2.
25. ———, *Connected components of the strata of the moduli spaces of quadratic differentials*, Ann. Sci. Éc. Norm. Supér. (4) **41** (2008), no. 1, 1–56, doi:10.24033/asens.2062, arXiv:math/0506136v2.
26. Anne Larsen, Chaya Norton, and Bradley Zykoski, *Strongly obtuse rational lattice triangles*, Trans. Amer. Math. Soc. **374** (2021), no. 10, 7119–7142, doi:10.1090/tran/8415; numbering as in the journal.
27. Maryam Mirzakhani and Alex Wright, *The boundary of an affine invariant submanifold*, Invent. Math. **209** (2017), 927–984, numbering as in arXiv:1508.01446v4.
28. ———, *Full-rank affine invariant submanifolds*, Duke Math. J. **167** (2018), no. 1, 1–40, doi:10.1215/00127094-2017-0036, arXiv:1608.02147v2.
29. Jan-Christoph Puchta, *On triangular billiards*, Comment. Math. Helv. **76** (2001), no. 3, 501–505, doi:10.1007/PL00013215.
30. William A. Veech, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Invent. Math. **97** (1989), no. 3, 553–583, doi:10.1007/BF01388890; Erratum: Invent. Math. 103 (1991), 447, doi:10.1007/BF01239521.
31. Yaroslav B. Vorobets, *Planar structures and billiards in rational polygons*, Russian Math. Surveys **51** (1996), no. 1, 177–178, doi:10.1070/RM1996v051n01ABEH002769.
32. ———, *Planar structures and billiards in rational polygons: the Veech alternative*, Russian Math. Surveys **51** (1996), no. 5, 779–817, doi:10.1070/RM1996v051n05ABEH002993.
33. Clayton C. Ward, *Calculation of Fuchsian groups associated to billiards in a rational triangle*, Ergodic Theory Dynam. Systems **18** (1998), no. 4, 1019–1042, doi:10.1017/S0143385798117479.
34. Alex Wright, *The field of definition of affine invariant submanifolds of the moduli space of abelian differentials*, Geom. Topol. **18** (2014), no. 3, 1323–1341, doi:10.2140/gt.2014.18.1323.
35. ———, *Cylinder deformations in orbit closures of translation surfaces*, Geom. Topol. **19** (2015), no. 1, 413–438, doi:10.2140/gt.2015.19.413; numbering and pages as in the journal.
36. Alexander N. Zemljakov and Anatole B. Katok, *Topological transitivity of billiards in polygons*, Math. Notes **18** (1975), no. 2, 760–764, doi:10.1007/BF01818045.

Toronto, Canada
Email address: manvirjaswal@icloud.com
URL: https://manvirjaswal.github.io