NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 52 (2021), 773–819
https://doi.org/10.53733/198

COMMUTATORS IN SL_2 AND MARKOFF SURFACES I

Amit Ghosh, Chen Meiri, and Peter Sarnak

(Received 20 October, 2021)

To the memory of Vaughan Jones with admiration.

Abstract. We show that the commutator equation over $\mathrm{SL}_2(\mathbb{Z})$ satisfies a profinite local to global principle, while it can fail with infinitely many exceptions for $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$. The source of the failure is a reciprocity obstruction to the Hasse Principle for cubic Markoff surfaces.

Contents

Vaughan Jones' mathematical works and brilliance are well known. Those of us who knew him personally were greatly inspired by his deep mathematical insights and a positive philosophy that extended well beyond mathematics. My enthusiasm for rugby would match Vaughan's on the rare occasion that South Africa defeated New Zealand in a test match, and I always enjoyed Vaughan's prompt and friendly emails following the other matches. I will miss these lighter things that we shared, but it his large presence in the mathematical world that I and others will sorely miss. We have lost one of our best but it is a comfort to know that his mathematics will be around for a long time.

—Peter Sarnak

1. Introduction

An element Z in a group $\mathbb{G}$ is a commutator if the equation

$$\mathscr{C}_{\mathsf{Z}}: \qquad \mathsf{X}\mathsf{Y}\mathsf{X}^{-1}\mathsf{Y}^{-1} = \mathsf{Z}, \tag{1.0.1}$$

has a solution with $\mathsf{X}, \mathsf{Y} \in \mathbb{G}$.

There is an extensive literature on understanding the set of commutators for various $\mathbb{G}$'s and the results are decisive for finite simple groups, and for semi-simple matrix groups over local fields and their rings of integers (see **[24]**, Conjecture 1.3

and [**2**] for a discussion). In these cases, most if not all elements are commutators. On the other hand if $\mathbb{G}$ is an S-arithmetic group, little is known and a description of its commutators appears to be a difficult problem, even for the simplest case that we investigate here, namely $\mathbb{G} = \Gamma_D = \mathrm{SL}_2(D)$ where D is a ring of S-integers.

A necessary condition for $Z \in \Gamma_D$ to be a commutator is that it be so in every finite quotient of Γ_D. If this condition is also sufficient then we say that Γ_D satisfies a profinite local to global principle, or a profinite Hasse principle (for commutators). These $\mathrm{SL}_2(D)$'s appear to be good candidates for such a Hasse principle, but one of our main results below shows that there may be subtle diophantine obstructions that intervene.

A fundamental difference between the case that D contains infinitely many units and when it does not, is that in the former case essentially all the finite quotients of $\mathrm{SL}_2(D)$ are congruence quotients ([**15**], [**22**]) and correspondingly the local (finite) obstructions are all simply congruence obstructions. In particular this is true for the Ihara groups $\mathrm{SL}_2([\frac{1}{\ell}])$, with ℓ a prime, which will be our central focus. The main results of this paper are that

(I). $\mathrm{SL}_2(\mathbb{Z})$ satisfies the profinite Hasse principle for commutators (and it is crucial that one allows all finite quotients here, and not only congruence quotients).

(II). For $\ell \equiv \pm 1 \pmod 5$ a prime, the commutator Hasse principle fails for $\mathrm{SL}_2([\frac{1}{\ell}])$, and in each case there are infinitely many conjugacy classes which are commutators in every finite (= congruence) quotient, but are not commutators.

(I) is proved using group theoretic tools. Results of this type are known for the equation $Z = X^m$ (that is Z is a m-th power), by Lubotsky for the free group, and Thompson for $\mathrm{SL}_2(\mathbb{Z})$ (see [**26**]). For a free group F, Khelif [**12**] proved that if an element of F is a commutator in every finite quotient of F, then it is a commutator in F. Our proof of (I) (see Theorem 2.4) follows Khelif's arguments, and we outline the main steps of this proof here. Since $-I_2$ does not belong to the commutator subgroup $\mathrm{SL}_2(\mathbb{Z})'$ of $\mathrm{SL}_2(\mathbb{Z})$ and $[\mathrm{SL}_2(\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z})'] = 12$, it is enough to prove an analogous theorem for $\mathrm{PSL}_2(\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z})$. The advantage in working with $\mathrm{PSL}_2(\mathbb{Z})$ is that it is a free product of cyclic groups of orders 2 and 3.

The first step of the proof implies that if $d \in \mathrm{PSL}_2(\mathbb{Z})$ is a commutator in the profinite completion of $\mathrm{PSL}_2(\mathbb{Z})$, then there exists a subgroup $G \subseteq \mathrm{PSL}_2(\mathbb{Z})$ which is generated by two elements and such that d is the commutator of two topological generators of the profinite completion of G. In particular, G is not abelian and, by the Kurosh subgroup theorem, $G = \langle a \rangle * \langle b \rangle$, where the orders of a and b are either 2 or 3 or ∞. The proof of this step is purely combinatorial, and a similar statement holds in an arbitrary free product of finitely many cyclic groups.

In the second step we assume that d is a commutator of two topological generators of the profinite completion of a free product $G_{m,n}$ of two cyclic groups of orders $m, n \in \{2, 3, \infty\}$. In each case, we choose a specific embedding ρ of $G_{m,n}$ in $\mathrm{PSL}_2(\mathbb{Z})$ and show that there are only finitely many possible values t for $|\mathrm{Tr}(\rho(d))|$. Every finitely generated subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ contains only finitely many conjugacy classes of elements of trace t. For each such conjugacy class we show that it either consists of commutators or that its elements are not commutators in some

finite quotient of $G_{m,n}$. The proof of the second step relies on the congruence structure of $PSL_2(\mathbb{Z})$ and the structure of the $\mathbb{Z}[G_{m,n}/G'_{m,n}]$-module $G'_{m,n}/G''_{m,n}$ for $m, n \in \{2, 3, \infty\}$. We do not know how to generalize it to arbitrary m, n.

The proof of (II) is number theoretic. Equation (1.0.1) for X and Y in $SL_2(D)$ can be viewed as seeking the D-points on the affine variety in $\mathbb{A}^8$ cut out by the four equations of degree four in the eight variables which are the entries in X and Y, together with the two quadratic equations $\det X = \det Y = 1$. In the case that $SL_2(D)$ satisfies the congruence subgroup property, the profinite obstruction to solving (1.0.1) is the same as the familiar congruence obstruction to solving (1.0.1) over D. This puts us in the realm of the usual Hasse principle for integral points on an affine variety, albeit a complicated system when viewed directly.

To study (1.0.1) we introduce two intermediate varieties defined over D: for $t \in D$

$$\mathcal{T}_t : \qquad \mathrm{Tr}(XYX^{-1}Y^{-1}) = t\,, \tag{1.0.2}$$

and the Markoff surfaces for $k \in D$

$$\mathcal{M}_k : \qquad x^2 + y^2 + z^2 - xyz = k\,. \tag{1.0.3}$$

The relation between these three varieties (for a full discussion, see Section 3) is that a solution X, Y to (1.0.1) yields a solution X, Y to (1.0.2) with $t = \mathrm{Tr}(Z)$, while a solution to (1.0.2) yields one to (1.0.3) with $x = \mathrm{Tr}(X)$, $y = \mathrm{Tr}(Y)$ and $z = \mathrm{Tr}(XY)$ with $k = t + 2$ (which follows from Fricke's identities [**8**]). In general, an integral solution of (1.0.3) does not *lift* to (1.0.2), and similarly one of (1.0.2) need not lift to a solution of (1.0.1). However, we show (see Section 3) that there is an effective procedure to decide if there are D-lifts in each of these two steps. This shows that the key diophantne equation that is at the heart of (1.0.1) is the cubic affine surface $\mathcal{M}_k$. For $k \neq 4$ these surfaces are nonsingular log K3's (see [**7**], [**27**]) and their diophantine analysis over D is delicate. If $D = \mathbb{Z}$, one can exploit the "Markoff" non-linear group of polynomial morphisims of $\mathbb{A}^3$ which preserve the surfaces $\mathcal{M}_k$, to give a diophantine theory of these surfaces (see [**9**]). In particular, failures of the Hasse principle for $\mathcal{M}_k$ that have their roots in quadratic reciprocity were discovered in [**9**], and have been interpreted as integral Brauer-Manin obstructions in [**7**] and [**13**]. In Section 5, we give a streamlined treatment of these reciprocity obstructions to Hasse principles for $\mathcal{M}_k$ and show that they extend to some of the rings D such as the ones occurring in (II) above.

On the other hand, we show that for certain D's, $\mathcal{M}_k$ and $\mathcal{T}_t$ may have no Hasse failures. In fact they can have no local congruence obstructions and (1.0.2) and (1.0.3) are universal for these D's, in that they have solutions for every choice of t and k (in D). This demonstrates the delicate nature and complexity of the diophantine properties of $\mathcal{M}_k$ over these rings D.

In Section 5, the "Brauer-Manin" obstructions to the Hasse principle for the $\mathcal{M}_k$'s are promoted to the Hasse failures of (1.0.1) that were mentioned in (II). The precise conjugacy classes which are locally commutators but not globally so, are given in Theorem 5.15. The D's in Section 4 for which $\mathcal{M}_k$ and $\mathcal{T}_t$ are universal are candidates for $SL_2(D)$'s for which every Z is a commutator, if indeed such exist.

In paper II of this series, we develop other aspects of the diophantine analysis of $\mathcal{M}_k$ over the base rings D. Specifically topological density and descent by the

nonlinear morphism group, which when D has infinitely many units acts with infinitely many orbits on $\mathscr{M}_k$ ([**3**], [**25**]), unlike the case $\mathbb{Z}$, where there are finitely many orbits. One of the goals is to find a procedure to decide whether a given Z in $SL_2(D)$ is a commutator. Apparently in going from $\mathbb{Z}$ to such D's, the integer solutions become more random and plentiful even though (1.0.3), (1.0.2) and (1.0.1) have only sparse solutions.

Acknowledgements.

It is a pleasure to thank I. Agol, N. Avni, W. Duke, A. Lubotzky and D. Puder for their valuable comments and insights concerning this paper.

AG thanks the Institute for Advanced Study and Princeton University for making possible visits during part of the years 2018-21, including an extended visit to the IAS in Spring 2020, when much of this work took place. He also gratefully acknowledges support from the Mathematics Fund of the IAS, a Simons Foundation grant No. 634846, and support from his home university for a sabbatical in 2020.

CM thanks the ISF for grant No. 1226/19. CM and PS thank the BSF for the grant No. 2014099.

PS is also supported by NSF/DMS Grant No. 1302952.

2. Local to Global Principle for the Commutator Word in $SL_2(\mathbb{Z})$

Notation 2.1.

(1) For every $n \in \mathbb{N} \cup \{\infty\}$, let C_n be a cyclic group of order n. Let

$$U := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } V := \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}. \tag{2.0.1}$$

Then $o(U) = 4$, $o(V) = 6$, $U^2 = V^3$ and

$$SL_2(\mathbb{Z}) = \langle U \rangle *_{\langle U^2 \rangle} \langle V \rangle \cong C_4 *_{C_2} C_6.$$

(2) We denote the image of U and V in $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}$ by u and v respectively. Then $PSL_2(\mathbb{Z}) = \langle u \rangle * \langle v \rangle \cong C_2 * C_3$.

(3) The derived subgroup of a group G is denoted by G' and $G'' = (G')'$.

(4) The profinite completion of a group G is denoted by $\widehat{G}$.

(5) An element g in a group G is called a commutator if there exists $x, y \in G$ such that $g = [x, y] := xyx^{-1}y^{-1}$. If $g \in G$ is a commutator then $g \in G'$ but there might be elements of G' which are not commutators.

Remark 2.2. We assume that the reader is familiar with the basic properties of profinite groups and profinite completions (see [**19**] and [**29**] for details).

Khelif [**12**] proved the following theorem:

Theorem 2.3 (Khelif)**.** *Let F be a free group and let $g \in F$. If g is a commutator in $\widehat{F}$ then g is a commutator in F.*

Here we prove a similar result, namely

Theorem 2.4. *Let Γ be either $SL_2(\mathbb{Z})$ or $PSL_2(\mathbb{Z})$ and let $d \in \Gamma$. If d is a commutator in $\widehat{\Gamma}$ then d is a commutator in Γ.*

We recall that a subset S of a topological group G is said to topologically generate G if the discrete subgroup generated by S is dense in G. The proof of Theorem 2.4 follows Khelif's argument closely and is based on the following two propositions.

Proposition 2.5. *Let $d \in \mathrm{PSL}_2(\mathbb{Z})$ be a commutator in $\widehat{\mathrm{PSL}_2(\mathbb{Z})}$. Then there exist $a, b \in \mathrm{PSL}_2(\mathbb{Z})$ such that $d \in G := \langle a, b\rangle$ and d is the commutator of a pair of topological generators of $\widehat{G}$.*

Proposition 2.6. *Let $m, n \in \{2, 3, \infty\}$ and let $G_{m,n} = \langle a\rangle * \langle b\rangle$ where $o(a) = m$ and $o(b) = n$. If $d \in G_{m,n}$ is a commutator of a pair of topological generators of $\widehat{G}_{m,n}$ then d is a commutator in $G_{m,n}$.*

Remark 2.7.

(1) For $(m, n) = (\infty, \infty)$, Proposition 2.6 follows from Theorem 2.3.
(2) The proof of Proposition 2.6 is easy in the case $(m, n) = (2, 2)$. Indeed, $G_{2,2}$ is the infinite dihedral group $D_\infty = C_\infty \rtimes C_2$ where the conjugation action of the generator g of C_2 on the generator h of C_∞ is given by $ghg^{-1} = h^{-1}$. Thus, every element in $H := \langle h^2\rangle$ is a commutator in D_∞. On the other hand, H is a normal subgroup in D_∞ and $D_\infty/H \simeq C_2 \times C_2$ is abelian so H is the commutator subgroup of D_∞. It follows that an element of $C_\infty \rtimes C_2$ is a commutator if and only if it belongs to $\langle h^2\rangle$. In particular, an element of $G_{2,2} \simeq C_\infty \rtimes C_2$ is a commutator if and only if its image in $C_2 \rtimes C_2 \simeq C_2 \times C_2$ is a commutator.
(3) We do not know how to prove Proposition 2.6 nor Theorem 2.4 for a general free product of two cyclic groups.

Proof of Theorem 2.4.

Assume first that $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. Since $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to $C_2 * C_3$, it follows from the Kurosh subgroup theorem (see Chap. 3.3 of [**14**]) that every non-trivial subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is a free product of cyclic groups and that every one of these cyclic groups is isomorphic to either C_2, C_3 or C_∞. It follows from the Grushko-Neumann theorem (see Chap. 3.3 of [**14**]) that the product of k non-trivial cyclic groups cannot be generated by less than k elements. Thus, every non-abelian subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is of the form $\langle a\rangle * \langle b\rangle$ where $o(a) = m$, $o(b) = n$ and $m, n \in \{2, 3, \infty\}$. Theorem 2.4 then follows from Propositions 2.5 and 2.6.

Now assume that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Let $D \in \mathrm{SL}_2(\mathbb{Z})$ be the commutator of two elements of $\widehat{\mathrm{SL}_2(\mathbb{Z})}$. The first paragraph implies that there exist $A, B \in \mathrm{SL}_2(\mathbb{Z})$ such that $[A, B] = \pm D$. Let g be a generator of the cyclic group C_{12}. The map $U \mapsto g^3$ and $V \mapsto g^2$ can be uniquely extended to a homomorphism from $\mathrm{SL}_2(\mathbb{Z}) = \langle U\rangle *_{\langle U^2\rangle} \langle V\rangle$ to C_{12}. The image of U^2 under this homomorphism is $g^6 \neq 1$. Since C_{12} is abelian, $U^2 = -I_2$ is not contained in $\mathrm{SL}_2(\mathbb{Z})'$. Thus, it is not possible that both D and $-D$ are commutators in the finite quotient $\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})'$. Since $\mathrm{PSL}_2(\mathbb{Z})/\mathrm{PSL}_2(\mathbb{Z})'$ is finite, the assumption implies that D is a commutator in $\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})'$ so $-D$ is not a commutator in $\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})'$. Thus it is not possible that $[A, B] = -D$. □

2.1. Proof of Proposition 2.5.

We first summarize the definitions and results we need about groups acting on trees, see [**23**] for more details.

(1) The sets of vertices and edges of a graph X are denoted by $V(X)$ and $E(X)$.
(2) Graphs are assumed to be oriented. Thus:
   (a) Every edge e has an origin $o(e)$ and a terminus $t(e)$.
   (b) There exists an involution $^{-}\colon E(X) \to E(X)$ such that for every $e \in E(X)$, $o(e) = t(\bar{e})$ and $\bar{e} \neq e$.
   (c) There is an orientation $E^+(X) \subseteq E(X)$, so for every $e \in E(X)$,
$$|E^+(X) \cap \{e, \bar{e}\}| = 1.$$
(3) A tree is a graph such that between any two vertices there exists a unique directed path without backtracking.
(4) An action of a group G on a tree X is called a good action if for every non-identity $g \in G$ and every $e \in E^+(X)$, $ge \in E^+(X)$ and $ge \neq e$.
(5) If a group G has a good action on a tree X, then the quotient graph $G\backslash X$ is oriented.
(6) If G acts on a tree X and $v \in V(X)$ then the stabilizer of v is defined to be $G_v := \{g \in G \mid gv = v\}$.
(7) If $G = H_1 * \cdots * H_k$ then there exists a good action of G on a tree X with the following two properties:
   (a) For every $1 \leqslant i \leqslant k$, there exists a vertex v such that $H_i = G_v$.
   (b) For every $v \in V(E)$, there exists $1 \leqslant i \leqslant k$ such that G_v is conjugate to H_i.
(8) In the special case where $G = H_1 * \cdots * H_k$ and each H_i is cyclic, there exists a good action of G on a tree X with the following two properties:
   (a) For every $1 \leqslant i \leqslant k$, if H_i is finite then there exists a vertex v such that $H_i = G_v$.
   (b) For every $v \in V(E)$, G_v is finite and either G_v is trivial or there exists $1 \leqslant i \leqslant k$ such that G_v is conjugate to H_i.

The following Lemma is a special case of the structure theorem of groups acting on trees (Chap. 5 of [**23**]).

Lemma 2.8. *Let G be a group which has a good action on a tree X.*
(1) *Let T_G be a maximal tree of $X_G := G\backslash X$ and let T be a lift of T_G to X.*
(2) *For every $e \in E^+(X_G) \setminus E(T_G)$, let $\tilde{e} \in E^+(X)$ be a lift of e such that $o(\tilde{e}) \in T$ and let $g_e \in G$ be such that $g_e t(\tilde{e}) \in T$.*

Then every g_e is of infinite order and G is the free product
$$(*_{v \in V(T)} G_v) * (*_{e \in E^+(X_G) \setminus E(T_G)} \langle g_e \rangle).$$

The following corollary is a well known consequence of the Kurosh subgroup theorem.

Corollary 2.9. *Let K be free factor of a group G and let L be a subgroup of G. Then $K \cap L$ is a free factor of L.*

Proof. There exists a good action of G on a tree X such that K is the stabilizer of some vertex v of X. Let T_L be a maximal tree of $X_L := L\backslash X$ and let T be a lift of T_L to X such that v is a vertex of T. Lemma 2.8 implies that $L \cap K$ is a free factor of L. □

Corollary 2.10. *Let G be a group which has a good action on a tree X and let H be a subgroup of G.*

(1) *Let* S_H *and* T_G *be maximal trees of* $X_H := H\backslash X$ *and* $X_G := G\backslash X$ *and let* S *and* T *be lifts of* S_H *and* T_G *to* X.
(2) *For every* $e \in E^+(X_H) \setminus E(S_H)$, *let* $\tilde{e}$ *be a lift of* e *to* X *such that* $o(\tilde{e}) \in V(S)$ *and let* $h_e \in H$ *be such that* $h_e t(\tilde{e}) \in V(S)$.
(3) *Let* $D \subseteq E^+(X_H) \setminus E(S_H)$ *and* $U \subseteq V(S)$.

Assume that

(a) $V(S \cap T)$ *contains* $U \cup \{o(\tilde{e}), h_e t(\tilde{e}) \mid e \in D\}$.
(b) *For every* $v \in U \cup \{o(\tilde{e}) \mid e \in D\}$, $G_v = H_v$.

Then $L := (*_{v\in U} H_v) * (*_{e\in D} \langle h_e \rangle)$ *is a free factor of* G.

Proof. Let $\pi_H : X \to X_H$ and $\pi_G : X \to X_G$ be the quotient maps. We claim that for every distinct $e_1, e_2 \in \{\tilde{e} \mid e \in D\} \cup E(S \cap T)$, $\pi_G(e_1) \neq \pi_G(e_2)$. Assume otherwise. Assumption (a) implies that $o(e_1), o(e_2) \in V(S \cap T)$. Since the map π_G is injective on $V(T)$, $o(e_1) = o(e_2)$. Thus, there exists $g \in G_{o(e_1)}$ such that $ge_1 = e_2$. Assumption (b) implies that $G_{o(e_1)} = H_{o(e_1)}$ so $\pi_H(e_1) = \pi_H(e_2)$. This is a contradiction since π_H is injective on $E(S) \cup \{\tilde{e} \mid e \in E^+(X_H) \setminus E(S_H)\}$.

Let $e \in D$. We want to show that $\hat{e} := \pi_G(\tilde{e})$ belongs to $E^+(X_G) \setminus E(T_G)$. Since $\pi_G(t(\tilde{e})) = \pi_G(h_e t(\tilde{e}))$, assumption (a) implies that the subtree $\pi_G(S \cap T)$ of T_G contains a path from $o(\hat{e}) = \pi_G(o(\tilde{e}))$ to $t(\hat{e}) = \pi_G(t(\tilde{e}))$. Since $\{\tilde{e} \mid e \in D\}$ and $E(S \cap T)$ are disjoint, the first paragraph implies that $\hat{e} \notin E(\pi_G(S \cap T))$. Since $\pi_G(S \cap T)$ is a subtree of T_G and $\pi_G(S \cap T)$ contains the origin and terminus of $\hat{e}$ but does not contain $\hat{e}$, $\hat{e} \notin E(T_G)$ as desired.

If $e \in D$ then:

- By the first two paragraphs, $\pi_G(\tilde{e}) \in E^+(X_G) \setminus E(T_G)$.
- Assumption (a) implies that $o(\tilde{e}) \in T$.
- $h_e \in G$ satisfies $h_e t(e) \in T$.

Since $U \subseteq V(S \cap T) \subseteq V(T)$, Lemma 2.8 implies that

$$(*_{v\in U} G_v) * (*_{e\in D} \langle h_e \rangle)$$

is a free factor of G. The result follows since for every $v \in U$, $G_v = H_v$. □

Corollary 2.11. *Let* G *be a free product of cyclic groups and let* H_n *be a decreasing sequence of finite index subgroups of* G. *If* K *is a finitely generated free factor of* $H := \cap_{n\geqslant 1} H_n$ *then for every large enough* n, K *is a free factor of* H_n.

Proof. Fix a good action of G on a tree X such that the stabilizer of every vertex of X is a finite cyclic group. Let S_H be a maximal tree of $X_H := H\backslash X$. and let S be a lift of S_H to X. For every $e \in E^+(X_H) \setminus E(S_H)$, let $\tilde{e}$ be a lift of e to X such that $o(\tilde{e}) \in V(S)$ and choose $h_e \in H$ be such that $h_e t(\tilde{e}) \in V(S)$. There exists a finite set of vertices $U \subseteq V(S)$ and a finite set of edges $D \subseteq E^+(X_H) \setminus E(S_H)$ such that K is contained in $L := *_{u\in U} H_u *_{e\in D} \langle h_e \rangle$. Corollary 2.9 implies that $K = K \cap L$ is a free factor of L so it is enough to prove that there exists n such that L is a free factor of H_n.

Let $R \subseteq S$ be the minimal subtree of X which contains $U \cup \{o(\tilde{e}), h_e t(\tilde{e}) \mid e \in D\}$ and note that R is finite. For every n, let $\pi_n : X \to X_{H_n} := H_n\backslash X$ be the quotient map. Since the stabilizer of every vertex of X is finite, for every $v_1, v_2 \in V(X)$, $\{g \in G \mid gv_1 = v_2\}$ is finite. Thus, since π_H is injective on $V(S)$, for every large enough n:

(a) π_n is injective on $V(R)$ so there exists a maximal tree T_{H_n} of X_{H_n} and a lift T_n of T_{H_n} to X such that $R \subseteq T_n \cap S$.
(b) For every $v \in V(R)$, $(H_n)_v = H_v$.

The result follows from Corollary 2.10 applied to H_n instead of G and L instead of H. □

Lemma 2.12. *Let K be the free product of m non-trivial cyclic groups. Then $\widehat{K}$ is not topologically generated by less than m elements.*

Proof. Abert and Hegedus [**1**] proved that the profinite completion of a free product of m non-trivial finite groups cannot be topologically generated by less than m elements. The result follows since a free product of m non-trivial cyclic groups projects onto a free product of m non-trivial finite cyclic groups. □

Proof of Proposition 2.5 **.**

We can assume that $d \neq 1$. Let $x, y \in \widehat{PSL_2(\mathbb{Z})}$ be such that $d = [x, y]$.

For every $L \leqslant \widehat{PSL_2(\mathbb{Z})}$, let $\overline{L}$ be the closure of L in $\widehat{PSL_2(\mathbb{Z})}$. For every $n \geqslant 1$, let M_n be the intersection of all subgroups of $PSL_2(\mathbb{Z})$ of index at most n. The following properties hold:

(1) $(M_n)_{n\geqslant 1}$ is a decreasing sequence of finite index normal subgroups of $PSL_2(\mathbb{Z})$.
(2) For every $L \leqslant \widehat{PSL_2(\mathbb{Z})}$, $\overline{L} = \cap_{n\geqslant 1} L\overline{M_n}$.

For every n, denote $H_n := \overline{\langle x, y, M_n\rangle} \cap PSL_2(\mathbb{Z})$. Then:

(3) For every $n \geqslant 1$, $\overline{H_n} = \overline{\langle x, y, M_n\rangle}$ and $\cap_{n\geqslant 1}\overline{H_n} = \overline{\langle x, y\rangle}$.
(4) $H := \cap_{n\geqslant 1} H_n$ contains d.

Since H is a subgroup of $PSL_2(\mathbb{Z}) \simeq C_2 * C_3$, Kurosh's subgroup theorem implies that H is a free product of (possibly infinitely many) cyclic groups. Choose a finitely generated free factor K of H which contains d. Corollary 2.11 implies that there exists n such that K is a free factor of H_n so there exists a retraction $\rho : H_n \to K$. We claim that ρ can be extended to a a retraction $\bar{\rho} : \overline{H_n} \to \overline{K}$. By the universal property of profinite completions, ρ can be extended to a continuous homomorphism $\hat{\rho} : \widehat{H_n} \to \widehat{K}$. Since H_n has a finite index in $PSL_2(\mathbb{Z})$ and K is a free factor of H_n, $\widehat{H_n} = \overline{H_n}$ and $\widehat{K} = \overline{K}$ as topological groups. Thus, there exists an extension of ρ to a continuous homomorphism $\bar{\rho} : \overline{H_n} \to \overline{K}$. Since ρ is continuous and $\rho \restriction_K$ is the identity map, $\bar{\rho} \restriction_{\overline{K}}$ is the identity map as desired.

Since $\overline{K} \subseteq \overline{\langle x, y\rangle}$,

$$\overline{K} = \bar{\rho}(\overline{K}) \subseteq \bar{\rho}(\overline{\langle x, y\rangle}) \subseteq \overline{\langle \bar{\rho}(x), \bar{\rho}(y)\rangle} \subseteq \overline{K}.$$

Since $\widehat{K} = \overline{K}$ as topological groups, $\widehat{K}$ is topologically generated by $\bar{\rho}(x), \bar{\rho}(y)$ and $d = \rho(d) = \bar{\rho}(d) = \bar{\rho}([x, y]) = [\bar{\rho}(x), \bar{\rho}(y)]$. Kurosh's subgroup theorem implies that K is a free product of cyclic groups. Lemma 2.12 implies that K is a free product of at most two cyclic groups. Since $d \neq 1$, K is not abelian so K is the free product of two cyclic groups. □

2.2. The ring $\mathbb{Z}[G_{m,n}/G'_{m,n}]$ and the module $G'_{m,n}/G''_{m,n}$.

Notation 2.13. Let $2 \leqslant m \leq \infty$ and $2 \leqslant n \leqslant \infty$. Recall that $G_{m,n} = \langle a\rangle * \langle b\rangle$ where $\langle a\rangle$ and $\langle b\rangle$ are cyclic groups of orders m and n respectively. For every i, j, let $c_{i,j} := a^i b^j [a, b] b^{-j} a^{-i}$ and let $\bar{c}_{i,j}$ be the image of $c_{i,j}$ in $G'_{m,n}/G''_{m,n}$. Note

that for every i, j, the image of $ac_{i,j}a^{-1}$ in $G'_{m,n}/G''_{m,n}$ is equal to $\bar{c}_{i+1,j}$ and the image of $bc_{i,j}b^{-1}$ in $G'_{m,n}/G''_{m,n}$ is equal to $\bar{c}_{i,j+1}$

Remark 2.14. In all the cases that we are interested in, the order m of a is finite. However, in some definitions given below we allow m to be infinite if there is no harm in doing so.

The goal of this section is to prove:

Proposition 2.15. *Under Notation 2.13, assume that*

$$(m, n) \in \{(2, 3), (2, \infty), (3, 3), (3, \infty)\}.$$

Let $d \in G_{m,n}$ *and assume that* d *is the commutator of a pair of profinite generators of* $\widehat{G}_{m,n}$. *Then* d *is conjugate to* $[a, b]^{\pm 1}$ *modulo* $G''_{m,n}$.

Note that for every group G, G'/G'' is a $\mathbb{Z}[G/G']$-module under the conjugation action and that the $\mathbb{Z}[G/G']$-submodules of G'/G'' are the normal subgroup of G/G'' which are contained in G'/G''. In order to prove Lemma 2.15 we will study the $\mathbb{Z}[G_{m,n}/G'_{m,n}]$-module $G'_{m,n}/G''_{m,n}$.

The following lemma is well known, we only sketch a proof for the convenience of the reader.

Lemma 2.16. *Under Notation 2.13,* $G'_{m,n}$ *is a free group of rank* $(m-1)(n-1)$.

Proof. The Kurosh subgroup theorem implies that every subgroup of $G_{m,n}$ is a free product of cyclic groups and that the only finite cyclic groups which can appear as factors in this free product are conjugates of subgroups of $\langle a\rangle$ or of $\langle b\rangle$. Since $G'_{m,n}$ is normal and $G'_{m,n} \cap \langle a\rangle = G'_{m,n} \cap \langle b\rangle = 1$, $G'_{m,n}$ is a free product of infinite cyclic groups, i.e. $G'_{m,n}$ is a free group.

The Euler-Poincaré characteristic of $G_{m,n}$ is $\frac{1}{m}+\frac{1}{n}-1$ (see **[23]** for the definition and properties of the Euler-Poincaré characteristic). Since $G'_{m,n}$ is a free subgroup of index mn, the Euler-Poincaré characteristic of $G'_{m,n}$ is $mn(\frac{1}{m} + \frac{1}{n} - 1) = m + n - mn$. Thus, the rank of $G'_{m,n}$ is $1 - (m + n - mn) = (m-1)(n-1)$. □

Lemma 2.17. *Under Notation 2.13, assume that* $n < \infty$. *Then* $G'_{m,n}/G''_{m,n}$ *is a free abelian group with basis* $C := \{\bar{c}_{i,j} \mid 0 \leqslant i \leqslant m-2, 0 \leqslant j \leqslant n-2\}$ *and for every* i, j,

$$\bar{c}_{i,n-1} = (\bar{c}_{i,0})^{-1} \cdots (\bar{c}_{i,n-2})^{-1} \text{ and } \bar{c}_{m-1,j} = (\bar{c}_{0,j})^{-1} \cdots (\bar{c}_{m-2,j})^{-1}. \quad (2.2.1)$$

Proof. Since $G'_{m,n}$ is a free group of rank $(m-1)(n-1)$, $G'_{m,n}/G''_{m,n}$ is a free abelian group of rank $(m-1)(n-1)$. Since C contains $(m-1)(n-1)$ elements, if C generates $G'_{m,n}/G''_{m,n}$ then it is a free basis.

Let g, h, k be elements of a group G. The identity $[g, hk] = [g, h]h[g, k]h^{-1}$ and induction implies that for every $l \geqslant 1$,

$$[g, h^l] = [g, h](h[g, h]h^{-1}) \cdots (h^{l-1}[g, h]h^{1-l}).$$

Since $b^n = 1$, by taking $g = a$, $h = b$ and $l = n$ we the get the identity

$$\bar{c}_{0,n-1} = (\bar{c}_{0,0})^{-1} \cdots (\bar{c}_{0,n-2})^{-1}. \quad (2.2.2)$$

For every i, j, $a^i\bar{c}_{0,j}a^{-i} = c_{i,j}$. It follows form Equation (2.2.2) that for every i,

$$\bar{c}_{i,n-1} = (\bar{c}_{i,0})^{-1} \cdots (\bar{c}_{i,n-2})^{-1}.$$

Since $[x,y]=[y,x]^{-1}$, the proof that for every j,

$$\bar{c}_{m-1,j}=(\bar{c}_{0,j})^{-1}\cdots(\bar{c}_{m-2,j})^{-1}.$$

is similar.

Denote $c:=c_{0,0}$. For every $g\in G_{m,n}$, there there are $0\leqslant i\leqslant m-1$ and $0\leqslant j\leqslant n-1$ such that $g\in a^i b^j G'_{m,n}$ so $gcg^{-1}\in c_{i,j}G''_{m,n}$. Since the conjugacy class of c generates $G'_{m,n}$, the set

$$\{\bar{c}_{i,j}\mid 0\leqslant i\leqslant m-1, 0\leqslant j\leqslant n-1\}$$

generates $G'_{m,n}/G''_{m,n}$. Equation (2.2.1) implies that C generates $G'_{m,n}/G''_{m,n}$. □

A similar argument shows:

Lemma 2.18. *Under Notation 2.13, assume that $n=\infty$. Then $G'_{m,\infty}/G''_{m,\infty}$ is a free abelian group with basis $C:=\{\bar{c}_{i,j}\mid 0\leqslant i\leqslant m-2, j\in\mathbb{Z}\}$ and for every j,*

$$\bar{c}_{m,j}=(\bar{c}_{0,j})^{-1}\dots(\bar{c}_{m-1,j})^{-1}. \tag{2.2.3}$$

Notation 2.19. Let $2\leqslant m<\infty$ and $2\leqslant n\leqslant\infty$.

(1) $\phi_m(X):=X^m-1$.
(2) $\psi_m(X):=\frac{\phi_m(X)}{X-1}=X^{m-1}+\ldots+X+1$.
(3) $\phi_\infty(X)=\psi_\infty(X)=0$,
(4) $R_{m,n}:=\mathbb{Z}[X,X^{-1},Y,Y^{-1}]/(\phi_m(X),\phi_n(Y))$.
(5) $S_{m,n}:=\mathbb{Z}[X,X^{-1},Y,Y,^{-1}]/(\psi_m(X),\psi_n(Y))$.
(6) $x^{\pm1}$ and $y^{\pm1}$ are the images of $X^{\pm1}$ and $Y^{\pm1}$ in $R_{m,n}$ and in $S_{m,n}$.

Remark 2.20. $S_{m,n}$ is a quotient of $R_{m,n}$ so it is both a finitely generated ring and a cyclic $R_{m,n}$-module. The action of an element $r\in R_{m,n}$ on an element $s\in S_{m,n}$ is the multiplication of s with the image of r in S. In particular, a subset of $S_{m,n}$ is an $R_{m,n}$-submodule if and only if it is an ideal in $S_{m,n}$.

Lemma 2.21. *Under Notations 2.13 and 2.19:*

(1) *There exists a unique ring isomorphism $\rho:\mathbb{Z}[G_{m,n}/G'_{m,n}]\to R_{m,n}$ such that $\rho(a)=x$ and $\rho(b)=y$.*
(2) *Assume that $n<\infty$. There exists a unique group isomorphism π from $G'_{m,n}/G''_{m,n}$ to the additive group $S_{m,n}$ such that for every $0\leqslant i\leqslant m-2$ and every $0\leqslant j\leqslant n-2$, $\pi(\bar{c}_{i,j})=x^iy^j$.*
(3) *Assume that $n=\infty$. There exists a unique group isomorphism π from $G'_{m,n}/G''_{m,n}$ to the additive group $S_{m,n}$ such that for every $0\leqslant i\leqslant m-2$ and every $j\in\mathbb{Z}$, $\pi(\bar{c}_{i,j})=x^iy^j$.*
(4) *For every $g\in G_{m,n}/G'_{m,n}$ and $h\in G'_{m,n}/G''_{m,n}$,*

$$\pi(ghg^{-1})=\rho(g)\cdot\pi(h).$$

Thus, π is a ρ-equivariant isomorphism of the $\mathbb{Z}[G_{m,n}/G'_{m,n}]$-module $G'_{m,n}/G''_{m,n}$ and the $R_{m,n}$-module $S_{m,n}$.

Proof. The first claim is clear. The second and third are immediate consequences of Lemmas 2.17 and 2.18, respectively. We check the forth claim. Let C be as in Lemma 2.17 if $n<\infty$ and as in Lemma 2.18 otherwise.

Since $\{a,a^{-1},b,b^{-1}\}$ generate $\mathbb{Z}[G_{m,n}/G'_{m,n}]$ as a ring and C generates $G'_{m,n}/G''_{m,n}$ as a $\mathbb{Z}$-module, it is enough to check that for every $\bar{c}_{i,j}\in C$,

$$\pi(a\bar{c}_{i,j}a^{-1})=x^{i+1}y^j \text{ and } \pi(b\bar{c}_{i,j}b^{-1})=x^iy^{j+1}.$$

Indeed, for every $\bar{c}_{i,j} \in C$ the following holds:

- If $0 \leqslant i \leqslant m-3$ then $a\bar{c}_{i,j}a^{-1} = \bar{c}_{i+1,j}$ and $\pi(\bar{c}_{i+1,j}) = x^{i+1}y^j$.
- If $i = m-2$ then $a\bar{c}_{m-2,j}a^{-1} = \bar{c}_{m-1,j} = (\bar{c}_{0,j})^{-1}\cdots(\bar{c}_{m-2,j})^{-1}$ and
$$\pi\left((\bar{c}_{0,j})^{-1}\dots(\bar{c}_{m-2,j})^{-1}\right) = -y^j - \cdots - x^{m-2}y^j = x^{m-1}y^j.$$
- If $0 \leqslant j \leqslant n-3 < \infty$ then $b\bar{c}_{i,j}b^{-1} = \bar{c}_{i,j+1}$ and $\pi(\bar{c}_{i,j+1}) = x^i y^{j+1}$.
- If $j = n-2 < \infty$ then $b\bar{c}_{i,n-2}b^{-1} = \bar{c}_{i,n-1} = (\bar{c}_{i,0})^{-1}\cdots(\bar{c}_{i,n-2})^{-1}$ and
$$\pi\left((\bar{c}_{i,0})^{-1}\cdots(\bar{c}_{i,n-2})^{-1}\right) = -x^i - \ldots - x^i y^{n-2} = x^i y^{n-1}.$$
- If $j \in \mathbb{Z}$ and $n = \infty$ then $b\bar{c}_{i,j}b^{-1} = \bar{c}_{i,j+1}$ and $\pi(\bar{c}_{i,j+1}) = x^i y^{j+1}$.

□

Lemma 2.22. *Let Γ be a finitely generated group and let $x, y \in \widehat{\Gamma}$. If $d := [x,y] \in \Gamma$ then $d \in \Gamma'$.*

Proof. Assume otherwise. The structure theorem of finitely generated abelian groups implies that every such group is residually finite. Since Γ/Γ' is a finitely generated abelian group and $d \notin \Gamma'$, there exists a finite abelian quotient Δ of Γ such that the image of d in Δ is not trivial. Let Λ be a normal finite index subgroup of Γ such that $\Delta = \Gamma/\Lambda$. Let $\overline{\Lambda}$ be the closure of Λ in $\widehat{\Gamma}$. Then $\widehat{\Gamma}/\overline{\Lambda} \simeq \Gamma/\Lambda$ is an abelian group so $d = [x,y] \in \overline{\Lambda}$. On the other hand, since $\overline{\Lambda} \cap \Gamma = \Lambda$, $d \notin \overline{\Lambda}$, a contradiction. □

Lemma 2.23. *Under Notations 2.13 and 2.19, let $d \in G_{m,n}$ be a commutator of a pair of profinite generators of $\widehat{G}_{m,n}$. Denote the normal subgroup of $G_{m,n}$ generated by d by D. Then $DG''_{m,n} = G'_{m,n}$.*

In particular, $\pi(d)$ is an invertible element of the ring $S_{m,n}$ where π is as in Corollary 2.21.

Proof. Denote $c := c_{0,0}$. Assume that $DG''_{m,n}$ is properly contained in $G'_{m,n}$. Since c normally generates $G'_{m,n}$, $c \notin DG''_{m,n}$. We will show that there exists a finite index normal subgroup L of $G_{m,n}$ such that $d \in L$ but $c \notin L$. Then $G_{m,n}/L$ is not abelian. Let $\overline{L}$ be the closure of L in $\widehat{G}_{m,n}$, then $G_{m,n}/L \simeq \widehat{G}_{m,n}/\overline{L}$ so $\widehat{G}_{m,n}/\overline{L}$ is not abelian. On the other hand, $d \in \overline{L}$ and the conjugacy class of d in $\widehat{G}_{m,n}$ topologically generates $(\widehat{G}_{m,n})'$. Thus $\widehat{G}_{m,n}/\overline{L}$ must be abelian, a contradiction.

Let π be as in Corollary 2.21. Denote $I := \pi(D)$. Then I is a proper $R_{m,n}$-submodule of $S_{m,n}$ and thus a proper ideal of the ring $S_{m,n}$ (see Remark 2.20). Since every finitely generated ring is residually finite (cf. **[16]**) and $\pi(c) \notin I$, there exists an ideal $J \supseteq I$ such that $S_{m,n}/J$ is finite and $\pi(c) \notin J$. Remark 2.20 implies that J is an $R_{m,n}$-submodule of $S_{m,n}$. Thus, there exists a normal subgroup K of $G_{m,n}$ which contains $G''_{m,n}$ such that $K/G''_{m,n} = \pi^{-1}(J)$. Then $d \in K$ and $c \notin K$.

If $n < \infty$ then

$$[G_{m,n} : K] = [G_{m,n} : G'_{m,n}][G'_{m,n} : K] = mn[G'_{m,n} : K] < \infty$$

so we can take $L := K$.

Assume that $n = \infty$. If $H \leqslant G$ are groups and M is a normal subgroup of G then $[G : H] \leqslant [G : MH]|M|$. Since $O(a) = m < \infty$,

$$[G_{m,n}/K : \langle b\rangle K/K] \leqslant [G_{m,n}/K, \langle b\rangle G'_{m,n}/K][G'_{m,n} : K] = m[G'_{m,n} : K] < \infty.$$

If a finitely generated group Γ has a finite index residually finite subgrup, then Γ itself is residually finite. Since $\langle b\rangle K/K$ is an infinite cyclic group, $G_{m,n}/K$ is residually finite. Hence, there exists a normal subgroup L of $G_{m,n}$ such that $L \supseteq K$, $G_{m,n}/L$ is finite and $c \notin L$. Clearly, $d \in K \subseteq L$.

The "in particular" part follows since $\pi(D)$ is the ideal of $S_{m,n}$ generated by $\pi(d)$.

□

Corollary 2.24. *Under Notations 2.13 and 2.19, assume that* $(m,n) = (3,3)$. *Let* r *be a non-zero integer and denote* $h_1 := (ab)^{3r}$, $h_2 := (ba)^{3r}$ *and* $h_3 := (b^2a^2)^{3r}$. *Then non of* h_1, h_2 *and* h_3 *is a commutator of profinite generators of* $\widehat{G}_{3,3}$.

Proof. Since $ba = a^{-1}(ab)a$ and $b^2a^2 = (ab)^{-1}$, it is enough to prove the claim with respect to $h_1 = (ab)^3$. Let π be as in Lemma 2.21. It is enough to prove that for every $1 \leqslant i \leqslant 3$, $\pi(h_1^{3r})$ is not invertible in $S_{3,3}$. Since

$$(ab)^3 = [a,b]a^2[a,b]a^{-2}(a^2b^2)[a,b](a^2b^2)^{-1},$$

$\pi((ab)^{3r}) = r(1+x^2+x^2y^2)$. The claim follows since $1+x^2+x^2y^2$ is in the kernel of the homomorphism $\eta : S_{3,3} \to \mathbb{Z}/3\mathbb{Z}$ defined by $\eta(x) = \eta(y) = 1$. □

Lemma 2.25. *Let* $(m,n) \in \{(2,3),(2,\infty),(3,3),(3,\infty)\}$. *The invertible elements in* $S_{m,n}$ *are the elements of the form* $\pm x^i y^j$.

Proof. Denote $T = \mathbb{Z}[X,X^{-1}]/\psi_m(X)$. Then $S_{m,n} \simeq T[Y,Y^{-1}]/(\psi_n(Y))$. If $m = 2$ then $\psi_m(X) = X+1$ so $T \simeq \mathbb{Z}$ while if $m = 3$ then $\psi_m(X) = X^2+X+1$ so T is isomorphic to the ring of Eisenstein integers $\mathbb{Z}[\xi]$ where $\xi = \frac{-1+\sqrt{-3}}{2}$ is a primitive third root of unity.

If $(m,n) = (2,3)$ then $S_{m,n} \simeq \mathbb{Z}[Y,Y^{-1}]/(\psi_n(Y)) \simeq \mathbb{Z}[\xi]$ where the isomorphism from $S_{m,n}$ to $Z[\xi]$ sends x to -1 and y to ξ. The claim follows since the invertible elements in the Eisenstein integers are the elements of the from $\pm\xi^j$.

If $(m,n) = (2,\infty)$ then $S_{m,n} \simeq \mathbb{Z}[Y,Y^{-1}]/(\psi_n(Y)) \simeq \mathbb{Z}[Y,Y^{-1}]$ where the isomorphism from $S_{m,n}$ to $Z[Y,Y^{-1}]$ sends x to -1 and y to Y. The claim follows since the invertible elements $\mathbb{Z}[Y,Y^{-1}]$ are the elements of the from $\pm Y^j$.

If $(m,n) = (3,\infty)$ then $S_{m,n} \simeq \mathbb{Z}[\xi][Y,Y^{-1}]/(\psi_n(Y)) \simeq \mathbb{Z}[\xi][Y,Y^{-1}]$ where the isomorphism from $S_{m,n}$ to $\mathbb{Z}[\xi]$ sends x to ξ and y to Y. The claim follows since the invertible elements $\mathbb{Z}[\xi][Y,Y^{-1}]$ are the elements of the from $\pm\xi^i Y^j$.

We are left with the case $(m,n) = (3,3)$. In this case $T \simeq \mathbb{Z}[\xi]$ and

$$S_{3,3} = \mathbb{Z}[X,X^{-1},Y,Y^{-1}]/(\psi_3(X),\psi_3(Y)) \simeq \mathbb{Z}[\xi][Y,Y^{-1}]/(\psi_3(Y)).$$

Since $x^3 = 1$ and $y^3 = 1$, every element of the from $\pm x^i y^j$ is invertible in $S_{3,3}$ and there are 18 such elements. Thus, it is enough to prove that there are at most 18 invertible elements in $Z[\xi][Y,Y^{-1}]/(\psi_3(Y))$. The ring $\mathbb{Z}[\xi]$ is a unique factorization domain, $Y-\xi, Y-\xi^{-1} \in \mathbb{Z}[\xi][Y]$ are coprime and $\psi_3(Y) = Y^2+Y+1 = (Y-\xi)(Y-\xi^{-1})$, hence, the map $Y \mapsto (\xi,\xi^{-1})$ induces an injective homomorphism of rings

$$\phi : \mathbb{Z}[\xi][Y,Y^{-1}]/(\psi_3(Y)) \to \mathbb{Z}[\xi] \times \mathbb{Z}[\xi].$$

The restriction of ϕ to the set of invertible elements is an injective homomorphism of the groups of invertible elements

$$\phi^* : \big(\mathbb{Z}[\xi][Y,Y^{-1}]/(\psi_3(Y))\big)^* \to \mathbb{Z}[\xi]^* \times \mathbb{Z}[\xi]^*.$$

Since $\mathbb{Z}[\xi]^* \times \mathbb{Z}[\xi]^*$ contains 36 elements and the image of ϕ^* is a subgroup of $\mathbb{Z}[\xi]^* \times \mathbb{Z}[\xi]^*$, it is enough to show that ϕ^* is not onto. We claim that $(1, -\xi^{-1})$ in not in the image of ϕ and thus not in the image of ϕ^*. Every element of $\mathbb{Z}[\xi][Y, Y^{-1}]/(\psi_3(Y))$ is of the form $a + bY + (\psi_3(Y))$ where $a, b \in \mathbb{Z}[\xi]$ and

$$\phi^*(a + bY + (\psi_3(Y))) = (a + b\xi, a + b\xi^{-1}).$$

Thus, if $(1, -\xi^{-1})$ was in the image of ϕ, then there would have been $a, b \in \mathbb{Z}[\xi]$ such that

$$a + b\xi = 1\ ,\ a + b\xi^{-1} = -\xi^{-1}.$$

This is impossible since then

$$a = \frac{1+\xi}{1-\xi^2} = \frac{1}{1-\xi} \notin \mathbb{Z}[\xi].$$

□

Proof of Proposition 2.15.

Lemma 2.21 implies that there is an isomorphism π from $G'_{m,n}/G''_{m,n}$ to the additive group of $S_{m,n}$ and that the images under π of the conjugates of $[a, b]^{\pm 1}$ are the elements of the from $\pm x^i y^j$. Lemma 2.25 implies that the invertible elements in the ring $S_{m,n}$ are elements of the from $\pm x^i y^j$. Finally, Lemmas 2.22 and 2.23 imply that if $d \in G_{m,n}$ is a commutator of topological generators of $\widehat{G}_{m,n}$ then $d \in G'_{m,n}$ and $\pi(d)$ in invertible in $S_{m,n}$. □

2.3. Trace computations.

In this section we define a specific embedding of $G_{m,n}$ in $PSL_2(\mathbb{Z})$ and show that under this embedding there are only finitely many possible values for the trace of an element $d \in G_{m,n}$ which is a commutator of profinite generators of $\widehat{G}_{m,n}$.

Notation 2.26. Recall that

$$U := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } V := \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

For every $(m, n) \in \{(2,3), (2,\infty), (3,3), (3,\infty)\}$ denote:

(n, m)	A	B	$C := [A, B]$
$(2,3)$	$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$V = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$
$(2,\infty)$	$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$VUV = \begin{bmatrix} 0 & 1 \\ -1 & -2 \end{bmatrix}$	$\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$
$(3,3)$	$V = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$	$UVU^3 = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$
$(3,\infty)$	$V = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$	$(UV)^3U = \begin{bmatrix} -3 & 1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & -4 \\ -4 & 17 \end{bmatrix}$

Finally, for every $(m, n) \in \{(2,3), (2,\infty), (3,3), (3,\infty)\}$, let a, b, c be the images of A, B, C in $\mathrm{PSL}_2(\mathbb{Z})$ and denote $G_{m,n} := \langle a, b\rangle$. Then for every $(m, n) \in \{(2,3), (2,\infty), (3,3), (3,\infty)\}$, $o(a) = m$, $o(b) = n$ and Lemma 2.43 below implies that $G_{m,n}$ is the free product of $\langle a\rangle$ and $\langle b\rangle$ so the notation defined here is consistent with Notation 2.13.

Lemma 2.27. *Under Notation 2.26, for every odd prime p, $G_{m,n}$ projects onto $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof. If $(m, n) = (2,3)$, then $G_{m,n} = \mathrm{PSL}_2(\mathbb{Z})$ and the claim is clear. Assume $(m, n) \neq (2,3)$. Gauss elimination implies that for every prime p, $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is generated by

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

If follows that p is odd, then for every $r, s \in \mathbb{Z}$, the group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is generated by

$$\begin{bmatrix} 1 & \pm 2^r \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ \pm 2^s & 1 \end{bmatrix}.$$

The result follows the following computations:

(1) If $(m, n) = (2,\infty)$ then

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ and } A^2BA^{-1} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}.$$

(2) If $(m, n) = (3,3)$ then

$$AB = \begin{bmatrix} -1 & 0 \\ 2 & -1 \end{bmatrix} \text{ and } BA = \begin{bmatrix} -1 & -2 \\ 0 & -1 \end{bmatrix}.$$

(3) If $(m, n) = (3,\infty)$ then

$$BA = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \text{ and } AB = \begin{bmatrix} 1 & 0 \\ -4 & 1 \end{bmatrix}.$$

□

The following lemma is well known and is proved only for the convenience of the reader:

Lemma 2.28. *Let* $\mathfrak{p}$ *be an odd prime. Then the exact sequence*

$$1 \to \{\pm 1\} \to \mathrm{SL}_2(\mathbb{Z}/\mathfrak{p}\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/\mathfrak{p}\mathbb{Z}) \to 1$$

does not split

Proof. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which projects onto $\mathrm{PSL}_2(\mathbb{Z})$. Then there exists $\epsilon = \pm 1$ such that

$$\begin{bmatrix} \epsilon & 1 \\ 0 & \epsilon \end{bmatrix} \in \Gamma \text{ so } \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \epsilon & 1 \\ 0 & \epsilon \end{bmatrix}^2 \in \Gamma.$$

Similarly, $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \in \Gamma$ so $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. □

Definition 2.29. The projection map $\rho : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$ induces an epimorphosm $\hat{\rho} : \widehat{\mathrm{SL}_2(\mathbb{Z})} \to \widehat{\mathrm{PSL}_2(\mathbb{Z})}$ and $\ker \rho = \ker \hat{\rho} = \{\pm \mathrm{I}_2\}$. Since $-\mathrm{I}_2 \notin \widehat{\mathrm{SL}_2(\mathbb{Z})}'$, the restriction of $\hat{\rho}$ to $\widehat{\mathrm{SL}_2(\mathbb{Z})}'$ is an isomorphism from $\widehat{\mathrm{SL}_2(\mathbb{Z})}'$ onto $\widehat{\mathrm{PSL}_2(\mathbb{Z})}'$. We refer to the inverse of this isomorphism as the commutator subgroup section and denote it by $\mathrm{css} : \widehat{\mathrm{PSL}_2(\mathbb{Z})}' \to \widehat{\mathrm{SL}_2(\mathbb{Z})}'$. Note that $\mathrm{css}(\mathrm{PSL}_2(\mathbb{Z})') = (\mathrm{SL}_2(\mathbb{Z}))'$.

Since $\ker \hat{\rho}$ is central in $\widehat{\mathrm{SL}_2(\mathbb{Z})}$, for every $\mathsf{x}, \mathsf{y} \in \widehat{\mathrm{PSL}_2(\mathbb{Z})}$ and every lifts $\mathsf{X}, \mathsf{Y} \in \mathrm{SL}_2(\mathbb{Z})$ of x and y to $\widehat{\mathrm{SL}_2(\mathbb{Z})}$, $\mathrm{css}([\mathsf{x}, \mathsf{y}]) = [\mathsf{X}, \mathsf{Y}]$.

Lemma 2.30. *Under Notation 2.26, if* $\mathsf{d} \in \mathsf{G}_{m,n}$ *is the commutator of a pair of profinite generators of* $\widehat{\mathsf{G}}_{m,n}$ *then there exists* $k \geqslant 0$ *such that* $\mathrm{Tr}(\mathrm{css}(\mathsf{d})) = 2 \pm 2^k$.

Proof. Since a homomorphism between groups induces a homomorphism between their profinite completions, we have the following commutative squares:

$$\begin{array}{ccc} \langle \mathsf{A}, \mathsf{B} \rangle & \xrightarrow{\alpha} & \mathrm{SL}_2(\mathbb{Z}) \\ \downarrow \psi & & \downarrow \rho \\ \mathsf{G}_{m,n} & \xrightarrow{\beta} & \mathrm{PSL}_2(\mathbb{Z}) \end{array} \quad \text{and} \quad \begin{array}{ccc} \widehat{\langle \mathsf{A}, \mathsf{B} \rangle} & \xrightarrow{\hat{\alpha}} & \widehat{\mathrm{SL}_2(\mathbb{Z})} \\ \downarrow \hat{\psi} & & \downarrow \hat{\rho} \\ \widehat{\mathsf{G}_{m,n}} & \xrightarrow{\hat{\beta}} & \widehat{\mathrm{PSL}_2(\mathbb{Z})} \end{array}$$

where ρ, ψ, $\hat{\rho}$ and $\hat{\psi}$ are epimorphisms, α and β are inclusions and $\ker \rho = \ker \hat{\rho} = \{\pm 1\}$.

Assume that x, y are topological generators of $\widehat{\mathsf{G}_{m,n}}$ such that $[\mathsf{x}, \mathsf{y}] = \mathsf{d}$. Let $\mathsf{X}, \mathsf{Y} \in \widehat{\mathrm{SL}_2(\mathbb{Z})}$ be lifts of $\hat{\beta}(\mathsf{x})$ and $\hat{\beta}(\mathsf{y})$ to $\widehat{\mathrm{SL}_2(\mathbb{Z})}$. Then

$$[\mathsf{X}, \mathsf{Y}] = \mathrm{css}([\hat{\beta}(\mathsf{y}), \hat{\beta}(\mathsf{y})]) = \mathrm{css}(\hat{\beta}([\mathsf{x}, \mathsf{y}])) = \mathrm{css}(\beta(\mathsf{d})) = \mathrm{css}(\mathsf{d}) \in \mathrm{SL}_n(\mathbb{Z})'.$$

Thus, we have to show that $\mathrm{Tr}[\mathsf{X}, \mathsf{Y}] = 2 \pm 2^k$.

For every odd prime $\mathfrak{p}$, let $\pi_\mathfrak{p} : \widehat{\mathrm{SL}_2(\mathbb{Z})} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/\mathfrak{p}\mathbb{Z})$ and $\bar{\pi}_\mathfrak{p} : \widehat{\mathrm{PSL}_2(\mathbb{Z})} \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}/\mathfrak{p}\mathbb{Z})$ be the modulo-$\mathfrak{p}$ homomorphisms. Lemma 2.27 implies that

$$\mathrm{PSL}_2(\mathbb{Z}/\mathfrak{p}\mathbb{Z}) = (\bar{\pi}_\mathfrak{p} \circ \beta)(\mathsf{G}_{m,n}) = (\bar{\pi}_\mathfrak{p} \circ \hat{\beta})(\langle \mathsf{x}, \mathsf{y} \rangle) = (\bar{\pi}_\mathfrak{p} \circ \hat{\rho})(\langle \mathsf{X}, \mathsf{Y} \rangle).$$

Since the sequence

$$1 \to \{\pm 1\} \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1$$

does not split, $\pi_p(\langle X, Y\rangle) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. The result follows from the fact that for an odd prime p, the trace of the commutator of two generators of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ cannot be equal to 2 (see, for example, Lemma 3 of **[12]**). □

Claim 2.31. Let $k \in \mathbb{Z}$, $X := \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ and $Y := \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$. Then

$$[X, YXY^{-1}] = \begin{bmatrix} 1-k^2+k^4 & k^3 \\ k^3 & 1+k^2 \end{bmatrix} \equiv \begin{bmatrix} 1-k^2 & 0 \\ 0 & 1+k^2 \end{bmatrix} \pmod{k^3}.$$

Lemma 2.32. *Let H be a group which is generated by two elements h_1, h_2 and $o(h_1) = m < \infty$. Then:*

(1) $H' \subseteq N := \langle h_1^i (h_1 h_2) h_1^{-i} \mid 0 \leqslant i \leqslant m-1 \rangle$.
(2) *If h_1^2 is central in H, then H'' is contained in the subgroup generated by H-conjugates of $[h_1^2 h_2 h_1^{-1}, h_1 h_2]$.*
(3) *If h_1^3 is central in H, H'' is contained in the subgroup generated by H-conjugates of $[h_2 h_1, h_1 (h_2 h_1) h_1^{-1}]$.*

Proof. We start by proving the first claim. Note that for every k, $h_1^k N h_1^{-k} = N$. Therefore, in order to show that N is normal in H, it is enough to show that $h_2 N h_2^{-1} = N$ and $h_2^{-1} N h_2 = N$. Since $h_1 h_2$ and $h_1^m h_2 h_1^{m-1} = h_2 h_1^{m-1}$ belong to N,

$$h_2 N h_2^{-1} = (h_2 h_1^{m-1}) N (h_2 h_1^{m-1})^{-1} = N \text{ and } h_2^{-1} N h_2 = (h_1 h_2)^{-1} N (h_1 h_2) = N.$$

Since $h_1 N = h_2^{-1} N$, the quotient H/N is cyclic and in particular abelian so $H' \subseteq N$.

We now prove the second claim. Since h_1^2 is central in H, $N = \langle h_1 h_2, h_1^2 h_2 h_1^{-1} \rangle$. Denote $g := [h_1^2 h_2 h_1^{-1}, h_1 h_2]$. Then,

$$H'' \subseteq N' = \langle hgh^{-1} \mid h \in N \rangle \subseteq \langle hgh^{-1} \mid h \in H \rangle.$$

Finally, we prove the third claim. For every k, denote $g_k := h_1^k (h_2 h_1) h_1^{-k}$. Since N contains H', it is enough to prove that N' is contained in the subgroup generated by H-conjugates of $[g_0, g_1]$. Since h_1^3 is central in H, if $k = k' \pmod 3$ then $g_k = g_{k'}$. Since $h_1^{-1}(h_1 h_2) h_1 = h_2 h_1$,

$$N = \langle g_k \mid 0 \leqslant i \leqslant m-1 \rangle = \langle g_0, g_1, g_2 \rangle.$$

Thus N' is the subgroup of N generated by the N-conjugates of the elements $[g_0, g_1]$, $[g_1, g_2]$ and $[g_2, g_0]$. The result follows since $[g_1, g_2] = h_1 [g_0, g_1] h_1^{-1}$ and $[g_2, g_0] = [g_2, g_3] = h_1^2 [g_0, g_1] h_1^{-2}$. □

Lemma 2.33. *Under Notation 2.26,*

(1) *If $(m, n) = (2, 3)$ then the elements of $\langle A, B\rangle''$ are equal to I_2 modulo 2.*
(2) *If $(m, n) = (2, \infty)$ then the elements of $\langle A, B\rangle''$ are equal to I_2 or to $5I_2$ modulo 8.*
(3) *If $(m, n) = (3, 3)$ then the elements of $\langle A, B\rangle''$ are equal to I_2 or to $5I_2$ modulo 8.*
(4) *If $(m, n) = (2, \infty)$ then the elements of $\langle A, B\rangle''$ are equal to I_2 or to $17I_2$ modulo 32.*

Proof.

(1) $SL_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ and $S_3'' = 1$.

(2) Since $o(A) = 4$ and $A^2 = -I_2$, Lemma 2.32 implies that $\langle A, B\rangle''$ is contained in the subgroup generated by $SL_2(\mathbb{Z})$-conjugates of

$$[A^2BA^{-1}, AB] = \begin{bmatrix} 5 & -8 \\ -8 & 13 \end{bmatrix}.$$

The result follows since $5^2 = 1 \pmod 8$.

(3) Since $o(A) = 6$ and $A^3 = -I_2$, Lemma 2.32 implies that $\langle A, B\rangle''$ is contained in the subgroup generated by $SL_2(\mathbb{Z})$-conjugates of $[BA, A(BA)A^{-1}]$. Since $5^2 = 1 \pmod 8$, the result follows from Claim 2.31 with respect to

$$X = BA = \begin{bmatrix} -1 & -2 \\ 0 & -1 \end{bmatrix} \text{ and } Y = A = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

(4) Since $o(A) = 6$ and $A^3 = -I_2$, Lemma 2.32 implies that $\langle A, B\rangle''$ is contained in the subgroup generated by $SL_2(\mathbb{Z})$-conjugates of $[BA, A(BA)A^{-1}]$. Since $(17)^2 = 1 \pmod{32}$, the result follows from Claim 2.31 with respect to

$$X = BA = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \text{ and } Y = A = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

□

Lemma 2.34. *Under Notation 2.26, assume that* $d \in G_{m,n}$ *is the commutator of profinite generators of* $\widehat{G}_{m,n}$. *Then the possible values for* $\mathrm{Tr}(\mathrm{css}(d))$ *are given in Table 1.*

(n, m)	C	λ	l	$\mathrm{Tr}(\mathrm{css}(d))$
$(2, 3)$	$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$	1	2	1 *or* 3
$(2, \infty)$	$\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$	1 *or* 5	8	-2 *or* 6
$(3, 3)$	$\begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$	1 *or* 5	8	-2 *or* 6
$(3, \infty)$	$\begin{bmatrix} 1 & -4 \\ -4 & 17 \end{bmatrix}$	1 *or* 17	32	-14 *or* 18

TABLE 1. Possible values of $\mathrm{Tr}(\mathrm{css}(d))$

Proof. Lemma 2.15 implies that the images of $c = [a, b]$ and d in $G_{m,n}/G''_{m,n}$ are conjugates so there exist $r \in G_{m,n}$ and $s \in G''_{m,n}$ such that $d = rcr^{-1}s$. Let A, B and C be as in Notation 2.26. Let R be a lift of r to $SL_2(\mathbb{Z})$ so $\operatorname{css}(c) = [A, B] = C$ and

$$\operatorname{css}(d) = RCR^{-1} \operatorname{css}(s) \in SL_2(\mathbb{Z})'.$$

Lemma 2.33 implies that $\operatorname{Tr}(\operatorname{css}(d)) = \lambda \operatorname{Tr}(C) \pmod{l}$ where C, the value of l and the possible values of λ are given in Table 1.

Lemma 2.30 implies that there exists $k \in \mathbb{N}$ such that $\operatorname{Tr}(\operatorname{css}(d)) = 2 \pm 2^k$. Hence, the only possible values for $\operatorname{Tr}(\operatorname{css}(d))$ are the values written in the right column of Table 1.

□

2.4. Proof of Proposition 2.6.

The goal of this section is to complete the proof of Proposition 2.6.

Definition 2.35. The trace of an element $g \in PSL_2(\mathbb{Z})$, denoted by $|\operatorname{Tr} g|$, is the absolute value of the trace of its lifts to $SL_2(\mathbb{Z})$.

Let $d \in G_{m,n}$ be a commutator of a pair of topological generating set of $\widehat{G}_{m,n}$. Lemma 2.34 gives the possible values of the trace of d. We will describe an algorithm such that for a given t, the algorithm computes a representatives set to the finitely many $G_{m,n}$-conjugacy classes of trace t. By applying this algorithm to the finitely many possible values of the trace of d, we will get a finite list of elements such that d is $G_{m,n}$-conjugate to one of them. Then we will show that for every element in this list which in not a commutator, there exists a finite quotient in which this element is not a commutator,

Definition 2.36. Let $G = \langle a \rangle * \langle b \rangle$ where $o(a) = m$ and $o(b) = n$. If $m < \infty$ define $L_a := \{a\}$, otherwise, define $L_a := \{a, a^{-1}\}$. Define L_b similarly. An $L_{a,b}$-word is a finite sequence of elements of $L_{a,b} =: L_a \cup L_b$ (including the empty sequence). The set of $L_{a,b}$-words is denote by $W_{a,b}$. If w is a word then its length is denote by $l(w)$. We say that a word $(x_1, \ldots, x_k) \in W_{a,b}$ represents the element $g \in G_{m,n}$ if $g = x_1 \cdots x_k$ (the empty word represents the identity element). If w_1 and w_2 are words, then $w_1 w_2$ denotes their concatenation.

We recall some standard definitions and facts about $L_{a,b}$-words.

(1) An $L_{a,b}$-word is called reduced if the following two conditions hold:
   (a) If $m < \infty$ then there are no m consecutive appearances of a and if $n < \infty$ then there are no n consecutive appearances of b.
   (b) If $m = \infty$ then there are no consecutive appearances of the from a, a^{-1} or a^{-1}, a and if $n = \infty$ then there are no consecutive appearances of the from b, b^{-1} or b^{-1}, b.

(2) For every $g \in G$ there exists a unique reduced word which represents g.

(3) An $L_{a,b}$-word is called cyclically reduced if every cyclic permutation of it is reduced.

(4) (a) If z is a reduced word which represents an element g we denote by z^{-1} the reduced word which represents g^{-1}.
   (b) For every conjugacy class C of G there exists a cyclically reduced word w, unique up to cyclic permutation, such that every element of C is

represented by a reduced word of the form $zw'z^{-1}$ where w' is a cyclic permutation of w and z is a reduced word. In particular, the only elements of C which are represented by a cyclically reduced word are the elements which are represented by a cyclic permutation of w.

We recall the description of the conjugacy classes of $PSL_2(\mathbb{Z})$ with a given trace. The following two Lemmas are well known. We sketch the proofs only for the convenience of the reader.

Lemma 2.37. (1) *If* $g \in PSL_2(\mathbb{Z})$ *and* $|\operatorname{Tr} g| = 0$ *then* g *is conjugate to* u.
(2) *If* $g \in PSL_2(\mathbb{Z})$ *and* $|\operatorname{Tr} g| = 1$ *then* g *is conjugate to* v *or to* v^2.
(3) *If* $g \in PSL_2(\mathbb{Z})$ *and* $|\operatorname{Tr} g| = 2$ *then* g *is conjugate to* $(uv)^r$ *for some* $r \in \mathbb{Z}$.

Proof.
1. Let $g \in PSL_2(\mathbb{Z})$ with $|\operatorname{Tr} g| = 0$. Then g can be lifted to an element $\tilde{g} \in SL_2(\mathbb{Z})$. The characteristic polynomial of $\tilde{g}$ is $T^2 + 1$ so $g^2 = 1$. Every element of order 2 in the free product $PSL_2(\mathbb{Z}) = \langle u \rangle * \langle v \rangle$ is conjugate to u.

2. Let $g \in PSL_2(\mathbb{Z})$ with $|\operatorname{Tr} g| = 1$. Then g can be lifted to an element $\tilde{g} \in SL_2(\mathbb{Z})$ with $\operatorname{Tr} \tilde{g} = -1$. The characteristic polynomial of $\tilde{g}$ is $T^2 + T + 1 = \frac{T^3-1}{T-1}$ so $g^3 = 1$. Every element of order 3 in the free product $PSL_2(\mathbb{Z}) = \langle u \rangle * \langle v \rangle$ is conjugate either to v or to v^2.

3. Let $g \in PSL_2(\mathbb{Z})$ with $|\operatorname{Tr} g| = 2$. Then g can be lifted to an element $\tilde{g} \in SL_2(\mathbb{Z})$ with $\operatorname{Tr} \tilde{g} = 2$. The characteristic polynomial of $\tilde{g}$ is $(T-1)^2$ so 1 is the only eigenvalue of $\tilde{g}$. Let $z \in \mathbb{Z}^2$ be a primitive eigenvector of $\tilde{g}$. Let $h \in SL_2(\mathbb{Z})$ be an element whose left column is z. There exists $0 \neq r \in \mathbb{Z}$ such that $h^{-1}\tilde{g}h = \left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right] = (-UV)^r$. □

Lemma 2.38. *Let* C *be a* $PSL_2(\mathbb{Z})$*-conjugacy class of trace* $|t| \geqslant 3$. *Then there exists* $g \in C$ *and* $s_1, \ldots, s_k \in \{1, 2\}$ *such that* $g = uv^{s_1}uv^{s_2} \ldots uv^{s_k}$.

Proof. The elements of C have infinite order so $u, v, v^2 \notin C$. Take $g \in C$ to be any element such that $w_{u,v}(g)$ is cyclically reduced and starts with u. □

Lemma 2.39. *Under Notation 2.26, assume that* $\{s_1, \ldots, s_k\} = \{1, 2\}$. *Then* $|\operatorname{Tr}(uv^{s_1} \ldots uv^{s_k})| \geqslant k$.

Proof. It is enough to prove the claim when $s_1 = 1$. Let U, V be as in Notation 2.26. Denote

$$R := -UV = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} S := -UV^2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Note that

$$R^{m_1}S^{m_2} = \begin{bmatrix} 1 + m_1m_2 & m_1 \\ m_2 & 1 \end{bmatrix}$$

so $\operatorname{Tr}(R^{m_1}S^{m_2}) = 2 + m_1m_2 \geqslant m_1 + m_2$ and all the entries of $R^{m_1}S^{m_2}$ are positive. A simple induction argument shows that for every $k \geqslant 2$ and every sequence $m_1, \ldots, m_k$ of positive integers all the entries of the product $R^{m_1}S^{m_2}R^{m_3}S^{m_4} \cdots$ are positive and

$$\operatorname{Tr}(R^{m_1}S^{m_2}R^{m_3}S^{m_4} \cdots) \geqslant m_1 + \cdots + m_k.$$

□

Remark 2.40. Under the assumption of Lemma 2.39 it is possible to give a better bound to $|\operatorname{Tr}(uv^{s_1}\dots uv^{s_k})|$. Since the exact bound is not important to us, no attempt was made to make it optimal.

The next step is to find a description of the conjugacy classes in $G_{m,n}$ of a given trace $t \geqslant 3$.

Notation 2.41. Under Notation 2.26, let $(m,n) \in \{(2,\infty),(3,3),(3,\infty)\}$. Then $\langle a\rangle * \langle b\rangle = G_{m,n} \leqslant \mathrm{PSL}_2(\mathbb{Z}) = \langle u\rangle * \langle v\rangle$. We can regard an element $g \in G_{m,n}$ as an element in the free product $\langle a\rangle * \langle b\rangle$ and as an element in the free product $\langle u\rangle * \langle u\rangle$. Thus, g can be represented by a reduced $L_{a,b}$-word $w_{a,b}(g) \in W_{a,b}$ and also by a reduced $L_{u,v}$-word $w_{u,v}(g) \in W_{u,v}$.

Lemma 2.42. *Under Notations 2.26 and 2.41, let* $(m,n) \in \{(2,\infty),(3,3),(3,\infty)\}$. *For every* $g \in G_{m,n}$*:*

(1) $l(w_{u,v}(g)) \geqslant l(w_{a,b}(g))$.
(2) *If* $w_{a,b}(g)$ *starts with* $a^{\pm 1}$ *and ends with* $b^{\pm 1}$ *then* $w_{u,v}(g)$ *is cyclically reduced.*
(3) *Let* C *be a conjugacy class of* $G_{m,n}$ *which does not contain a power of* a *nor a power of* b*. Then there exists* $g \in C$ *such that* $w_{u,v}(g)$ *is cyclic reduced and starts with* u*.*

Proof. If $o(a) < \infty$ denote $I_a := \{0,\dots,o(a)-1\}$, otherwise, denote $I_a := \mathbb{Z}$. Define I_b similarly. The claims easily follow from the following properties:

(a) For every $r \in I_a$ and $s \in I_b$, $l(w_{u,v}(a^r)) \geqslant |r|$ and $l(w_{u,v}(b^s)) \geqslant |s|$.
(b) If $w_{v,u}(a)$ starts with u then $w_{v,u}(b)$ starts with v.
(c) If $w_{v,u}(a)$ starts with v then $w_{v,u}(b)$ starts with u.
(d) For every $0 \neq r \in I_a$, the first and last letters of $w_{u,v}(a)$ and $w_{u,v}(a^r)$ are all equal.
(e) For every $0 \neq s \in I_b$, the first and last letters of $w_{u,v}(b)$ and $w_{u,v}(b^s)$ are all equal.
(f) For every $r \in I_a$ and $s \in I_b$, the words $w_{u,v}(a^r)w_{u,v}(b^s)$ and $w_{u,v}(b^s)w_{u,v}(a^r)$ are reduced.

□

The proof of Lemma 2.42 also implies:

Lemma 2.43. *Under Notation 2.26,* $G_{m,n}$ *is a free product of* $\langle a\rangle$ *and* $\langle b\rangle$*.*

Algorithm 2.44. Fix $(m,n) \in \{(2,3),(2,\infty),(3,3),(3,\infty)\}$ and $3 \leqslant t \in \mathbb{N}$. Use the following steps to find a finite subset of $G_{m,n}$ with a non-empty intersection with every $G_{m,n}$-conjugacy class of elements with trace t.

(1) Apply Lemmas 2.37, 2.38 and 2.39 to find a finite set $\{g_1,\dots,g_k\} \subseteq \mathrm{PSL}_2(\mathbb{Z})$ such that:
   (a) $\{g_1,\dots,g_k\}$ contains a representative of every $\mathrm{PSL}_2(\mathbb{Z})$-conjugacy class of trace $|t|$.
   (b) $w_{u,v}(g_1),\dots,w_{u,v}(g_k)$ are cyclically reduced.
(2) For every $1 \leqslant i \leqslant k$, let $r_i := l(w_{u,v}(g_i))$ and let $g_{i,1},\dots,g_{i,r_i}$ be such that $w_{u,v}(g_{i,1}),\dots,w_{u,v}(g_{i,r_i})$ are the cyclic permutations of $w_{u,v}(g_i)$. Item (3) of Lemma 2.42 implies that every $G_{m,n}$-conjugacy class of elements of trace t contains an element in $\{g_{i,j} \mid 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant r_i\}$.
(3) Lemma 2.42 implies that for every $g \in G_{m,n}$, $l(w_{a,b}(g)) \leqslant l(w_{u,v}(g))$. For every $1 \leqslant i \leqslant k$, compute $X_i := \{g \in G_{m,n} \mid l(w_{a,b}(g)) \leqslant r_i\}$ and $Y_i := \{g_{i,j} \mid$

$1 \leqslant j \leqslant r_i$ and $g_{i,j} \in X_i\}$. Lemma 2.42 implies that $\cup_{1\leqslant i\leqslant k} Y_i$ contains at least one element of every conjugacy class of $G_{m,n}$ of element of trace t.

Lemma 2.45. *Under Notation 2.26, in the following table, for the given values of* (m,n) *and* t*, the set* R_t *non-trivially intersects every* $G_{m,n}$*-conjugacy class consisting of elements of trace* t*:*

(n,m)	t	R_t	$R_t \cap G'_{m,n}$
$(2,3)$	3	$\{[a,b]\}$	$\{[a,b]\}$
$(2,\infty)$	6	$\{[a,b], ab^3, ab^{-3}, abab^2, ab^{-1}ab^{-2}\}$	$\{[a,b]\}$
$(3,3)$	6	$\{[a,b],[a,b^2]\}$	$\{[a,b],[a,b^2]\}$
$(3,\infty)$	14	$\{b^2a^2, ab^{-2}\}$	$\emptyset$
$(3,\infty)$	18	$\{[a,b],[a,b^{-1}]\}$	$\{[a,b],[a,b^{-1}]\}$

Proof. The set R_t was found by using a computer program which implemented algorithm 2.44. □

Lemma 2.46. *Under Notations 2.26. Let* $d \in G_{m,n}$ *be the commutator of topological generators of* $\widehat{G_{m,n}}$*. If* $(m,n) \in \{(2,\infty),(3,3)\}$ *then* $|\operatorname{Tr} d| \neq 2$*.*

Proof. Assume first that $(m,n) = (2,\infty)$. Lemma 2.22 implies that $d \in G'_{2,\infty}$. Lemmas 2.37 and 2.42 imply that every $g \in G_{2,\infty}$ with trace 2 is conjugate in $G_{2,\infty}$ to b^r or b^{-r} or $(ab)^r$ or $(ab^{-1})^r$ for some $r \geqslant 1$. In particular, such g does not belong to $G'_{2,\infty}$.

Assume that $(m,n) = (3,3)$. Lemma 2.22 implies that $d \in G'_{3,3}$. Lemmas 2.37 and 2.42 imply that every $g \in G_{3,3}$ with trace 2 is conjugate in $G_{3,3}$ to $(ba)^r$ or $(b^2a^2)^r$ for some $r \geqslant 1$. If in addition, $g \in G'_{3,3}$ then r is divisible by 3. Corollary 2.24 implies that such an element g is not a commutator of topological generators of $\widehat{G}_{m,n}$. □

Proof of Proposition 2.6 **.**

Lemma implies that $d \in G'_{m,n}$ and Lemma 2.34 gives the possible values for $|\operatorname{Tr} d|$. Since $\nu, \nu^2 \notin G'_{2,3}$, it follows from Lemma 2.37 that if $(m,n) = (2,3)$ then $|\operatorname{Tr} d| \neq 1$. It follows from Lemma 2.46 that if $(m,n) \in \{(2,\infty),(3,3)\}$ then $|\operatorname{Tr} d| \neq 2$. In all the other cases, it follows from Lemma 2.45 that d is a commutator. □

3. Lifting Solutions

3.1. General D

The three equations that are central to our study are:

($\mathscr{E}_1$) $W(X,Y) = XYX^{-1}Y^{-1} = Z$, with $Z \in \Gamma_D = SL_2(D)$ given and to be solved in X, $Y \in \Gamma_D$. Denote the set of solutions by $\mathscr{C}_Z(D)$.

($\mathscr{E}_2$) $\mathrm{Tr}\,(W(X,Y)) = t$, where $t \in D$ is given, to be solved for $X,\ Y \in \Gamma_D$. Denote by $\mathscr{T}_t(D)$ the set of solutions (X,Y).

($\mathscr{E}_3$) $M(x_1,x_2,x_3) := x_1^2+x_2^2+x_3^2-x_1x_2x_3 = t+2$ for $t \in D$ given, and to be solved for $\mathbf{x} = (x_1,x_2,x_3) \in D^3$. Denote the set of solutions by $\mathscr{M}_{t+2}(D)$.

There are a number of infinite symmetries that the solutions to these equations satisfy and which facilitate their analysis. The first is the action by simultaneous conjugation by Γ_D on the solutions (X,Y) to ($\mathscr{E}_1$) and ($\mathscr{E}_2$).

If $Z' = gZg^{-1}$ for some $Z \in \Gamma_D$, then

$$\mathscr{C}_{Z'}(D) = g\mathscr{C}_Z(D)g^{-1}, \tag{3.1.1}$$

where

$$g[(X,Y)]g^{-1} = (gXg^{-1}, gYg^{-1})\,. \tag{3.1.2}$$

The relation between the solutions to ($\mathscr{E}_1$) for conjugate Z's suggests that we modify the solution set $\mathscr{C}_Z(D)$ of ($\mathscr{E}_1$) to

($\hat{\mathscr{E}}_1$) $\mathrm{COM}_Z(D) := \{(X,Y) \in \Gamma_D \times \Gamma_D \ :\ W(X,Y) \text{ is a conjugate of } Z\}$.

In this way $\mathrm{COM}_Z(D)$ depends only on the conjugacy class of Z, Γ_D acts on $\mathrm{COM}_Z(D)$, and we naturally divide by this action to get equivalence classes $\overline{(X,Y)}$ of solutions to ($\hat{\mathscr{E}}_1$) and whose totality is denoted by

$$\mathrm{COM}_Z(D)/\Gamma_D\ . \tag{3.1.3}$$

If $\mathrm{Tr}(Z) = t$ then $\mathrm{COM}_Z(D) \subset \mathscr{T}_t(D))$, and the action of Γ_D on pairs extends to $\mathscr{T}_t(D)$. Dividing the latter by Γ_D gives classes of solutions, the totality of which is denoted by

$$\mathscr{T}_t(D)/\Gamma_D\ . \tag{3.1.4}$$

So for $\mathrm{Tr}(Z) = t$, we have $\mathrm{COM}_Z(D)/\Gamma_D \subset \mathscr{T}_t(D)/\Gamma_D$.

In what follows we make use of some well known properties of the S-arithmetic groups Γ_D. These are the extensions of the reduction theory of Hermite and Minkowski as developed by Borel [**4**] and algorithmically by Grunewald-Segal in [**10**] and [**11**].

For a given $t \in D$ there are finitely many conjugacy classes in Γ_D represented by $Z_1, ..., Z_h$ say, of trace equal to t. It follows that we have the decomposition

$$\mathscr{T}_t(D) = \bigcup_{j=1}^{h} \mathrm{COM}_{Z_j}(D)\,. \tag{3.1.5}$$

The decomposition respects the Γ_D-action on these sets so that

$$\mathcal{T}_t(D)/\Gamma_D = \bigcup_{j=1}^{h} \left(\mathrm{COM}_{Z_j}(D)/\Gamma_D\right). \tag{3.1.6}$$

There are further symmetries that $\mathrm{COM}_Z(D)$, $\mathcal{T}_t(D)$ and $\mathcal{M}_{t+2}(D)$ carry. These come from the action of outer automorphisms of the free group, that is the Nielsen automorphisms on pairs (X,Y) and which descend to the Markoff group action on $\mathcal{M}_{t+2}(D)$. The Nielsen and Markoff groups are isomorphic (to $\mathrm{PGL}_2(\mathbb{Z})$ in fact) and we denote them here by G with the action on (X,Y) or (x_1,x_2,x_3) being implicit below. These are given explicitly in terms of generators of these groups in the tables in Lemma 3.1.

Denote by π the map from $\mathcal{T}_t(D)$ to $\mathcal{M}_{t+2}(D)$ given by

$$\pi(\,(X,Y)\,) = (\mathrm{Tr}(X), \mathrm{Tr}(Y), \mathrm{Tr}(XY)). \tag{3.1.7}$$

π preserves the Γ_D-classes, and induces a map

$$\pi \,:\, \mathcal{T}_t(D)/\Gamma_D \to \mathcal{M}_{t+2}(D). \tag{3.1.8}$$

The G-actions on $\mathcal{T}_t(D)$ and $\mathcal{M}_{t+2}(D)$ are π equivariant, that is for $g \in G$

$$\pi(\,g(X,Y)\,) = g(\pi(\,(X,Y)\,)). \tag{3.1.9}$$

Dividing $\mathcal{T}_t(D)/\Gamma_D$ and $\mathcal{M}_{t+2}(D)$ by this G-action gives a further collapsing into G-equivalence classes $\mathcal{T}_t(D)/G$ and $\mathcal{M}_{t+2}(D)/G$. Note that G preserves the decompositions (3.1.5) and (3.1.6) so that we retain the decomposition

$$\mathcal{T}_t(D)/G = \bigcup_{j=1}^{h} (\mathrm{COM}_{Z_j}(D)/G), \tag{3.1.10}$$

and

$$\pi \,:\, \mathcal{T}_t(D)/G \to \mathcal{M}_{t+2}(D)/G. \tag{3.1.11}$$

With the set up above we can analyse the relations between the solubility of $(\hat{\mathscr{E}}_1)$, $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$ and decision procedures for them. From the decompositions (3.1.5), (3.1.6) and (3.1.10), and that for a given t, the h classes $Z_1, ..., Z_h$ can be effectively computed ([**11**]), it follows that a decision procedure for $(\mathscr{E}_1)$ gives one for $(\mathscr{E}_2)$. In the other direction, we can certainly decide if a given solution in $\mathcal{T}_t(D)$ lifts to a solution of $(\mathscr{E}_1)$ with a specific Z. This is asking whether in (3.1.5) the given solution (X,Y) is in $\mathrm{COM}_Z(D)$, which is the same as whether $W(X,Y)$ is a conjugate of Z. Again, by [**11**] this can be determined effectively. This however does not allow us to decide $(\mathscr{E}_1)$ from simply having a solution to $(\mathscr{E}_2)$. If the solution at hand lifts to the desired Z one succeeds, but in principle one has to examine infinitely many solutions in $\mathcal{T}_t(D)/G$. If however the latter is finite as is the case for $D = \mathbb{Z}$ (see below), then one can go from a decision procedure for $\mathcal{T}_t(D)$ to $(\mathscr{E}_1)$. In any case, if $\mathcal{T}_t(D)$ is empty then so is $\mathrm{COM}_Z(D)$ for any Z with $\mathrm{Tr}(Z) = t$.

We turn to the question of lifting solutions from $\mathcal{M}_{t+2}(D)$ to $\mathcal{T}_t(D)$ in (3.1.8) and (3.1.11).

In the forward direction, if $\mathcal{M}_{t+2}(D)$ is empty then so is $\mathcal{T}_t(D)$, which is one of the primary ways that we exploit equations $(\mathscr{E}_1)$, $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$. In the other

direction starting with $\mathscr{M}_{t+2}(D)$, the key feature is that the map π in (3.1.8) is finite to one and effectively so. That is given $\mathbf{x} \in \mathscr{M}_{t+2}(D)$, $\pi^{-1}(\mathbf{x}) \in \mathscr{T}_t(D)/\Gamma_D$ is finite and there is an effective procedure to find each point in $\pi^{-1}(\mathbf{x})$, including the case where this set is empty. To see this let V be the 8-dimensional vector space over F (the number field from which our D is taken) of pairs (A, B) of 2×2 matrices. Then $SL_2(F)$ acts linearly via the diagonal conjugation representation $\rho(g) : (A, B) \mapsto (gAg^{-1}, gBg^{-1})$. We are primarily interested in Zariski closed orbits of this action. ρ preserves $\det(A)$, $\det(B)$, $\mathrm{Tr}(A)$, $\mathrm{Tr}(B)$ and $\mathrm{Tr}(AB)$, and these generate the ring of ρ-invariants.

Fixing the values $\det(A) = 1$, $\det(B) = 1$, $\mathrm{Tr}(A) = x_1$, $\mathrm{Tr}(B) = x_2$ and $\mathrm{Tr}(AB) = x_3$, with $x_1, x_2, x_3 \in D$, defines a homogeneous affine variety $X \subset V$ corresponding to an orbit of a F point (see Prop. 3.3). X is defined over F and we seek the points in $X(D)$. By [**4**], $X(D)$ consists of finitely many $\rho(SL_2(D))$ orbits, and by [**11**] these can be determined effectively. Thus, for any $\mathbf{x} \in \mathscr{M}_{t+2}(D)$ the lifts of $\mathbf{x}$ to $\mathscr{T}_t(D)/\Gamma_D$, that is $\pi^{-1}(\mathbf{x})$ are finite in number and effectively so.

In the case that $\mathscr{M}_{t+2}(D)/G$ is finite (and effectively so), the above shows that $\mathscr{T}_t(D)/G$ is also finite and so is $\mathrm{COM}_Z(D)/G$. So in this case $(\mathscr{E}_1)$, $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$ are all effectively decidable. When D has infinitely many units, $\mathscr{M}_k(D)/G$ is not necessarily finite and our analysis here falls short of giving a decision procedure for all three.

3.1.1. *An explicit analysis*

For matrices X and Y in $\Gamma_D = SL_2(D)$, for any ring D (or field F), we consider the tuple (X, Y) with commutator $W(X, Y) = Z$. Putting $t = \mathrm{Tr}\, Z$, $x_1 = \mathrm{Tr}\, X$, $x_2 = \mathrm{Tr}\, Y$ and $x_3 = \mathrm{Tr}\, XY$, for $\mathbf{x} = (x_1, x_2, x_3)$ on the Markoff surface $\mathscr{M}_{t+2}(D)$ in $(\mathscr{E}_3)$, we have double sign-changes, permutations and the (non-linear) Vieta maps as invariant actions. The double sign-changes are easily lifted from $(\mathscr{E}_3)$ to $(\mathscr{E}_1)$, corresponding to the three maps $(X, Y) \mapsto (-X, Y)$, $(X, Y) \mapsto (X, -Y)$ and $(X, Y) \mapsto (-X, -Y)$, preserving $W(*, *) = Z$. The six permutations and three Vieta maps of the x_i are less trivial, but lift if we identify commutators with their inverses, as follows:

Lemma 3.1. *The first table gives the permutations of the subscripts of* (x_1, x_2, x_3) *in* $(\mathscr{E}_3)$*, the corresponding action on* $(\mathscr{E}_1)$*, and the commutator:*

$(1, 2, 3)$	(X, Y)	Z
$(1, 3, 2)$	$(YXY^{-1}, X^{-1}Y^{-1})$	Z^{-1}
$(2, 1, 3)$	(Y, X)	Z^{-1}
$(2, 3, 1)$	$(XYX^{-1}, Y^{-1}X^{-1})$	Z
$(3, 1, 2)$	(XY, X^{-1})	Z
$(3, 2, 1)$	(YX, Y^{-1})	Z^{-1}

This second table gives the lifting action of the three Vieta moves from $(\mathscr{E}_3)$ *to* $(\mathscr{E}_1)$ *giving the Nielsen moves, with the resulting commutator indicated:*

Remark 3.2. One notes that for $D = F$ a field, if $Z \in \Gamma_F$ with $\mathrm{Tr}\, Z = t$, then Z is not conjugate to Z^{-1} in Γ_F if and only if Z is not a diagonal matrix and if the equation $x^2 - (t^2 - 4)y^2 = -1$ has no solutions $(x, y) \in F^2$.

$(x_1, x_2, x_3) \mapsto (x_1, x_2, x_1x_2 - x_3)$	$(X, Y) \mapsto (X^{-1},\ XYX^{-1})$	Z^{-1}
$(x_1, x_2, x_3) \mapsto (x_2x_3 - x_1, x_2, x_3)$	$(X, Y) \mapsto (YXY,\ Y^{-1})$	Z^{-1}
$(x_1, x_2, x_3) \mapsto (x_1, x_1x_3 - x_2, x_3)$	$(X, Y) \mapsto (X^{-1},\ XYX)$	Z^{-1}

For $F = \mathbb{R}$, $Z \not\sim Z^{-1}$ if and only if Z is elliptic.

For $F = \mathbb{F}_p$ a prime field with $p > 2$, using Lemma B.1, we see that Z is not conjugate to Z^{-1} in Γ_F if and only if Z is not a diagonal matrix, $p \equiv 3 \pmod 4$ and $t \equiv \pm 2 \pmod p$).

We now state a (weak) lifting result from $(\mathscr{C}_3)$ to $(\mathscr{C}_1)$ over fields:

Proposition 3.3.
Let F be a field with char$(F) = 0$, $\Gamma_F = SL_2(F)$, $Z \in \Gamma_F$ with $\operatorname{Tr} Z = t \neq \pm 2$, and suppose $(x_1, x_2, x_3) \in \mathscr{M}_{t+2}(F)$ is given. Suppose there is a matrix $Y \in \Gamma_F$ such that $\operatorname{Tr} ZY = \operatorname{Tr} Y = x_j$ for some $1 \leqslant j \leqslant 3$. Then, either Z or Z^{-1} is Γ_F-conjugate to $W(X, Y)$ for some $X \in \Gamma_F$.

Remark 3.4. The proposition also holds for fields with finite but sufficiently large characteristic.

The condition $Y \in \Gamma_F$ such that $\operatorname{Tr} ZY = \operatorname{Tr} Y = x_j$ for some $1 \leqslant j \leqslant 3$ is obviously necessary for $(x_1, x_2, x_3) \in \mathscr{M}_{t+2}(F)$ to be a candidate to be lifted from $(\mathscr{C}_3)$ to $(\mathscr{C}_1)$.

The proof will follow from the following

Lemma 3.5. *With the notation as in the proposition above, suppose $\Delta = t+2-x_2^2 \neq 0$. Then, given any $Y \in \Gamma_F$ with $\operatorname{Tr} ZY = \operatorname{Tr} Y = x_2$, there exists a unique $X \in \Gamma_F$ such that (i). $\operatorname{Tr} X = x_1$, (ii). $\operatorname{Tr} XY = x_3$, and (iii). $W(X, Y) = Z$.*

The conclusion also holds if F is replaced with D a ring but with the requirement $\Delta \in D^\times$.

Proof. The proof is an application of Prop. A.3.

Uniqueness follows readily from (A.0.1): assume there are two matrices X_1 and X_2 satisfying all the conditions satisfied by X, so that on subtracting the two expressions obtained from (A.0.1), we have $(X_1 - X_2)[x_3Y + (x_1 - x_2x_3)I] = 0$, from which we have $X_1 = X_2$, since $\det[x_3Y + (x_1 - x_2x_3)I] = \Delta$ is invertible.

For the existence, choose X so that

$$\begin{aligned} \Delta X &= -x_3ZY + x_1Z + (x_3 - x_1x_2)Y^{-1} + x_1I\ , \\ &= \left(Z - Y^{-2}\right)(x_1I - x_3Y)\,. \end{aligned} \tag{3.1.12}$$

To show $X \in \Gamma_F$, we note that $X(x_1Y - x_3I) = (ZY - Y^{-1})$. We have $\det(x_1X - x_3I) = x_1^2 - x_1x_2x_3 + x_3^2 = t+2-x_2^2 = \Delta$. Similarly, $\det(ZY - Y^{-1}) = 1 - \operatorname{Tr} ZY^2 + 1 = 2 - \operatorname{Tr} Z(x_2Y - I) = 2 - x_2^2 + t = \Delta$. Hence $\det X = 1$.

For (i), since $\operatorname{Tr} ZY = x_2$, taking the trace in (3.1.12) gives

$$\Delta \operatorname{Tr} X = [-x_3x_2 + x_1t + (x_3 - x_1x_2)x_2 + 2x_1] = \Delta x_1.$$

For (ii), we have $\Delta XY = -x_3Z(x_2Y - I) + x_1ZY + (x_3 - x_1x_2)I + x_1Y$, using $Y^2 = x_2Y - I$. Expanding and taking the trace gives the result.

Finally, for (iii), we solve for Z in $X(x_1Y - x_3I) = (ZY - Y^{-1})$, and using $Y^{-2} = x_2Y^{-1} - I$ and $Y^{-1} = -Y + x_2I$, together with Prop. A.3 gives the result.

□

Proof of Prop. 3.3.

Suppose $x_j^2 = t + 2$ for at least two j's. There are only a bounded number of such points on $\mathscr{M}_{t+2}(F)$ and by Zariski density we look at other points equivalent to the original under the Markoff group $\mathfrak{M}$ to get to one for which we may assume a coordinate does not satisfy $x_j^2 = t + 2$. If the proposition is proved for this latter point, we will have a pair of matrices X_0 and Y_0 with $W(X_0, Y_0) = Z^{\pm 1}$. Then, reversing the process and using Lemma 3.1 gives a pair of matrices associated with the original point. Now assume $x_3^2 = t + 2$, but not for x_1 and x_2. Then, the point obtained by a Vieta move $(x_1, x_2, x_1x_2 - x_3)$ is problematic only if $(x_1x_2 - x_3)^2 = t+2$, in which case we conclude that $x_1x_2 = 2x_3$ and also $(x_1^2 - 2)(x_2^2 - 2) = 4$, so that there are only a finite number of such exceptions. Then, we repeat the argument given above.

So assume $x_j^2 \neq t+2$ for all j. If $Y \in \Gamma_F$ can be found satisfying $\operatorname{Tr} ZY = \operatorname{Tr} Y = x_j$ for some j , we apply a permutation to move that x_j to the middle coordinate, noting by Lemma 3.1 that the corresponding Y can be found. Then Lemma 3.5 above can be used to find X. The ambiguity of Z or Z^{-1} comes from the application of the permutation map.

□

Proposition 3.6. *Suppose* F *is a field with* $\mathbf{card}(F) > 5$. *If* $Z \in \Gamma_F$ *with* $\operatorname{Tr} Z \neq -2$, *then* Z *is a commutator.*

Proof. We consider two cases: $\operatorname{Tr} Z = 2$ and $\operatorname{Tr} Z = t \neq \pm 2$.

When $\operatorname{Tr} Z = 2$, we assume $Z \neq I$, in which case, Z is Γ_F-conjugate to a matrix of the type $\left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right]$ for some $b \in F$; this is easily verified using matrices of the type $\left[\begin{smallmatrix} 0 & 1 \\ -1 & x \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ to conjugate with. To verify that Z is a commutator, it suffices to consider the case $Z = \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right]$ with $b \neq 0$.

Put $X = \left[\begin{smallmatrix} x_1 & x_2 \\ 0 & x_1^{-1} \end{smallmatrix}\right]$ and $Y = \left[\begin{smallmatrix} y_1 & y_2 \\ 0 & y_1^{-1} \end{smallmatrix}\right]$. Substituting into $Z = W(X, Y)$ requires us to find x_2 and y_2 such that $(x_1 - x_1^{-1})y_2 - (y_1 - y_1^{-1})x_2 = bx_1^{-1}y_1^{-1}$. This is solvable if $x_1,\ y_1 \neq \pm 1$. For this part of the proof, we need $\mathbf{card}(F) > 3$.

For $\operatorname{Tr} Z = t \neq \pm 2$, we will use Lemma 3.5. To do so, we first create a suitable point $(x_1, x_2, x_3) \in \mathscr{M}_{t+2}(F)$; and then a $Y \in \Gamma_F$ satisfying all the conditions (these are easy to do on a field). The result then follows.

Let $\zeta \neq 0,\ \pm 1$ and put $x_2 = \zeta + \zeta^{-1}$. Put $x_3 = \frac{x_2^2 - t - 1}{\zeta - \zeta^{-1}}$ and $x_1 = 1 + \zeta x_3$. Then, $(x_1, x_2, x_3) \in \mathscr{M}_{t+2}(F)$. Choose ζ such that $x_2^2 \neq t + 2$ (this requires $\mathbf{card}(F) > 5$ if $t+2$ is a square). Now, put $Y = \left[\begin{smallmatrix} \zeta & \eta \\ 0 & \zeta^{-1} \end{smallmatrix}\right]$, with $\eta \in F$ to be chosen. If $Z - I = \left[\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right]$, then $\operatorname{Tr} ZY = \operatorname{Tr} Y$ iff $a_1\zeta + a_3\eta + a_4\zeta^{-1} = 0$. This is solvable in F when $a_3 \neq 0$. If $a_3 = 0$ but $a_2 \neq 0$, we conjugate Z with $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ to get a new matrix with the corresponding $a_3 \neq 0$, giving a suitable Y. Finally, if $a_2 = a_3 = 0$, we conjugate Z with $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ to get a matrix with a non-zero off-diagonal entry $a_1 - a_4 \neq 0$ (since $Z \neq \pm I$), giving Y. Hence we conclude using Lemma 3.5 that some conjugate of Z or Z^{-1} is a commutator, giving the result. □

3.2. The case $D = \mathbb{Z}$

Since $\Gamma_D := \Gamma = \mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, the purely group theoretic equation $(\mathscr{E}_1)$ can be solved explicitly by expressing Z (or its conjugacy class in Γ denoted by $\{Z\}_\Gamma$) in terms of its generators. Wicks' theorem [**28**] describes

explicitly which elements are commutators in such a free product, in terms of their spelling as words in the generators. As shown in **[18]**, if one orders the $\{Z\}_\Gamma$'s by their minimal word length, then very few of these are commutators; roughly square-root of the total number. According to Theorem 2.4, the failure of the typical Z to be a commutator is witnessed in some finite quotient of Γ. One can ask about the local to global principle when restricting locally to congruence quotients of Γ; which we call the "congruence" Hasse principle.

For $D = \mathbb{Z}$ this congruence version for $(\mathscr{C}_1)$ has mostly failures. This version is also relevant for $(\mathscr{C}_2)$ and $(\mathscr{C}_3)$ which are no longer purely group theoretic equations. For each of $(\mathscr{C}_1')$, $(\mathscr{C}_2)$ and $(\mathscr{C}_3)$, the local congruence obstructions are passed for a positive proportion of the choices on the right hand sides, and we call such choices admissible.

For $\mathscr{M}_k(\mathbb{Z})$, $k = t + 2$ is admissible if and only if

$$t \not\equiv 1 \pmod 4 \quad \text{and} \quad t \not\equiv 1, 4 \pmod 9 \,. \tag{3.2.1}$$

This and the corresponding Hasse principle for $(\mathscr{C}_3)$ were studied in depth in **[9]**.

The congruence obstructions for $\mathscr{M}_{t+2}(\mathbb{Z})$ lead to ones for $\mathscr{T}_t(\mathbb{Z})$ and there are further ones: t is not admissible if

$$t \equiv 0, 1, 4, 5, 8, 9, 10, 12, 13 \pmod{16}$$

and

$$t \equiv 1, 4, 5, 8 \pmod 9 \,. \tag{3.2.2}$$

We expect but have not verified that (3.2.2) gives a complete description of the admissible t's, see Section 5.2 (Prop. 5.12).

For $(\mathscr{C}_1')$ an explicit description of the (congruence) admissible conjugacy classes $\{Z\}_\Gamma$ is more complicated, but it consists of a positive proportion of the sets

$$\{\{Z\}_\Gamma \ : |\operatorname{Tr}(Z)| \leqslant T\}. \tag{3.2.3}$$

Indeed if A is the matrix in $SL_2(\mathbb{Z}/q\mathbb{Z})$, with $q = 2^2.3^3.5$ in Theorem 5.15, then according to that theorem if $Z \in \Gamma \pmod q$ is conjugate to $A \pmod q$, then $\{Z\}_\Gamma$ is (congruence) admissible for $(\hat{\mathscr{C}}_1)$. By the Chebotarev Theorem for prime geodesics (**[20]**) it follows that

$$\frac{\#\left\{\{Z\}_\Gamma : |\operatorname{Tr}(Z)| \leqslant T,\ \{Z\}_{SL_2(\mathbb{Z}/q\mathbb{Z})} = \{A\}_{SL_2(\mathbb{Z}/q\mathbb{Z})}\right\}}{\#\{\{Z\}_\Gamma : |\operatorname{Tr}(Z)| \leqslant T\}} \to \frac{|\{A\}_{SL_2(\mathbb{Z}/q\mathbb{Z})}|}{|SL_2(\mathbb{Z}/q\mathbb{Z})|} \,,$$

as $T \to \infty$. This yields a positive proportion lower bound for the congruence admissible Z's for $(\mathscr{C}_1')$. Pushing this analysis a bit further, one can show that the proportion of such admissible conjugacy class tends to a limit.

The algorithm above to decide $(\mathscr{C}_1')$ can be used to decide $(\mathscr{C}_2)$. Given an admssible t for $\mathscr{T}_t(\mathbb{Z})$, one computes the $h(t)$ classes $\{Z\}_\Gamma$ with trace equal to t. This is a classical calculation, in fact the number $h(t)$ is the Hurwitz class number of binary quadratic forms of discriminant $t^2 - 4$ (**[5]**) and there are approximately t such classes for t large. For each class one runs $(\mathscr{C}_1)$ and checks whether it is a commutator. This gives a list of which of these are commutators, and in particular whether $\mathscr{T}_t(\mathbb{Z})$ has a solution or not.

In [**17**] this procedure was implemented for $|\mathsf{t}| < 1000$. He finds that for most admissible t's, $\mathcal{T}_{\mathsf{t}}(\mathbb{Z})$ is not empty, and typically only a few of the $\mathfrak{h}(\mathsf{t})$ classes are commutators. He also found a number of Hasse failures, some examples being:

(1) $\mathsf{t} = 3$: the one conjugacy class of trace 3 is not even in the commutator subgroup of Γ.
(2) $\mathsf{t} = -21$: there are two conjugacy classes of this trace which are in the commutator subgroup. However, neither is a commutator.
(3) $\mathsf{t} = 15$: this is not a Hasse failure but it is typical. There are four conjugacy classes which are in the commutator subgroup; two are not commutators and two of them $\mathsf{Z}_1 = \left[\begin{smallmatrix} 2 & 5 \\ 5 & 13 \end{smallmatrix}\right]$ and $\mathsf{Z}_2 = \left[\begin{smallmatrix} 2 & -5 \\ -5 & 13 \end{smallmatrix}\right]$ are. Hence only $\{\mathsf{Z}_1\}_\Gamma$ and $\{\mathsf{Z}_2\}_\Gamma$ are lifts of solutions from $(\mathscr{E}_2)$ to $(\mathscr{E}_1')$ with $\mathsf{t} = 15$.

The top down procedure from $(\mathscr{E}_1)$ to $(\mathscr{E}_2)$ gives an algorithm to decide both of these equations. However, it offers less in terms of proving theoretical results for $(\mathscr{E}_2)$. The bottom up approach, that starts with $(\mathscr{E}_3)$ and lifts solutions is useful in this regard, and since in this case $\mathscr{M}_{\mathsf{t}+2}(\mathbb{Z})/\mathsf{G}$ is finite for generic points, it can also be used to give a decision procedure for all three of $(\mathscr{E}_1)$, $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$.

If $\mathscr{M}_{\mathsf{t}+2}(\mathbb{Z}) = \emptyset$ and t is admissible (if it satisfies (3.2.2)), then $\mathcal{T}_{\mathsf{t}}(\mathbb{Z}) = \emptyset$ and is a Hasse failure. An example of such is $\mathsf{t} = -21$ ($\mathscr{M}_{-19}(\mathbb{Z})$ is one of the Hasse failures from [**9**]). Moreover, infinitely many such Hasse failures for $\mathcal{T}_{\mathsf{t}}(\mathbb{Z})$ can be constructed using the theory in [**9**], and we give some of these in Section 5 (see Prop. 5.7 and Prop. 5.8). In fact these are promoted to give infinitely many conjugacy classes $\{\mathsf{Z}\}_\Gamma$ for which the congruence Hasse principle fails for $(\mathscr{E}_1')$.

Our purpose in this section is the decision procedure for the $(\mathscr{E})$'s. As detailed in Section 3.1, once $\mathscr{M}_{\mathsf{t}+2}(\mathsf{D})/\mathsf{G}$ is finite as it is here, we have only finitely many lifting problems to solving $\mathcal{T}_{\mathsf{t}}(\mathbb{Z})/\mathsf{G}$, each of which is effective, and then a further finite number of effective liftings to $(\mathscr{E}_1')$, with $\mathrm{Tr}(\mathsf{Z}) = \mathsf{t}$. This gives a complete decision procedure for all the $(\mathscr{E})$'s over $\mathbb{Z}$. As the analysis from [**9**] yields an effective and feasible algorithm for $(\mathscr{E}_3)$, we apply it to do the same for $(\mathscr{E}_1)$ and $(\mathscr{E}_2)$ in the following subsection.

3.2.1. *An algorithmn for* $(\mathscr{E}_2(\mathbb{Z}))$

If $\mathsf{x}_1 = \mathrm{Tr}\,\mathsf{X}$, $\mathsf{x}_2 = \mathrm{Tr}\,\mathsf{Y}$ and $\mathsf{x}_3 = \mathrm{Tr}\,\mathsf{XY}$, then $(\mathscr{E}_3)$ holds when $(\mathscr{E}_2)$ holds for a given k with $\mathsf{t} = \mathsf{k} - 2$. Given a vector $\mathbf{x} = (\mathsf{x}_1, \mathsf{x}_2, \mathsf{x}_3) \in \mathscr{M}_{\mathsf{k}}(\mathbb{Z})$, we say it is $(\mathscr{E}_2)$-good if we can find matrices X and Y such that $(\mathscr{E}_2)$ holds in this way, and otherwise $\mathbf{x}$ is $(\mathscr{E}_2)$-bad. We know (see [**9**] for references), that when $\mathsf{D} = \mathbb{Z}$, there is an algorithm to determine if $(\mathscr{E}_3)$ is solvable for generic $\mathsf{k} > 4$.

Proposition 3.7. *Let* $\mathsf{k} \in \mathbb{Z}$ *be generic such that the odd part of* $\mathsf{k}-4$ *is squarefree. Let* $\mathbf{x}_\mathsf{j}$ *be fundamental solutions to* $(\mathscr{E}_3)$ *with* $1 \leqslant \mathsf{j} \leqslant \mathfrak{h}(\mathsf{k})$*, where* $\mathfrak{h}(\mathsf{k})$ *is the "class number" of* $(\mathscr{E}_3)$*. Denote the coordinates of* $\mathbf{x}_\mathsf{j}$ *by* $\mathsf{x}_{\mathsf{j}\mathsf{i}}$ *with* $1 \leqslant \mathsf{i} \leqslant 3$*. Suppose for each* j *there is an odd prime factor* p *of* $\mathsf{k}-4$ *and a coordinate* $\mathsf{x}_{\mathsf{j}\mathsf{i}}$*, such that* $\mathsf{x}_{\mathsf{j}\mathsf{i}}^2 - 4$ *is a quadratic non-residue modulo* p*. Then no solution* $\mathbf{x}$ *of* $(\mathscr{E}_3)$ *is* $(\mathscr{E}_2)$*-good.*

Example 3.8. $\mathsf{k} = 108$ is generic with $\mathsf{k} - 4 = 8 * 13$. One computes $\mathfrak{h}(108) = 1$ with fundamental solution $(-3, 3, 6)$, using Theorem 1.1 of [**9**]. Since $3^2 - 4 = 5$ is a quadratic nonresidue modulo 13, the proposition states that $(\mathscr{E}_3)$ is solvable with $\mathsf{k} = 108$ but $(\mathscr{E}_2)$ is not solvable with $\mathsf{t} = 106$. Note that $\mathsf{t} = 106$ has no congruence

obstructions in $(\mathscr{E}_2)$ (see Section 5.1) and so is a Hasse failure for $(\mathscr{E}_2)$, but not for $(\mathscr{E}_3)$.

The proof follows from the following lemmas.

Lemma 3.9. *Let $(x_1, x_2, x_3) \in \mathscr{M}_k(\mathbb{Z})$ and let $p|(k-4)$ be odd. Then*
(1). *If $p \nmid x_i^2 - 4$ for all i , then $x_i^2 - 4$ are either all quadratic residues (QR) or all non-residues (QNR) modulo p.*
(2). *If $p|x_i^2 - 4$ for some i, then it does not do so for the other two. Moreover $x_j^2 - 4$ are then either both QR or both QNR modulo p for $j \neq i$.*

Proof. Let i, j, l be any permutation of $1, 2, 3$. Completing the square in $(\mathscr{E}_3)$ gives

$$(2x_i - x_j x_l)^2 - (x_j^2 - 4)(x_l^2 - 4) = 4(k-4) \equiv 0 \pmod{p} .$$

Since the products $(x_j^2 - 4)(x_l^2 - 4)$ are all squares mod p for each pair of subscripts, the first case of the lemma follows.

Next, it also follows that p cannot divide two of $x_i^2 - 4$, as then $p^2|k-4$. The second case now follows. □

Definition 3.10. We say $\mathbf{x} = (x_1, x_2, x_3)$ is a QR mod p if at least two of $x_i^2 - 4$ are QR mod p. Otherwise we say it is a QNR

Lemma 3.11. *Let $\mathfrak{M}$ be the Markoff group and $\mathfrak{m} \in \mathfrak{M}$. If $\mathbf{x}$ satisfies $(\mathscr{E}_3)$, then $\mathbf{x}$ is a QR mod p if and only if $\mathfrak{m}\mathbf{x}$ is a QR mod p.*

Proof. It suffices to verify this for a single Vieta move, say $(x_1, x_2, x_3) \to (x_4, x_2, x_3)$ with $x_4 = x_2 x_3 - x_1$. From the assumption, it follows that either $x_2^2 - 4$ or $x_3^2 - 4$ is a QR. If p does not divide either, it follows from Lemma 3.9 that both are QR and we are done. So assume $p|x_2^2 - 4$, in which case the assumption implies $x_3^2 - 4$ is a QR, so that again Lemma 3.9 implies $x_4^2 - 4$ is too. □

Lemma 3.12. *Suppose $\mathbf{x}$ satisfying $(\mathscr{E}_3)$ is $(\mathscr{E}_2)$-good. Then so is $\mathfrak{m}\mathbf{x}$ for all $\mathfrak{m} \in \mathfrak{M}$.*

Proof. It suffices to check this for a Vieta move, but the trace identity $\operatorname{Tr} XY^{-1} = (\operatorname{Tr} X)(\operatorname{Tr} Y) - \operatorname{Tr} XY$ verifies this. □

Let $\mathscr{M}_k(\mathbb{Z})$ be decomposed into its $\mathfrak{h}(k)$ connected components $V_k^{(j)}(\mathbb{Z})$. Lemma 3.12 implies that all elements of $V_k^{(j)}(\mathbb{Z})$ are either $(\mathscr{E}_2)$-good or all $(\mathscr{E}_2)$-bad. So to prove Prop. 3.7 it suffices to verify that all elements of a fundamental set are $(\mathscr{E}_2)$-bad.

Proof of Prop. 3.7.

Suppose $\mathbf{x} = (x_1, x_2, x_3) \in \mathscr{M}_k(\mathbb{Z})$ is $(\mathscr{E}_2)$-good. Write $x_1 = \operatorname{Tr} X$, $x_2 = \operatorname{Tr} Y$, $x_3 = \operatorname{Tr} XY$ with X, Y in $SL_2(\mathbb{Z})$. Write

$$X = \begin{bmatrix} a_1 & a_2 \\ a_3 & x_1 - a_1 \end{bmatrix}, \qquad Y = \begin{bmatrix} b_1 & b_2 \\ b_3 & x_2 - b_1 \end{bmatrix}$$

so that $x_3 = a_1 b_1 + a_2 b_3 + a_3 b_2 + (x_1 - a - 1)(x_2 - b_1)$. Put $u = 2a_1 - x_1$ and $v = x_2 - 2b_1$. We get three equations
(i). $u^2 + 4a_2 a_3 = x_1^2 - 4$,
(ii). $v^2 + 4b_2 b_3 = x_2^2 - 4$,
(iii). $uv = (x_1 x_2 - 2x_3) + 2(a_2 b_3 + a_3 b_2)$.

These imply

$$(x_2^2-4)(a_2\nu+b_2u)^2=[a_2(x_2^2-4)+(x_1x_2-2x_3)b_2]^2-4b_2^2(k-4).$$

Let $p|k-4$ be an odd prime factor. If $p\nmid(a_2\nu+b_2u)$, it follows that x_2^2-4 is zero or a QR mod p. Next, if $p|(a_2\nu+b_2u)$, since $p^2\nmid(k-4)$, it follows that $p|b_2$ so that (ii) implies again that x_2^2-4 is zero or a QR mod p. By symmetry, it follows that the same possibilities are true for x_1^2-4 and x_3^2-4. This is true for all odd prime factors of $k-4$. Thus if there is such a prime factor with one of x_i^2-4 is a QNR, we get that $\mathbf{x}$ is not $(\mathscr{C}_2)$-good. Then, by Lemmas 3.11 and 3.12, if this property holds for each point of a fundamental set, it holds for all points of $\mathscr{M}_k(\mathbb{Z})$, as required. □

Remark 3.13.

The analysis in this section corresponds to the an extension of $(\mathscr{C}_1)$ to subgroups Ω of Γ_D. Here, we choose Ω to be a subgroup of Γ_D invariant under the map $X\to -X$, so that it is closed under the Nielsen automorphisms. We then ask for solutions $(X,Y)\in\Omega\times\Omega$ satisfying $Z=W(X,Y)$ for a given $Z\in\Omega$; the analogue of $(\mathscr{C}_2)$ is described similarly. The projection of $(\mathscr{C}_1)$ and $(\mathscr{C}_2)$ then gives a subset of solutions to $(\mathscr{C}_3)$ with the coordinates of $\mathbf{x}$ restricted in some way, as illustrated below.

Example 3.14. Let p be an odd prime, and $D=\mathbb{Z}$.

(i). Let $\Omega=\{U\in\Gamma\ :U\equiv\pm I\pmod p\}$. Then $\mathbb{Z}=W(X,Y)$ being solvable in Ω implies $Z\equiv I\pmod p$, so that $\operatorname{Tr}Z=t\equiv 2\pmod p$. The projection from $(\mathscr{C}_1)$ to $(\mathscr{C}_3)$ gives points Markoff-equivalent to $(2,2,2)$ modulo p .

One can generalize this to subgroups $\Omega_a=\{U\in\Gamma\ :U\equiv\pm R_a^m\pmod p, m\in\mathbb{Z}\}$ where $R_a=\left[\begin{smallmatrix}a&1\\-1&0\end{smallmatrix}\right]$, so that a commutator is congruent to I. By choosing a suitably, the corresponding points in $(\mathscr{C}_3)$ are Markoff-equivalent to $(2,b,b)$ modulo p for all b (such points $(2,b,b)$ represent the Markoff-inequivalent orbits on the Cayley surface $\mathscr{M}_4$ (see [**9**])).

(ii). Let $\Omega=\Gamma_0(p)$. Then $\mathbb{Z}=W(X,Y)$ implies $Z\equiv\left[\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right]\pmod p$, so that $t\equiv 2\pmod p$. Then, $x_1=\operatorname{Tr}X$ implies x_1^2-4 is a QR modulo p; similarly for $x_2=\operatorname{Tr}Y$. Then, x_3^2-4 is a QR since $x_3=\operatorname{Tr}XY$ (this is reflected in Lemma 3.9).

3.3. $D=\mathbb{Z}[\sqrt{-d}]$, Bianchi groups

For $d<0$ squarefree, the groups $SL_2(D)$ are known as the Bianchi groups. The commutator story for these is similar to that of $D=\mathbb{Z}$. There are only finitely many units in D and the congruence subgroup property is known to fail ([**22**]). In principle one can still proceed to give an effective procedure for equations $(\mathscr{C}_1)$ and $(\mathscr{C}_2)$, thanks to the type of decidability results of [**21**]. While Sela's general results apply only to torsion-free Gromov hyperbolic groups, we understand from Ian Agol that one can decide the commutator problem for hyperbolic 3-manifold groups. However, one does not have an explicit description as with Wick's theorem so that the feasibility of implementing these procedures is less clear. On the other hand, the bottom up approach works equally well here as it does over $\mathbb{Z}$. The key is that $\mathscr{M}_{t+2}(D)/G$ is finite (for generic points) here as well. This was proved for $t=-2$ in [**25**], and using Markoff descent this extends to all $t\neq -2$. The geometric descent in [**27**] is carried out over these rings and also yields this finiteness. As explained in Section 3.1 this effective finiteness together with the general lifting procedures,

yields an effective and feasible means to decide all of $(\mathscr{E}_1)$, $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$. While we have not implemented this procedure, we expect that doing so will yield results similar to that of $D = \mathbb{Z}$ in Section 3.2. Whether these Γ's satisfy a profinite local to global principle (the analogue of Theorem 2.4) is less clear.

4. Universal Domains

Definition 4.1. For a domain D, ff any of $(\mathscr{E}_1)$, $(\mathscr{E}_2)$, $(\mathscr{E}_3)$ has a solution for all choices of the right hand side in D, we say that D is *universal* for that $(\mathscr{E}_j)$. By abuse of language, we also say the corresponding $(\mathscr{E}_j)$ is universal, if the domain D is implicit.

We do not know of a choice of any of our domains D for which $(\mathscr{E}_1)$ is universal. However for $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$ we give some examples below.

Proposition 4.2. *Let D be any ring containing a unit ε such that $\varepsilon - \varepsilon^{-1}$ is also a unit. Then, $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$ are universal.*

Proof. For any $t \in D$, put $\eta = \varepsilon - \varepsilon^{-1} \in D^\times$ and $\tau = (t-2)\eta^{-2} \in D$.

For $(\mathscr{E}_2)$, we use $X = \left[\begin{smallmatrix} 1 & \tau \\ -1 & 1-\tau \end{smallmatrix}\right]$ and $Y = \left[\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right]$, giving $\operatorname{Tr} W(X,Y) = t$.

For $(\mathscr{E}_3)$, take $x_1 = 2-\tau$, $x_2 = \varepsilon + \varepsilon^{-1}$, $x_3 = \varepsilon + (1-\tau)\varepsilon^{-1}$ and $t = k-2$, for any $k \in D$. □

Example 4.3.

(1) For any q with $(6, q) = 1$, the equations in $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$ are solvable in $D = \mathbb{Z}/q\mathbb{Z}$. In particular, there are no congruence obstructions over $\mathbb{Z}$ in $(\mathscr{E}_2)$ and $(\mathscr{E}_3)$ modulo primes powers exceeding 3. Here, we take $\varepsilon = 2$.
(2) For the S-integers, take $D = \mathbb{Z}[\frac{1}{6}]$ using the unit $\varepsilon = 2$.
(3) Let F be the complex cubic field determined by the roots ρ of the polynomial $x^3 - x^2 + 1$, and let $D = \mathcal{O}_K$, the ring of integers generated by $1, \rho$ and ρ^2. It has discriminant -23 and has class number one. Since $\rho^2(1-\rho) = 1$, ρ is a unit, and so is $\rho - \rho^{-1} = \rho^2$.

Then Prop 4.2 holds in all cases, as does Prop. 4.6 below.

Another version of universality for $(\mathscr{E}_3)$ is

Proposition 4.4. *If char$(D) \neq 2$ and D contains elements z and w with w a unit satisfying $z^2 - 4 = w^2$, then $(\mathscr{E}_3)$ is universal for D.*

Proof. The split binary form $f(x_1, x_2) = x_1x_2$ is universal for any D. Given z as above, we put $x_3 = z$ in $(\mathscr{E}_3)$. The restriction of $M(x_1, x_2, x_3)$ to this hyperplane section yields a binary quadratic form whose homogenous part is $g = x_1^2 + x_2^2 - zx_1x_2$, having discriminant w^2. Since w is a unit, g is equivalent over D to f, giving universality. This construction is similar to the construction of the universal form U_2 in Section 5.1 of [**9**].

Since $\zeta = \frac{z+w}{2}$ is a unit, we obtain a point in $\mathscr{M}_k(D)$ with coordinates $x_1 = w^{-1}(1 - k + z^2)$, $x_2 = w^{-1}\left(\zeta - (k - z^2)\zeta^{-1}\right)$ and $x_3 = z$, for any $k \in D$. □

For D a PID, we can say a bit more.

Definition 4.5. Given a matrix A defined over D, we let $\mathfrak{S}(A)$ be the set over D given by

$$\mathfrak{S}(A) = \{X : \operatorname{Tr} AX = \operatorname{Tr} X\ , |X| = 1\}.$$

Proposition 4.6. *Let* D *be a PID containing a unit* ε *such that* $\eta = \varepsilon - \varepsilon^{-1}$ *is also a unit. Let* $Z \in \Gamma_D = \mathrm{SL}_2(D)$*, and suppose there exists a* $U \in \mathfrak{S}(Z)$ *with* $\operatorname{Tr} U = \varepsilon + \varepsilon^{-1}$*. Then* Z *is a commutator.*

Proof. (See Remark 4.8 for another proof).

We first note that $\mathfrak{S}(\sigma Z \sigma^{-1}) = \sigma^{-1}\mathfrak{S}(Z)\sigma$ for any $\sigma \in \mathrm{SL}_2(D)$. Moreover, Z is a commutator if any conjugate of it is. Thus, it suffices to verify the proposition by using a suitable conjugate of the matrix U. Since U has ε for an eigenvalue and D is a PID, there is a matrix $M \in \mathrm{SL}_2(D)$ such that $M^{-1}UM = U_0 := \left(\begin{smallmatrix} \varepsilon & \alpha \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right)$ for some $\alpha \in D$. Conjugating U_0 with $\left[\begin{smallmatrix} 1 & \alpha\eta^{-1} \\ 0 & 1 \end{smallmatrix}\right]$ shows that we may take $\alpha = 0$. So we will prove the proposition with $U = U_1 := \left[\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right]$.

It suffices to show that ZU_1 and U_1 are conjugates in Γ, since then $(\mathscr{E}_1)$ follows with $Y = U_1$. Putting $B = ZU_1 = \left[\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right]$, we seek $X = \left[\begin{smallmatrix} x_1 & x_2 \\ x_3 & x_4 \end{smallmatrix}\right] \in \Gamma$ such that $BX = XU_1$. Since $U_1 \in \mathfrak{S}(Z)$, we have $b_1 + b_4 = \varepsilon + \varepsilon^{-1}$, so that $(b_1 - \varepsilon)(b_4 - \varepsilon) = b_2 b_3$. Assume $b_2 \neq 0$ and put $\delta = \gcd(b_1 - \varepsilon, b_2)$. If $\delta = 0$, then $b_1 = \varepsilon$, $b_4 = \varepsilon^{-1}$ and $b_3 = 0$. Then put $X = \begin{bmatrix} -\eta^{-1} & b_2 \\ 0 & -\eta \end{bmatrix}$. If $\delta \neq 0$, then we have $\frac{b_2}{\delta} \mid (b_4 - \varepsilon)$ and so we put $X = \begin{bmatrix} \frac{b_2}{\delta} & -\delta\eta^{-1} \\ \frac{\varepsilon - b_1}{\delta} & -\frac{(b_4 - \varepsilon)\delta}{b_2\eta} \end{bmatrix} \in \Gamma$. The argument is similar if $b_3 \neq 0$. Finally, if b_2 and b_3 are both zero, then B is necessarily U_1 or its inverse, for which X is either the identity or $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$.

□

Remark 4.7. It is not true that if D is a PID containing a unit ε such that $\eta = \varepsilon - \varepsilon^{-1}$ is also a unit, that then $(\mathscr{E}_1)$ is universal. This can be seen with $D = \mathbb{Z}[\frac{1}{6}]$, for which $-I$ is not a commutator.

One can show that if D is a PID, then $-I$ is a commutator if and only if the equation $r_1^2 + r_2^2 + r_3^2 = 0$ has a non-trivial solution in D (see Remark A.8).

Remark 4.8.

We give here an alternative proof of Prop. 4.6 using lifting as in the proof of Lemma 3.5. All notation is that used in Prop. 4.6, and Lemma 3.5. The idea is to first construct a suitable point $\mathbf{x}$, a matrix Y and then verify that the matrix X in (3.1.12) is in Γ_D. We put $Y = U_1 = \left[\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{smallmatrix}\right]$ and assume $Y \in \mathfrak{S}(Z)$; use $x_2 = \operatorname{Tr} Y = \varepsilon + \varepsilon^{-1}$ and $\Delta = t + 2 - x_2^2$.

Assume first that $\Delta \neq 0$. Write $Z - Y^{-2} = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, with trace and determinant equaling Δ. Then, $Y \in \mathfrak{S}(Z)$ implies $\operatorname{Tr}(Z - Y^{-2})Y = 0$, so that $a\varepsilon + d\varepsilon^{-1} = 0$. If $c = 0$, a small calculation shows that $Z = \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]$, and this is a commutator (since ZY and Y are conjugates, using η is a unit). So we assume $c \neq 0$, and put $\mu = \gcd(c, \Delta)$. We then choose

$$x_1 = \eta^{-1}\left(\varepsilon\mu - \frac{\Delta}{\varepsilon\mu}\right) \quad \text{and} \quad x_3 = \eta^{-1}\left(\mu - \frac{\Delta}{\mu}\right).$$

The point $\mathbf{x} = (x_1, x_2, x_3) \in \mathscr{M}_{t+2}(D)$. Then, X in (3.1.12) satisfies $\det X = 1$, with

$$X = \Delta^{-1}\begin{bmatrix} \Delta a\mu^{-1} & b\mu \\ \Delta c\mu^{-1} & d\mu \end{bmatrix}.$$

We need to show that Δ divides all entries in the matrix. We have $0 = a\varepsilon + d\varepsilon^{-1} = a\varepsilon + (\Delta - a)\varepsilon^{-1} \equiv a\eta \pmod{\Delta}$, so that $\Delta | a$ and $\Delta | d$. Using the determinant $-a^2 - bc \equiv 0 \pmod{\Delta}$, we have $b \equiv 0 \pmod{\frac{\Delta}{\mu}}$ so that $X \in \Gamma_D$.

Next, if $\Delta = 0$, one concludes without much difficulty that

$$Z = \begin{bmatrix} \varepsilon^{-2} & * \\ 0 & \varepsilon^2 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} z_1 & z_2 \\ z_3 & t - z_1 \end{bmatrix},$$

with z_3 free, $z_1 = -\alpha\eta^{-1}z_3 + \mu^{-2}$, and $z_2 \in D$ determined. In either case, one shows that Z is a commutator (showing ZY is conjugate to Y, using elementary matrices and $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$).

5. Hasse Failures

5.1. Hasse failures for Markoff surfaces

5.1.1. *Markoff surfaces and ternary quadratic forms,* $SL_2(\mathbb{Z})$*-revisited*

Remark 5.1. We write this section mostly over $\mathbb{Z}$ but much carries over more generally to rings over number fields.

For D a ring, and $U(D)$ a subset of D^3, we set

$$\widetilde{U}(D) = \left\{ \mathbf{X} = X(\mathbf{x}) := \begin{bmatrix} 2 & x_1 & x_2 \\ x_1 & 2 & x_3 \\ x_2 & x_3 & 2 \end{bmatrix} \quad | \quad \mathbf{x} = (x_1, x_2, x_3) \in U(D) \right\},$$

and call the x_j's coordinates of $\mathbf{X}$.

We will be primarily concerned with $D = \mathbb{Z}$ and $U = \mathscr{M}_k(\mathbb{Z})$, the Markoff surface. Then, there is a one-one correspondence $\mathbf{x} \leftrightarrow \mathbf{X}$ between points in $\mathscr{M}_k(\mathbb{Z})$ and matrices in $\widetilde{\mathscr{M}}_k(\mathbb{Z})$ of determinant $-2(k-4)$. To each such point $\mathbf{x}$ and so matrix $\mathbf{X}$, we can then associate the ternary quadratic form

$$f_{\mathbf{X}}(\mathbf{u}) := \frac{1}{2}\mathbf{u}^\top \mathbf{X}\mathbf{u} = u_1^2 + u_2^2 + u_3^2 + x_1u_1u_2 + x_2u_1u_3 + x_3u_2u_3,$$

where $\mathbf{u} = (u_1, u_2, u_3)$.

For $k > 4$ generic (see [**9**], pg.2) and $\mathbf{X} \in \widetilde{\mathscr{M}}_k(\mathbb{Z})$, all such quadratic forms are indefinite, with signature (2,1). For each prime p, we consider the Hasse-invariant $c_p(f_{\mathbf{X}})$ (see below for details). The Hasse invariants satisfy the product formula $\prod_{p \leqslant \infty} c_p = 1$. One way to construct Hasse-failures k is to take any matrix $\mathbf{X} \in \widetilde{\mathscr{M}}_k(\mathbb{Z})$, and show that the product formula is violated for the corresponding quadratic form. This can be done for all the examples of Hasse failures (not using descent) we have constructed in [**9**]. Since the method is quite general and simple, we present it here, and also extend it to S-integers.

We will give some details below for completeness sake. Throughout, k will be generic, $k > 4$ and fixed. For any $\mathbf{X} \in \widetilde{\mathscr{M}}_k(\mathbb{Z})$ as above, and $\gamma \in GL(3, \mathbb{Z})$, we write $\gamma \cdot \mathbf{X} = \gamma^\top \mathbf{X}\gamma$, and we say γ is good if $\gamma \cdot \mathbf{X} \in \widetilde{\mathscr{M}}_k(\mathbb{Z})$.

Let

$$D_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad D_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad D_3 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

These matrices are all good for any $\mathbf{X} \in \widetilde{\mathscr{M}}_k(\mathbb{Z})$, with $D_j \cdot \mathbf{X}$ corresponding to a double sign-change on $\mathbf{x} \in \mathscr{M}_k(\mathbb{Z})$. The standard permutation matrices P_j are also all good, corresponding to permutations of the coordinates of $\mathbf{x}$. For the Vieta

moves, being non-linear, the associated matrix action depends on the coordinates of $\mathbf{X}$. We put

$$V_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & x_3 & 1 \end{bmatrix}, \quad V_2 = \begin{bmatrix} -1 & 0 & 0 \\ x_1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad V_3 = \begin{bmatrix} 1 & 0 & x_2 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

where $V_j \cdot \mathbf{X}$ is the matrix corresponding to the Vieta move applied to the j-th coordinate of $\mathbf{x}$, keeping the other two fixed. Obviously, these matrices are not unique, since they can be multiplied on the left by any automorph of $\mathbf{X}$. Since the Markoff group is generated by the three types of involutions, the action of any member of the Markoff group on $\mathbf{x}$ gives rise to $\mathbf{y}$ whose corresponding matrix satisfies $X(\mathbf{y}) = \gamma \cdot X(\mathbf{x})$, for some $\gamma \in \mathrm{GL}(3,\mathbb{Z})$; the entries of γ obviously depending on both the Markoff action and $X(\mathbf{x})$. We will say a $\gamma \in \mathrm{GL}(3,\mathbb{Z})$ of the type discussed here, coming from a Markoff group action on $\mathbf{x}$ is of M-type; thus, given $\mathbf{X}$, a M-type matrix is a word generated by the matrices D_j, P_j and specific V_j depending on the coordinates of $\mathbf{X}$.

By descent (see [**9**] for example), since $\mathscr{M}_k(\mathbb{Z})$ is a finite union of Markoff-orbits, there exists a fundamental set of matrices $\{\mathbf{X}_1, ..., \mathbf{X}_h\}$ such that any $\mathbf{X} \in \widetilde{\mathscr{M}_k}(\mathbb{Z})$ is M-type equivalent to a unique $\mathbf{X}_j$ (here $\mathbf{X}_j = X(\mathbf{z}_j)$ with $\{\mathbf{z}_1, ..., \mathbf{z}_h\}$ a fundamental set in $\mathscr{M}_k(\mathbb{Z})$ with $h = \mathfrak{h}(k)$ of [**9**]). Thus, the same statement holds for the corresponding ternary quadratic forms: there are ternary quadratic forms $f^{(1)}, ..., f^{(h)}$ that are inequivalent under M-type transformations, and any $f_{\mathbf{X}}$ is M-type equivalent to a unique $f^{(j)}$. Since M-type equivalence implies $\mathrm{GL}(3,\mathbb{Z})$-equivalence, all matrices coming from $\mathbf{x}$ in the same Markoff-orbit give rise to ternary forms in the same $\mathrm{GL}(3,\mathbb{Z})$-orbit, and as such, will all have the same invariants (this being important in our discussion of Hasse failures).

We first look at some examples regarding fundamental sets. One can ask various questions about the ternary quadratics we get via the Markoff fundamental sets: isotropic, anisotropic, genera, $\mathrm{GL}(3,\mathbb{Z})$-equivalence etc.. Obviously, if $\mathfrak{h}(k) = 1$, all the associated quadratic forms are $\mathrm{GL}(3,\mathbb{Z})$-equivalent. We begin with Legendre's theorem and consequences, together with some other verified facts:

Lemma 5.2.

(1). *Legendre's theorem: let* $a > 0$, $b, c < 0$ *be integers with* abc *squarefree. Then,* $ax^2 + by^2 + cz^2$ *is isotropic if and only if* $-ab$ *is a square mod* c, $-ac$ *is a square mod* b *and* $-bc$ *is a square mod* a.

(2). *Suppose* m *is the squarefree part of* $x_j^2 - 4$ *for some* j, *and* n *is the squarefree part of* $k-4$ *with* $(m,n) = 1$. *Then* $f = u_1^2 + u_2^2 + u_3^2 x_1 u_1 u_2 + x_2 u_1 u_3 + x_3 u_2 u_3$ *is isotropic if and only if* m *is a square mod* n *and* n *is a square mod* m.

(3). *Suppose there exists an odd prime* p *such that* $p \parallel (k-4)$ *and* $p \nmid (x_j^2 - 4)$ *for some* j. *If* $x_j^2 - 4$ *is a quadratic non-residue mod* p, *then the associated quadratic form is anisotropic.*

Proof. We may consider only the case $j = 1$. If $f = u_1^2 + u_2^2 + u_3^2 x_1 u_1 u_2 + x_2 u_1 u_3 + x_3 u_2 u_3$, then $4(x_1^2-4)f = (x_1^2-4)A^2 - B^2 + 4(k-4)u_3^2$, where $A = 2u_1 + x_1 u_2 + x_2 u_3$ and $B = (x_1^2 - 4)u_2 - (2x_3 - x_1 x_2)u_3$. Hence, $(4 - x_1^2)f$ is $\mathrm{GL}(3,\mathbb{Q})$ equivalent to $ax^2 + by^2 + cz^2$ with $a = 1$, $b = -m$ and $c = -n$. If m and n are coprime, the conditions of Legendre's theorem are satisfied. It is isotropic if and only if m is a square (mod n) and n is a square (mod m). Part (3) is a consequence. □

Examples 5.3.

(1) $\mathfrak{h}(70) = 1$ with $f^{(1)} = u_1^2 + u_2^2 + u_3^2 - 3u_1u_2 + 3u_1u_3 + 4u_2u_3$. By the lemma above, this is anisotropic with $p = 3$ and $x_1 = -3$..

(2) $\mathfrak{h}(3780) = 1$ with $f^{(1)} = u_1^2 + u_2^2 + u_3^2 - 3u_1u_2 + 3u_1u_3 + 57u_2u_3$. This is isotropic with $f^{(1)}(409, 251, 50) = 0$. Here, $m = 5$ and $n = 59$, satisfying the conditions of the lemma.

(3) $\mathfrak{h}(460) = 2$, with anisotropic forms (the lemma holds with $p = 3$ and $x_1 = -3$)

$$f^{(1)} = u_1^2 + u_2^2 + u_3^2 - 3u_1u_2 + 3u_1u_3 + 17u_2u_3\,,$$
$$f^{(2)} = u_1^2 + u_2^2 + u_3^2 - 3u_1u_2 + 9u_1u_3 + 10u_2u_3\,.$$

However, $f^{(1)}(\gamma\mathbf{u}) = f^{(2)}(\mathbf{u})$ with $\gamma = \left[\begin{smallmatrix} 1 & 0 & -18 \\ 0 & 1 & -16 \\ 0 & 0 & -1 \end{smallmatrix}\right]$ an involution. The fact that γ is not M-type is a non-trivial consequence of reduction theory and uses the fundamental sets on $\mathscr{M}_{460}(\mathbb{Z})$. Using γ in combination with the generators of the Markoff group, one can send any matrix in $\widetilde{\mathscr{M}}_{460}(\mathbb{Z})$ to any other.

(4) $\mathfrak{h}(329) = 2$, with

$$f^{(1)} = u_1^2 + u_2^2 + u_3^2 - 3u_1u_2 + 8u_1u_3 + 8u_2u_3\,,$$
$$f^{(2)} = u_1^2 + u_2^2 + u_3^2 - 4u_1u_2 + 4u_1u_3 + 11u_2u_3\,.$$

$f^{(1)}$ is anisotropic with $p = 13$ and $x_1 = -3$, while $f^{(2)}$ is isotropic with $m = 3$ and $n = 13$ with $f^{(2)}(9, 1, -1) = 0$. The two forms lie in different genera; not only are they M-type inequivalent, they are $GL(3, \mathbb{Q})$-inequivalent. The fact that they are $GL(3, \mathbb{Q})$-inequivalent gives a proof that $\mathfrak{h}(329) \geqslant 2$ without reduction theory.

5.1.2. *Some Hasse failures revisited*

We use the notation in [Pall1944]: for non-zero rational numbers a and b, and any prime p, $(a, b)_p$ has values ± 1 depending on the solvability over $\mathbb{Q}$ of the equation $ax^2 + by^2 \equiv 1 \pmod{p^r}$ for all r. The case $p = \infty$ corresponds to solvability over the reals and in all cases consider hereon, we will have $(a, b)_\infty = 1$. This is a reformulation of the Hilbert symbol over the p-adics. We state various properties that we will use repeatedly:

(1). $(a, b)_p = (a', b')_p$ if a, a' and b, b' differ multiplicatively by squares modulo prime powers of p;
(2). $(a, b)_p = (b, a)_p$;
(3). $(a, 1)_p = (a, 1 - a)_p = (a, -a)_p = 1$;
(4). $(a, a)_p = (a, -1)_p$;
(5). $(a, b_1b_2)_p = (a, b_1)_p(a, b_2)_p$;
(6). for odd p, $(a, b)_p = 1$ if a and b are units in $\mathbb{Q}_p$;
(7). for odd p, $(p^\alpha m, p^\beta n)_p = (-1|p)_J^{\alpha\beta}(m|p)_J^\beta((n|p)_J^\alpha$;
(8). $(2^\alpha m, 2^\beta n)_2 = (2|m)_J^\beta(2|n)_J^\alpha(-1)^{(m-1)(n-1)/4}$,

with integers m, n coprime to p, with α and β being 0 or 1, and $(x|y)_J$ the Jacobi symbol. One also has the validity of the product formula $\prod_{p\leqslant\infty}(a, b)_p = 1$.

The Hasse invariant $c_p(f)$ of the quadratic form $f = u_1^2 + u_2^2 + u_3^2 + x_1u_1u_2 + x_2u_1u_3 + x_3u_2u_3$ is given by $c_p(f) = C_p(x_1) = (x_1^2 - 4, k - 4)_p$, for any $(x_1, x_2, x_3) \in \mathscr{M}_k(\mathbb{Z})$. Note that $C_p(x_1) = C_p(x_2) = C_p(x_3)$ since permutations correspond to

$\mathrm{GL}(3,\mathbb{Z})$-equivalence for the forms, and the same being true for the coordinates of any Markoff-equivalent points. These invariants are well defined since we are assuming $k > 4$ is generic so that $x_j^2 - 4$ is never zero. We now derive proofs of Propositions 8.1(i,ii), 8.2 and 8.3 of Hasse failures in [**9**].

Proposition 5.4. *If $(x_1, x_2, x_3) \in \mathscr{M}_k(\mathbb{Z})$, for k generic, the product formula fails for the following choices of k:*

(i). $k = 4 + 2\nu^2$ *with ν having all of its prime factors in the congruence classes $\{\pm 1\}$ modulo 8;*

(ii). $k = 4 + 12\nu^2$ *with ν satisfying $\nu^2 \equiv 25$ (mod 32), and having all of its prime factors in the congruence classes $\{\pm 1\}$ modulo 12;*

(iii). $k = 4 + 20\nu^2$ *with ν having all of its prime factors in the congruence classes $\{\pm 1\}$ modulo 20.*

Proof.

(i). We have $C_p(x_1) = (x_1^2 - 4, 2)_p$, so that $C_p = 1$ if $p > 2$ and $p \nmid (x_1^2 - 4)$. We note that $C_2(x_1) = (2|x_1^2 - 4)_J = -1$ if x_1 is odd (since $x_1^2 - 4 \equiv -3$ modulo 8). Moreover, since $4 \nmid k$, at least one coordinate must be odd, so that $C_2 = -1$ always holds. To complete our proof, we need to ensure that $C_p = 1$ for all odd primes dividing $x_1^2 - 4$. If $p^\alpha \parallel (x_1^2 - 4)$ then $C_p(x_1) = (x_1^2 - 4, 2)_p = (2|p)_J^\alpha$. Using $A^2 - (x_1^2 - 4)(x_2^2 - 4) = 8\nu^2$, for some A, we see that if $p \nmid \nu$ and $p|(x_1^2 - 4)$, then 2 is a quadratic residue mod p, so that $C_p(x_1) = 1$ as needed. On the other hand if p divides both $x_1^2 - 4$ and ν, we cannot deduce that $(2|p)_J^\alpha = 1$, unless we force $(2|p)_J$ to equal one, which can be done if all primes factors of ν are restricted to ± 1 modulo 8. Since $C_p = -1$ for exactly one prime, the product formula is violated.

(ii , iii). We consider $k = 4 + 4q\nu^2$, where q is an odd prime not dividing ν, which is odd (q will be chosen later). Then, $C_p(x_1) = (x_1^2 - 4, q)_p$. We consider various cases:

(a). If $p \nmid 4q\nu^2$, suppose $p^\alpha \parallel (x_1^2 - 4)$ with $\alpha \geqslant 0$.then, $C_p(x_1) = (q|p)_J^\alpha = 1$ since $A^2 - (x_1^2 - 4)(x_2^2 - 4) = 4(k-4) = 16q\nu^2$ implies that q is a quadratic residue modulo p when $\alpha \geqslant 1$.

(b). If $p|\nu$, then $p \nmid q$, so using the same notation as in (a), we have $C_p(x_1) = (q|p)_J^\alpha$. We force $(q|p)_J$ to equal one. So, if $q \equiv 1$ (mod 4), we insist all prime factors of ν are congruent to quadratic residues modulo q. For $q \equiv 3$ (mod 4), we insist all prime factors of ν that are congruent to 1 (mod 4) are also quadratic residues modulo q; while those congruent to 3 (mod 4) are quadratic non-residues modulo q. This ensures that $C_p = 1$.
Example: when $q = 3$, the conditions needed are all prime factors of ν are congruent to ± 1 (mod 12), while the condition for $q = 5$ are the classes ± 1 (mod 20).

(c). The case $p = q$. If $q^\alpha \parallel (x_1^2 - 4)$, then from $A^2 - (x_1^2 - 4)(x_2^2 - 4) = 16q\nu^2$, we conclude that $\alpha = 0$ or 1. But if $\alpha = 1$ then $q \nmid ((x_2^2 - 4)(x_3^2 - 4)$, so that using x_2 or x_3 instead of x_1 leads us to consider only the case $\alpha = 0$. In that case we have $C_q(x_1) = (w^2 - 4, q)_q = (w^2 - 4|q)_J$ with $w = x_1$ or x_2 satisfying $q \nmid (w^2 - 4)$. we cannot say more without choosing special values of q,
When $q = 3$, $3 \nmid (w^2 - 4)$ implies $3|w$, so that $C_3 = (-1|3)_J = -1$.

When $q = 5$, $5 \nmid (w^2 - 4)$ if and only if $5|w$ or $w^2 - 4 \equiv 2 \pmod 5$. In the latter case, $C_5 = (2|5)_J = -1$. In the former case, $C_5 = (-4|5)_J = 1$, which is problematic ((the same is true if we had used the third coordinate and 5 divided it). We now show that this case cannot occur. Now if w is odd, then $w^2 - 4$ must have an odd prime factor $p \equiv \pm 2 \pmod 5$, and $p \nmid \nu$ from (b). Then, $A^2 - (x_1^2 - 4)(x_2^2 - 4) = 80\nu^2$ implies $(5|p)_J = 1$, a contradiction. Since w is either of two coordinates, we may now assume they are both even, so that x_1 is too. Putting $x_j = 2y_j$ gives us the equation $B^2 - (y_1^2 - 1)(y_2^2 - 1) = 5\nu^2$. If either y_1 or y_2 is odd, we have 5 is a quadratic residue (mod 8) while if both y_1 and y_2 are even, we conclude $B^2 \equiv 2 \pmod 4$. Hence these cases do not occur and $C_5 = -1$.

(d). When $p = 2$, suppose $2^\alpha \parallel (x_1^2 - 4)$. We have three cases (a). $\alpha = 0 \iff 2 \nmid x_1$, (b). $\alpha = 2 \iff 4 \| x_1$ and (c). $\alpha \geqslant 5 \iff 2 \parallel x_1$.
For case (a), $C_2(x_1) = (-1)^{(x_1^2-5)(q-1)/4} = 1$, since x_1 is odd as is q.
For case (b), writing $x_1 = 4t$, we have

$$C_2(x_1) = \left(\frac{x_1^2 - 4}{4}, q\right)_2 = (-1)^{(q-1)(2t^2-1)/2}.$$

Then $C_2 = 1$ if $q \equiv 1 \pmod 4$. For $q \equiv 3 \pmod 4$, this gives $C_2 = -1$, and we have to make sure this does not happen. This case happens when $4 \| x_j$ for all j, and so writing $x_j = 4y_j$, the Markoff equation gives $y_1^2 + y_2^2 + y_3^2 - 4y_1y_2y_3 = \frac{1+q\nu^2}{4}$. If the right side is odd, then either all y_j's are odd, or exactly one is. The left is then congruent to 7 (mod 8) or 1 (mod 4). So we restrict ν so that $\frac{1+q\nu^2}{4} \equiv 3 \pmod 8$, so that these cases of x_j do not occur. For $q = 3$, this corresponds to restricting ν to satisfy $\nu^2 \equiv 25 \pmod{32}$. Hence $C_2 = 1$.
For case (c), put $x_1^2 - 4 = 2^\alpha\lambda$, with odd λ and $\alpha \geqslant 5$. Then we have $C_2(x_1) = (2|q)_J^\alpha(-1)^{(\lambda-1)(q-1)/4}$. Now we have $B^2 - 2^{\alpha-4}\lambda(x_2^2 - 4) = q\nu^2$. If $q \equiv 3 \pmod 4$, we must have $\alpha = 5$ and x_2 odd, in which case we get $\lambda \equiv 3 \pmod 4$. Then $C_2 = (-1)^{(q^2-1)/8}(-1)^{(q-1)/2} = 1$ if $q \equiv 3 \pmod 8$. Hence $C_2 = 1$ if $q \equiv 3 \pmod 8$.
Finally, if $q \equiv 1 \pmod 4$, $C_2 = (2|q)_J^\alpha$. Then $B^2 - 2^{\alpha-4}\lambda(x_2^2 - 4) = q\nu^2$ implies $q \equiv 1 \pmod 8$ if $\alpha \geqslant 7$. we assume $q \equiv 5 \pmod 8$ to avoid this case. the case $\alpha = 6$ needs no work. Lastly if $\alpha = 5$, we get $1 - 2\lambda(x_2^2 - 4) \equiv 5 \pmod 8$, which is impossible.

For $q = 3$ and 5, we have shown $C_q = -1$ and $C_p = 1$ for all $p \neq q$, violating the product formula. □

5.1.3. *Hasse failures over S-integers*

We construct Hasse failures on the surface $\mathscr{M}_k(\mathbb{Z}[\frac{1}{\ell}])$ when ℓ is an odd prime satisfying $\ell \geqslant 5$ and some $k \in \mathbb{Z}$. By Prop. 6.1 of [**9**], the Markoff surface has solutions in $\mathbb{Z}/p^n\mathbb{Z}$ for all primes p and integers $n \geqslant 1$ except for those k's with congruence obstructions, coming from $p = 2$ or 3. Hence the congruence is solvable over $\mathscr{M}_k(\mathbb{Z}[\frac{1}{\ell}])$ when $p \neq 2,\ 3$. Since $\ell \neq 2,\ 3$, the congruence modulo p^n over $\mathbb{Z}$ is equivalent to that over $\mathbb{Z}[\frac{1}{\ell}]$ when $p = 2$ or 3. Hence, there are no congruence obstructions if k is not congruent to 3 (mod 4) and $\pm 3 \pmod 9$.

Lemma 5.5. *Suppose $\mathscr{M}_k(\mathbb{Z}[\frac{1}{\ell}])$ is non-empty. Then either there is an integer lattice point in $\mathscr{M}_k(\mathbb{Z}[\frac{1}{\ell}])$ or if not, there is a point of the form $(x_1, \frac{x_2}{\ell^a}, \frac{x_3}{\ell^a})$ with integers x_j where $\ell \nmid x_2x_3$, and $a \geqslant 1$.*

Proof. Consider the equation

$$\left(\frac{x_1}{\ell^a}\right)^2 + \left(\frac{x_2}{\ell^b}\right)^2 + \left(\frac{x_3}{\ell^c}\right)^2 - \left(\frac{x_1x_2x_3}{\ell^{a+b+c}}\right) = k, \tag{5.1.1}$$

with integers a, b, c and with $\ell \nmid x_1x_2x_3$.

If $\max(a, b, c) \geqslant 1$, then by checking denominators, we may assume that either $\min(a, b, c) \geqslant 1$ or $a \leqslant 0$, with $b,\ c \geqslant 1$.

Suppose there is a solution with $\min(a, b, c) \geqslant 1$. Rearranging the coordinates, we assume $a \leqslant b \leqslant c$, and among such triples, we choose one with minimal c. Comparing denominators implies that $a + b = c$ so that (5.1.1) becomes

$$\left(\frac{x_1}{\ell^a}\right)^2 + \left(\frac{x_2}{\ell^b}\right)^2 + \frac{x_3(x_3 - x_1x_2)}{\ell^{2(a+b)}} = k.$$

If $a \leqslant b$, we conclude that $\ell^{2a} \mid (x_3 - x_1x_2)$. Then, the point $\left(\frac{x_1}{\ell^a}, \frac{x_2}{\ell^b}, \frac{(x_1x_2-x_3)/\ell^{2a}}{\ell^{b-a}}\right)$ has exponents in ℓ less than c. This contradicts the minimal choice of c unless $a = b$, in which case we have a point with a coordinate over $\mathbb{Z}$. So we can assume that in (5.1.1) we have a point with $a \leqslant 0$, and $b,\ c \geqslant 1$, and checking denominators, conclude that $b = c$. □

Proposition 5.6. *Suppose ℓ is a prime satisfying $\ell \equiv \pm 1$ (mod 8). Let $k = 4 + 2\nu^2$ with ν having all of its prime factors in the congruence classes $\{\pm 1\}$ modulo 8, and in addition with $\nu \in \{0,\ \pm 3,\ \pm 4\}$ modulo 9. Then k is a Hasse-failure in $\mathbb{Z}[\frac{1}{\ell}]$.*

Proof. The conditions on ν ensures that there are no congruence obstructions in $\mathbb{Z}[\frac{1}{\ell}]$. By Prop. 8.1(b) of **[9]** (or Prop.5.4 (i)), there are no integral points. Applying Lemma 5.5 and clearing denominators gives us

$$(2x_2 - x_1x_3)^2 - 8\nu^2\ell^{2a} = (x_1^2 - 4)(x_3^2 - 4\ell^{2a}).$$

Since at least two of the x_j's must be odd, we have chosen x_3 to be odd. Then, $x_3^2 - 4\ell^{2a} \equiv -3 \pmod 8$, so that there must be a prime $q \equiv \pm 3 \pmod 8$ dividing the right hand side. Since $q \nmid \nu\ell$, we get a contradiction as the equation implies that 2 is a quadratic residue modulo q. □

Proposition 5.7. *Suppose ℓ is an odd prime satisfying $\ell \equiv \pm 1$ (mod 5). Let $\nu \equiv \pm 4$ (mod 9), with all prime factors congruent to ± 1 (mod 20). Then, $k = 4 + 20\nu^2 \in \mathbb{Z}$ is a Hasse-failure in $\mathbb{Z}[\frac{1}{\ell}]$.*

Proof. By the preamble above, these k's have no congruence obstructions. So it suffices to show that there are no lattice points in $\mathscr{M}_k(\mathbb{Z}[\frac{1}{\ell}])$. By Prop. 8.3 of **[9]** (or Prop.5.4 (iii)), there are no integeral lattice points, so that by Lemma 5.5 we have (5.1.1) in the form

$$x_1^2 + \left(\frac{x_2}{\ell^a}\right)^2 + \left(\frac{x_3}{\ell^a}\right)^2 - \frac{x_1x_2x_3}{\ell^{2a}} = k = 4 + 20\nu^2, \tag{5.1.2}$$

with $x_1, x_2, x_3 \in \mathbb{Z}$, $a \geqslant 1$, and $\ell \nmid x_2x_3$. We see that x_1, $\frac{x_2}{\ell^a}$ and $\frac{x_3}{\ell^a}$ are not equal to ± 2, so that we can apply the method considered above involving Hasse invariants. Exactly as we considered before, the Hasse invariants $c_p(f)$ are of the form $C_p(u_i) = (u_i^2 - 4, 5)_p = (x_i^2 - 4\ell^{2a_i}, 5)_p$, where we have written $u_i = \frac{x_i}{\ell^{a_i}}$ with

$a_i = 0$ or a as given above in (5.1.2) (but not necessarily in that order). Completing the square gives $A^2 - (x_1^2 - 4\ell^{2a_1})(x_2^2 - 4\ell^{2a_2}) = 5(4\ell^{a_1+a_2}\nu)^2$, all integers. We now follow the same procedure as in Prop. 5.4 (iii) above, where we give the details for completeness.

(a). If $p \nmid 10\ell\nu$, then 5 is a quadratic residue modulo p when $p^\alpha \parallel (x_j^2 - 4\ell^{2a_j})$ for any j with $\alpha \geqslant 1$. For such a j we have $C_p(u_j) = (5, p)_j^\alpha = 1$. On the other hand, if $p \nmid (x_j^2 - 4\ell^{2a_j})$, then $\alpha = 0$ so that $C_p(u_j) = 1$.

(b). If $p|\nu$, using the same notation as in (a), we have $C_p(u_j) = (5|p)_j^\alpha = (p|5)_j^\alpha = 1$.

(c). When $p = \ell$, there are two cases to consider namely when $a_j = 0$ and when $a_j \geqslant 1$. For the latter $C_\ell(u_j) = (x_j^2 - 4\ell^{2a_j}, 5)_\ell = (x_j^2\ , 5)_\ell = 1$. Since at least one of the a_j's is non-zero, we may permute the coefficients and get this value for C_ℓ.

(d). If $p = 5$, $(x_j^2 - 4\ell^{2a_j}) \equiv x_j^2 - 4 \pmod 5$, so that on replacing ν with $\nu_1 = \ell^{a_i+a_j}\nu$, noting that $\nu_1 \equiv \pm\nu \pmod 5$ and $\nu_1^2 \equiv \nu^2 \pmod 8$, we have exactly the same equations as in the case considered in Prop. 5.4 (iii, c) with $q = 5$, so that $C_5 = -1$.

(e). When $p = 2$, suppose $2^\alpha \parallel (x_1^2 - 4\ell_1^a)$. We have three cases: (a). $\alpha = 0 \iff 2 \nmid x_1$, (b). $\alpha = 2 \iff 4 \| x_1$ and (c). $\alpha \geqslant 5 \iff 2 \parallel x_1$.
For case (a), $C_2(u_1) = (-1)^{(x_1^2 - 4\ell^{2a_1} - 1)(5-1)/4} = 1$, since x_1 is odd.
For case (b), writing $x_1 = 4t$, we have

$$C_2(u_1) = \left(\frac{x_1^2 - 4\ell^{2a_1}}{4}, 5\right)_2 = (-1)^{(5-1)(4t^2 - \ell^{2a_1} - 1)/4} = 1.$$

For case (c), put $x_1^2 - 4\ell^{2a_1} = 2^\alpha\lambda$, with odd λ and $\alpha \geqslant 5$. Then we have $C_2(u_1) = (2|5)_j^\alpha(-1)^{(\lambda-1)(5-1)/4} = (-1)^\alpha$.
Since $A^2 - (x_1^2 - 4\ell^{2a_1})(x_2^2 - 4\ell^{2a_2}) = 80\nu_1^2$, we have $A_1^2 - 2^{\alpha-4}\lambda(x_2^2 - 4\ell^{2a_2}) = 5\nu_1^2$, with A_1 odd. Then, if $\alpha \geqslant 7$, we have $A_1^2 \equiv 5\nu_1^2 \equiv 5 \pmod 8$, a contradiction. If $\alpha = 6$, clearly $C_2(u_1) = 1$. Finally if $\alpha = 5$, we get $1 - 2\lambda(x_2^2 - 4\ell^{2a_2}) \equiv 5 \pmod 8$, which is impossible. Hence $C_2(u_1) = 1$.

We thus see that the product formula is violated, proving the proposition.

□

Matrices that are commutators give rise to points on the Markoff surface, and checking admissibility in (3.2.2) (see Prop. 5.12), we have

Proposition 5.8. *Let ℓ be an odd prime satisfying $\ell \equiv \pm 1$ (mod 5). Then, there are infinitely many Hasse failures for $(\mathscr{C}_2)$ over $D = \mathbb{Z}[\frac{1}{\ell}]$. In particular, if $t = 2 + 20\nu^2$ with ν as above, then t is admissible but is a Hasse failure.*

5.2. Hasse failures for commutators

Our purpose here is to construct failures to the Hasse principle for the commutator problem $(\mathscr{C}_1)$: construct matrices Z in an arithmetic group Γ_D over a ring D that are commutators in congruence subgroups, that lie in the commutator subgroup but that are not commutators (see the discussion in Section 3.2). Since we have constructed Hasse failures $\mathscr{M}_k(D)$ for certain infinite family of k's, for $D = \mathbb{Z}$ and $\mathbb{Z}[\frac{1}{\ell}]$ for some primes ℓ, it is natural to want to extend these to matrices with trace $t = k - 2$. It turns out that this does not always produce Hasse failures for the matrix problem as sometimes a Hasse failure $\mathscr{M}_k(D)$ corresponds to a congruence

obstruction in $(\mathscr{C}_1)$ and $(\mathscr{C}_2)$ for matrices with trace $t = k - 2$. We first give some exampes of these in Prop. 5.11, and then construct some Hasse failures for $(\mathscr{C}_1)$.

Lemma 5.9.

(a). *Suppose* $t \equiv 2\varepsilon \pmod q$ *with* $\varepsilon = \pm 1$ *and* $Z = \left[\begin{smallmatrix} \alpha & \beta \\ \gamma & t-\alpha \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$. *Then, if* $(\beta, q) = 1$, *there is a* $M \in \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ *with*

$$Z \equiv M \begin{bmatrix} \varepsilon & \beta^{-1} \\ 0 & \varepsilon \end{bmatrix} M^{-1} \pmod q.$$

(b). *For* $q = 2,\ 3,\ 4$, *if* $Z \in \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ *is congruent to* $\left[\begin{smallmatrix} 1 & s \\ 0 & 1 \end{smallmatrix}\right]$ *(or its transpose) modulo* q, *for some* s *coprime to* q, *then* Z *cannot be a commutator.*

Proof. For (a), take $M = \left[\begin{smallmatrix} \beta & 0 \\ \varepsilon - \alpha & \beta^{-1} \end{smallmatrix}\right]$.

For (b), it suffices to check one case; otherwise consider the transpose of Z. Write $Z = XYX^{-1}Y^{-1}$ with $X, Y \in \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$. Computing the traces $\mathrm{Tr}(ZY) \equiv \mathrm{Tr}(Y) \pmod q$ and $\mathrm{Tr}(ZX^{-1}) \equiv \mathrm{Tr}(X) \pmod q$, we conclude that X and Y are upper-triangular $(\mathrm{mod}\ q)$. With our choices of q, the diagonal entries must be congruent to $\varepsilon = \pm 1$ so that X and Y commute, giving $Z \equiv I_2 \pmod q$, a contradiction. □

Remark 5.10. The congruence obstructions above over $\mathbb{Z}$ also lead to congruence obstructions over $\mathbb{Z}[\frac{1}{\ell}]$ for $\ell \equiv \pm 1 \pmod 8$ for the first case, and $\ell \equiv \pm 1 \pmod{12}$ for the second.

Lemma 5.11. *For* $Z \in \mathrm{SL}_2(\mathbb{Z})$, *let* $t = \mathrm{Tr}(Z)$. *Then* Z *is not a commutator if* (a). $4 | t$ *or* (b). $t \equiv \pm 1, \pm 4 \pmod 9$.

Proof. Suppose there exist matrices $X,\ Y \in \mathrm{SL}_2(\mathbb{Z})$ such that $Z = XYX^{-1}Y^{-1}$. We write $Z = \left[\begin{smallmatrix} \alpha & \beta \\ \gamma & t-\alpha \end{smallmatrix}\right]$.

(a). If β is odd, then by Lemma 5.9(a), with $q = 2$, we may replace Z with $\left[\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right]$ (mod 2), and then with Lemma 5.9(b) conclude that Z is not a commutator. The same reasoning holds if γ was odd by transposing. So we can assume that both β and γ are even, so that $4|t$ implies that the determinant is $-\alpha^2 \equiv 1 \pmod 4$, a contradiction.

(b). We use the same argument as above with $q = 3$, $t = 2\varepsilon + 3s$, and $\varepsilon = \pm 1$. Then, 3 dividing both β and γ implies that $\alpha(t - \alpha) \equiv 1 \pmod 9$. Then, $(\alpha - \varepsilon - 6s)^2 \equiv 12\varepsilon s \pmod 9$, giving a contradiction when $3 \nmid s$. □

The admissible t's for $\mathscr{T}_t(\mathbb{Z})$ may be described as follows:

let $\mathscr{V}$ be the affine variety in $\mathbb{A}^8$ given by the equations

$$X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, \quad Y = \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix}, \quad \det X = \det Y = 1,$$

and let $f(\mathbf{x}, \mathbf{y}) = \mathrm{Tr}(XYX^{-1}Y^{-1})$, with $\mathbf{x} = (x_1, x_2, x_3, x_4)$ and $\mathbf{y} = (y_1, y_2, y_3, y_4)$. The obstructions $\pmod{p^l}$, with p a prime and $l \geqslant 1$ an integer, to $t \equiv f(\mathbf{x}, \mathbf{y})$ $\pmod{p^l}$ having a solution is equivalent to describing the image in the p-adic integers $\mathbb{Z}_p$ of f, that is $f(\mathscr{V}(\mathbb{Z}_p))$.

By general principles of quantifier elimination for the p-adics ([**6**]), $f(\mathscr{V}(\mathbb{Z}_p))$ has an effective and explicit description for each $p \geqslant 2$.

Proposition 5.12.
(a). *For* $\mathfrak{p} > 3$, $\mathfrak{f}(\mathcal{V}(\mathbb{Z}_\mathfrak{p})) = \mathbb{Z}_\mathfrak{p}$, *that is there are no local obstructions for* $\mathfrak{t}$ *in* $\mathbb{Z}_\mathfrak{p}$.
(b). *For* $\mathfrak{p} = 3$, *there are obstructions for* $\mathfrak{t} \equiv 1, 4, 5, 8 \pmod{3^2}$.
(c). *For* $\mathfrak{p} = 2$, *there are obstructions for* $\mathfrak{t} \equiv 0, 1, 4, 5, 8, 9, 10, 12, 13 \pmod{2^4}$.

Remark 5.13. Preliminary calculations indicate that the obstructions $\pmod{3^2}$ and $\pmod{2^4}$ are the only ones for $\mathbb{Z}_3$ and $\mathbb{Z}_2$ respectively, that is the admissible $\mathfrak{t}$'s for $\mathcal{T}_\mathfrak{t}(\mathbb{Z})$ are as in (3.2.2).

Proof of Prop. 5.12. By Example 4.3(1) in Section 4, or by Lemma 6.2 of **[9]**, there are no congruence obstructions on $\mathfrak{t}$ modulo prime powers $\mathfrak{p} > 3$, which proves the first statement. For $\mathfrak{p} = 3$, the obstructions listed are those in Lemma 5.11. For $\mathfrak{p} = 2$, we have the obstruction $\mathfrak{t} \equiv 1 \pmod 4$ coming from the Markoff equation with $\mathfrak{t} = \mathfrak{k} - 2$, while the $\mathfrak{t} \equiv 0 \pmod 4$ obstruction follows from Lemma 5.11. That leaves the case $\mathfrak{t} \equiv 10 \pmod{16}$. A matrix $\mathsf{Z} \in \mathrm{SL}_2(\mathbb{Z}_2)$ (or its transpose) with trace $\mathfrak{t}$ is either equivalent to $\mathsf{A} = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \pmod 2$ or equivalent to $\mathsf{B} = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right] \pmod 4$ or satisfies $\mathsf{Z} \equiv \mathrm{I} \pmod 4$. One checks directly that A is not a commutator $\pmod 2$, and neither is $\mathsf{B} \pmod 4$. Hence if Z is a commutator $\pmod{16}$, then $\mathsf{Z} \equiv \mathrm{I} \pmod 4$, from which it follows that $\mathfrak{t} \equiv 2 \pmod{16}$.

□

Remark 5.14. The Hasse failures for $\mathscr{M}_\mathfrak{k}(\mathbb{Z})$ constructed in Prop. 5.4 of the type $\mathfrak{k} = 4 + 2\nu^2$ and $4 + 12\nu^2$ do not lift to Hasse failures for $(\mathscr{C}_1)$ and $(\mathscr{C}_2)$, since the corresponding $\mathfrak{t}$'s are not admissible (with $4|\mathfrak{t}$ in the former, and $\mathfrak{t} \equiv 5 \pmod 9$ in the latter).

We now extend Prop. 5.8 and construct matrices that are Hasse failures to the commutator problem in the Ihara groups $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{\ell}])$ for primes $\ell \equiv \pm 1 \pmod 5$.

Theorem 5.15. *Suppose* ℓ *is an odd prime satisfying* $\ell \equiv \pm 1$ *(mod 5) and put* $\mathbb{D} = \mathbb{Z}[\frac{1}{\ell}]$. *Put* $\mathfrak{t} = 2 + 20\nu^2$, *where* $\nu \equiv 4$ *(mod 27) and with* ν *having all prime factors congruent to* $\pm 1 \pmod{20}$. *Let*

$$\mathsf{A} = \begin{bmatrix} \mathfrak{t} - 5 & \frac{2}{3}(5\nu - 2) \\ 6(5\nu + 2) & 5 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{D}).$$

Then, A *is a commutator in every finite (congruence) quotient of* $\mathrm{SL}_2(\mathbb{D})$, *but* A *is not a commutator in* $\mathrm{SL}_2(\mathbb{D})$.

Consequently, there are infinitely many Ihara groups, each containing infinitely many Hasse failures.

Proof. By Prop. 5.8, we know that A is not a commutator in $\mathrm{SL}_2(\mathbb{D})$. Since all the finite quotients of $\Gamma_\mathbb{D}$ are congruence quotients (**[15]**,**[22]**), to show that A is a Hasse-failure it remains to verify that A is a commutator locally for all primes $\mathfrak{p} \geqslant 2$ (note that since $\mathsf{A} \in \mathrm{SL}_2(\mathbb{Z})$, we do not have to consider the case $\mathfrak{p} = \ell$ separately). We have $\mathsf{A} \equiv \mathrm{I} \pmod 2$, $\mathsf{A} \equiv -\mathrm{I} \pmod 3$ and $\mathsf{A} \not\equiv \pm\mathrm{I} \pmod{\mathfrak{p}}$ for all primes $\mathfrak{p} \geqslant 5$. Thus, by Theorem 3.5 of **[2]**, our conclusion holds for $\mathfrak{p} \geqslant 5$, so that it remains to check the cases $\mathfrak{p} = 2$ and 3.

We write $\mathsf{A} = \mathrm{I} + 2\mathsf{B}$, where $\mathsf{B} = \left[\begin{smallmatrix} \mathfrak{b}_1 & \mathfrak{b}_2 \\ \mathfrak{b}_3 & \mathfrak{b}_4 \end{smallmatrix}\right] \in \mathbb{M}_2(\mathbb{Z})$ with $\mathfrak{b}_1 = 2(5\nu^2 - 1)$, $\mathfrak{b}_2 = \frac{1}{3}(5\nu - 2)$, $\mathfrak{b}_3 = 3(5\nu + 2)$ and $\mathfrak{b}_4 = 2$. We use the following properties of the coefficients extensively: modulo 2, we have $2|\mathfrak{b}_1$, $2\|\mathfrak{b}_4$, $2\|(\mathfrak{b}_1 - \mathfrak{b}_4)$ with $\mathfrak{b}_2$, $\mathfrak{b}_3$ odd; and modulo 3 we have $3 \nmid \mathfrak{b}_1\mathfrak{b}_4$, $3\|\mathfrak{b}_2$, $3\|\mathfrak{b}_3$ and $3\|(\mathfrak{b}_1 - \mathfrak{b}_4)$.

For the powers 2^n with $n \geqslant 2$, we appeal to Lemma 3.5 with $D = \mathbb{Z}/2^n\mathbb{Z}$. Since $t + 2 \equiv 0 \pmod 4$, $(1, 1, 1) \in \mathscr{M}_{t+2}(\mathbb{Z})$ is a non-singular solution modulo 2 and Hensel's lemma lifts this solution modulo 2^n (see Sec. 6 of [**9**]). Thus, we may choose x_2 to be odd in Lemma 3.5 so that Δ is invertible in D, giving $X \in \Gamma_D$. So we need to find $Y \in \Gamma_D$ satisfying $\operatorname{Tr} AY \equiv \operatorname{Tr} Y \equiv x_2 \pmod{2^n}$. Writing $Y = \left[\begin{smallmatrix} x_2 - y_1 & y_2 \\ y_3 & y_1 \end{smallmatrix}\right]$, we seek y_j satisfying the two equations $y_1(x_2 - y_1) - y_2y_3 \equiv 1$ and $b_1(x_2 - y_1) + b_3y_2 + b_2y_3 + b_4y_1 \equiv 0 \pmod{2^{n-1}}$. Since x_2 is odd, we have y_2 and y_3 odd, so that the two equations combine with a need to solve $b_3y_2^2 + (b_4 - b_1)y_1y_2 - b_2y_1^2 + b_1x_2y_2 + b_2x_2y_1 \equiv b_2 \pmod{2^{n-1}}$ with y_1 free and y_2 odd. Since b_2 and b_3 are odd, there are no solutions here for even y_2's and so we may drop the restriction that y_2 should be odd if $n \geqslant 2$. Completing the square, and using the fact that b_1 and b_4 are even, the equation to solve is equivalent to the equation $u^2 - \delta v^2 + \sigma v \equiv b_2b_3 + \left(\frac{b_1x_2}{2}\right)^2 \pmod{2^{n-1}}$, where $\delta = 5v^2(5v^2 + 1)$ is divisible exactly by 2, and σ is odd. Using Gauss sums, one shows that this equation has 2^{n-1} solutions, giving the existence of Y (alternatively one can appeal to Hensel's lemma, since the equation has trivially a non-singular solution modulo 2 that lifts to modulo 2^{n-1}). When $n = 1$, $A \equiv I$ is a commutator.

For $l = 3$, we are unable to use Lemma 3.5 directly since Δ is always divisible by 3, but we are able to use the proof of the lemma to deduce our result. We start with a non-singular solution $(x_1, x_2, x_3) \equiv (3, 3, 3) \pmod 9$ and extend this using Hensel's lemma to modulo 3^{n+2}, with $n \geqslant 0$ (see [**9**] Sec.6). Then, $\Delta = t + 2 - x_2^2 \equiv -9 \pmod{27}$, so that $9 \| \Delta$. The construction of X is then valid with $|X| \equiv 1 \pmod{3^{n-2}}$, this being so since in (3.1.12) we have 9 dividing the right-hand-side using $A \equiv -I \pmod 3$ and $3|x_j$ for all j. Thus, if $n \geqslant 2$, A will be a commutator modulo 3^{n-2} provided we can find a Y with $\operatorname{Tr} AY \equiv \operatorname{Tr} Y \pmod{3^{n+2}}$ with $|Y| \equiv 1 \pmod{3^{n+2}}$. To find Y, we follow the same strategy as the case above: we seek y_i such that $y_1(x_2 - y_1) - y_2y_3 \equiv 1$ and $b_1(x_2 - y_1) + b_3y_2 + b_2y_3 + b_4y_1 \equiv 0 \pmod{3^{n+2}}$. Since $3|x_2$, we must have $3 \nmid y_2y_3$ so that we are reduced to finding y_1 and y_2 satisfying $\frac{b_3}{3}y_2^2 + \frac{b_4 - b_1}{3}y_1y_2 - \frac{b_2}{3}y_1^2 + b_1\frac{x_2}{3}y_2 + \frac{b_2}{3}x_2y_1 \equiv \frac{b_2}{3} \pmod{3^{n+1}}$ with $3 \nmid y_2$. We may drop this latter condition as there are no solutions with $3|y_2$. Since $3 \| b_3$, we complete the square and obtain an equation of the type $u^2 - \delta v^2 + \sigma v \equiv \tau \pmod{3^{n+1}}$, where $3|\delta$ and $3 \nmid \sigma$. This is exactly as in the case above, and Hensel's lemma gives a solution lifted from a non-singular one modulo 3. Thus, the required Y exists modulo 3^{n+2}, so that A is a commutator modulo 3^{n-2} for all $n \geqslant 2$.

□

Appendix

A. Preliminaries

We put here some general information that will be used repeatedly without comment.

Notation A.1. D will be an integral domain and F a field (finite or not).

$\mathbb{M}_2(S)$ will denote 2×2 matrices with entries in the set S, and $\Gamma_S = \mathrm{SL}_2(S)$.

For $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathbb{M}_2(D)$, we put $A' = \left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right]$, and I to denote the identity matrix.

$W(A, B) = ABA^{-1}B^{-1}$ for $A,\ B\ \in \Gamma_D$.

Lemma A.2. *For* $A,\ B \in \mathbb{M}_2(D)$*, we have*
(i). $A + A' = (\operatorname{Tr} A)I$,
(ii). $AA' = |A|I$,
(iii). $A^2 = (\operatorname{Tr} A)A - |A|I$ *and* $A'^2 = (\operatorname{Tr} A)A' - |A|I$,
(iv). $|A + B| = |A| + |B| + \operatorname{Tr} AB'$.

Proposition A.3. *Let* $X,\ Y \in \Gamma_D$*, with* $x_1 = \operatorname{Tr} X$*,* $x_2 = \operatorname{Tr} Y$ *and* $x_3 = \operatorname{Tr} XY$*. Then*

$$W(X, Y) = x_3XY + (x_1 - x_2x_3)X + x_2Y^{-1} - I. \tag{A.0.1}$$

Proof. We have

$$\begin{aligned} W(X, Y) = XYX^{-1}Y^{-1} &= XY(-X + x_1I)Y^{-1}, \\ &= -(XY)^2Y^{-2} + x_1X, \\ &= -(x_3XY - I)(x_2Y^{-1} - I) + x_1X, \end{aligned}$$

from which the result follows on expanding. □

Remark A.4. Taking trace of (A.0.1) gives the Fricke identity, and so the Markoff equation $M(x_1, x_2, x_3) = x_1^2+x_2^2+x_3^2-x_1x_2x_3 = k$. We say $\mathbf{x} = (x_1, x_2, x_3) \in \mathscr{M}_k(D)$ with $k = \operatorname{Tr} W(X, Y) + 2$.

Remark A.5. If $W(X, Y) \neq I$, then the coefficients in (A.0.1) are uniquely determined in the following sense: if $W(X, Y) = \alpha XY + \beta X + \delta Y^{-1} - I$, then $\alpha = \operatorname{Tr} XY$, $\beta = \operatorname{Tr} X - \operatorname{Tr} Y \operatorname{Tr} XY$ and $\gamma = \operatorname{Tr} Y$. This is because if we suppose not, subtracting from (A.0.1) gives $(x_3 - \alpha)XY = s_1X + t_1Y^{-1}$, for some $s_1,\ t_1 \in D$ not both zero. Since $W(X, Y) \neq I$, we have $\alpha \neq x_3$, so that $XY = s_2X + t_2Y^{-1}$ for some s_2 and t_2, so that $X(Y - s_2I) = t_2Y^{-1}$. If $|Y - s_2I| = 0$, we have $t_2 = 0$, so that $Y = s_2I$, giving $W(X, Y) = I$. Hence, $X = t_2Y^{-1}(Y - s_2I)^{-1}$. But $(Y - s_2I)(Y^{-1} - s_2I) = (s_2^2 - x_2s_2 + 1)I \neq 0$. Hence X is a linear combination of Y^{-1} and Y^{-2}, and so commutes with Y, giving $W(X, Y) = I$. This provides the contradiction.

Definition A.6. For a matrix A defined over D, we let $\mathfrak{S}(A)$ denote the set over D given by

$$\mathfrak{S}(A) = \{X : \operatorname{Tr} AX = \operatorname{Tr} X\ , |X| = 1\}.$$

Lemma A.7. *Let* $X,\ Y,\ Z \in \Gamma_D$*. Suppose* D *is an integral domain and* $\operatorname{Tr} Z \neq 2$ *or* D *is a ring with* $\operatorname{Tr} Z - 2 \in D^\times$*. Then*

$$Z = W(X, Y) \quad \textit{if and only if} \quad Y \in \mathfrak{S}(Z),\ \textit{and}\ X,\ XY \in \mathfrak{S}(Z^{-1}).$$

Proof. That the left implies the right is immediate.

We now assume the right and put $\operatorname{Tr} Z = t$. We convert the trace equations on the right to matrix form using Lemma A.2, giving
(i). $ZY = Y + Y^{-1} - Y^{-1}Z^{-1}$,
(ii). $Z^{-1}X = X + X^{-1} - X^{-1}Z$, and
(iii). $XY + Y^{-1}X^{-1} = Z^{-1}XY + Y^{-1}X^{-1}Z$.
Substituting the first two into the third, and using Lemma A.2(i) to replace Z^{-1} with Z, and simplifying, gives

$$(Y^{-1}X^{-1} - X^{-1}Y^{-1})Z = Y^{-1}X^{-1} + (1 - t)X^{-1}Y^{-1}.$$

Multiplying with XY and putting $W(X,Y) = W$ gives

$$(I - W)Z = I + (1-t)W\ .$$

All of the above is true for any t. In what follows, we assume $t \neq 2$.

We take determinants of both sides: $|I - W| = 2 - \operatorname{Tr} W$, and $|I + (1-t)W| = 1 + (1-t)^2 + (1-t)\operatorname{Tr} W$. Equating the two gives $\operatorname{Tr} W = t$. Then multiplying both sides of the equation with $(I - W')$ and simplifying gives $(2-t)Z = (2-t)W$, from which the result follows. □

Remark A.8. Combining Lemmas A.3 and A.7 shows that $-I$ is a commutator in D if and only if there exist matrices X and $Y \in \Gamma_D$ such that $\operatorname{Tr} X = \operatorname{Tr} Y = \operatorname{Tr} XY = 0$, in which case $-I = W(X,Y)$. Finding such X and Y satisfying the trace equations is problematic in general as it requires solving simultaneously three quadratic equations over D, coming from $\operatorname{Tr} XY = 0$ and $|X| = |Y| = 1$. It is straightforward to see that $-I$ is not a commutator in $\mathrm{SL}_2(\mathbb{R})$, and hence not in any subring.

For a PID, one can say more. Suppose $r_1^2 + r_2^2 + r_3^2 = 0$ with $r_j \in D$ not all zero. Choose r_1 and r_2 so that $\gcd(r_1, r_2) = 1$. Pick u and $v \in D$ such that $r_1 u - r_2 v = 1$. Put $X = \begin{bmatrix} u r_3 & u^2 r_2 + v(r_1 u + 1) \\ r_2 & -u r_3 \end{bmatrix}$ and $Y = \begin{bmatrix} v r_3 & v^2 r_1 + u(r_2 v - 1) \\ r_1 & -v r_3 \end{bmatrix}$, both in Γ_D. Then $W(X,Y) = -I$. Conversely, given the latter, by equating the traces and determinants, we get a non-trivial solution to the sum of three squares being zero.

B. Local analysis

Lemma B.1 (Elementary)**.** *Let p be an odd prime and $\chi(.)$ the Legendre symbol mod p.*

(i). *The number of solutions to $x^2 - \Delta y^2 \equiv n$ (mod p) is*

$$= \begin{cases} [1 + \chi(n)]p & \text{if } p \nmid n \text{ and } p|\Delta\ , \\ p - \chi(\Delta) & \text{if } p \nmid n \text{ and } p \nmid \Delta\ , \\ p[1 + \chi(\Delta)] - \chi(\Delta) & \text{if } p|n\ . \end{cases}$$

(ii). *Let $\Delta = b^2 - 4ac$. Then*

$$\sum_{m,n \pmod p} e_p(am^2 + bmn + cn^2) = \begin{cases} \chi(\Delta)p & \text{if } p \nmid \Delta\ , \\ \chi(a)pS_p & \text{if } p \nmid a \text{ or } c, \text{ and } p|\Delta\ , \\ p^2 & \text{if } p|a\ , b \text{ and } c\ , \end{cases}$$

where $S_p = \sum_x e_p(x^2)$ is the Gauss sum.

Lemma B.2. *For $p \geqslant 3$ a prime, let $\Gamma = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. For any ζ with $p \nmid \zeta$, let $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} a & b\zeta \\ c\zeta^{-1} & d \end{smallmatrix}\right]$ be in Γ. Then, if $A \neq \pm I$, $\operatorname{Tr} A \equiv \pm 2$ and ζ is a QNR (mod p), A and B are not conjugates in Γ, and otherwise A and B are Γ-conjugates.*

Proof. We seek $\gamma = \left[\begin{smallmatrix} \gamma_1 & \gamma_2 \\ \gamma_3 & \gamma_4 \end{smallmatrix}\right]$ in Γ satisfying $\gamma A = B\gamma$. If $p|b$ and $p|c$, take $\gamma = I$. So, we assume $p \nmid c$; otherwise we transpose everything. This leads to the equation

$$c\gamma_1^2 - (d - a)\zeta\gamma_1\gamma_3 - b\zeta^2\gamma_3^2 = c\zeta,$$

with discriminant $\Delta = (\operatorname{Tr} A)^2 - 4$, with γ_2 and γ_4 determined. We apply Lemma B.1 with $n = 4c^2\zeta$.

If $\operatorname{Tr} A \equiv \pm 2 \pmod{p}$, and if ζ is a quadratic nonresidue, there are no solutions so that A and B are not conjugates. Otherwise there are solutions and A and B are Γ-conjugates. □

Lemma B.3. *For $p \geqslant 3$ a prime and $\Gamma = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, if $t \not\equiv \pm 2 \pmod{p}$, there is exactly one conjugacy class with trace t in Γ, with representative $\left[\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right]$.*

Proof. Let $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma$. First, we verify that A, A^{-1} and $A^\intercal$ are all Γ-conjugates. Conjugating with $S = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ shows that A^{-1} and $A^\intercal$ are conjugates. Then, if $p \nmid bc$, taking $\zeta = \frac{c}{b}$ in Lemma B.2 shows that A is conjugate to them too. If $p \nmid b$ and $p \mid c$, we have $p \nmid (a - a^{-1})$ and conjugating A with $\left[\begin{smallmatrix} b & (1+b^2)/(a-a^{-1}) \\ -(a-a^{-1}) & -b \end{smallmatrix}\right]$ gives A^{-1}.

Now if $p \nmid b$ or $p \nmid c$, conjugating A (or its transpose) with an upper triangular matrix gives rise to a matrix of the form $\left[\begin{smallmatrix} 0 & b \\ -b^{-1} & t \end{smallmatrix}\right] \in \Gamma$, which by Lemma B.2 is equivalent to $\left[\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right]$. If $p \mid b$ and $p \mid c$, conjugating with $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$ gives $\left[\begin{smallmatrix} a & a-d \\ 0 & d \end{smallmatrix}\right]$. Since $p \nmid a - d$, as otherwise $\operatorname{Tr} A = \pm 2$, the argument above again leads to the matrix $\left[\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right]$. □

Remark B.4. This lemma is related to the following.

Let K be a field of characteristic not 2, $Z \in \Gamma_F$, $\operatorname{Tr} Z = t$ with $t \neq \pm 2$. Then, Z or $Z^{-1} \sim \left[\begin{smallmatrix} 0 & \alpha \\ -\alpha^{-1} & t \end{smallmatrix}\right]$ for some $\alpha \neq 0$.

If F is a field with the following property: there exists an $\omega \in F^\times/\square_F$ such that $F = \square_F \cup w\square_F$, where $\square_F$ denotes the squares in F. Then Z or $Z^{-1} \sim \left[\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right]$ if $x^2 - (t^2 - 4)y^2 = \omega$ is solvable with $(x, y) \in F^2$. Otherwise Z or $Z^{-1} \sim \left[\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & \omega \\ -\omega^{-1} & t \end{smallmatrix}\right]$, the latter two being inequivalent.

References

[1] M. Abért and P. Hegedűs. On the number of generators needed for free profinite products of finite groups. *Israel Jour. Math.*, 162(1):81–92, 2007.

[2] N. Avni, T. Gerlander, M. Kassabov, and A. Shalev. Word values in p-adic and adelic groups. *Bull. Lond. Math. Soc*, 45(6):1323–1330, 2013.

[3] A. Baragar. The Markoff-Hurwitz equations over number fields. *Rocky Mountain J. Math*, 35(3):695–712, 2005.

[4] A. Borel. Some finiteness properties of adele groups over number fields. *Publications Mathématiques de l'IHÉS*, 16:5–30, 1963.

[5] S. Chowla, J. Cowles, and M. Cowles. On the number of conjugacy classes in SL(2,$\mathbb{Z}$). *Jour. Number Theory*, 12(3):372–377, 1980.

[6] P. J. Cohen. Decision procedures for real and p-adic fields. *Comm. on Pure and Applied Math.*, 22:131–151, 1969.

[7] J. L. Colliot-Thélène, D. Wei, and F. Xu. Brauer-Manin obstruction for Markoff surfaces. *Annali della Scuola Normale Superiore di Pisa*, vol. XXI:1257–1313, 2020.

[8] R Fricke. Über die Theorie der automorphen Modulgruppen. *Nachrichten Ges. Wiss. Göttingen*, pages 91–101, 1896.

[9] A. Ghosh and P. Sarnak. Integral points on Markoff type cubic surfaces. *arXiv:1706.06712 [math.NT]*, 2017.

[10] F. Grunewald and D. Segal. Some general algorithms. I: Arithmetic groups. *Annals of Math.*, 112(3):531–583, 1980.
[11] F. Grunewald and D. Segal. Decision problems concerning S-arithmetic groups. *Jour. Symbolic Logic*, 50(3):743–772, 1985.
[12] A. Khelif. Finite approximation and commutators in free groups. *J. Algebra*, 281(2):407–412, 2004.
[13] D. Loughran and V. Mitankin. Integral Hasse principle and strong approximation for Markoff surfaces. *IMRN /imrn/rnz114*, 10:1093, 2020.
[14] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory.* v.89 in Classics in Mathematics. Springer-Verlag, 1977.
[15] J. Mennicke. On Ihara's modular group. *Invent. Math*, 4:202–228, 1967/68.
[16] M. Orzech and L. Ribes. Residual finiteness and the Hopf property in rings. *J. Algebra*, 15:81–88, 1970.
[17] P. S. Park. Conjugacy growth of commutators, 2017. Princeton University senior thesis.
[18] P. S. Park. Conjugacy growth of commutators. *Jour. of Algebra*, 526:423–458, 2019.
[19] L. Ribes and P. Zalesskii. *Profinite groups.* A Series of Modern Surveys in Mathematics, 40. Springer-Verlag, Berlin xiv+435 pp, 2000.
[20] P. Sarnak. *Prime geodesic theorems.* PhD thesis, Stanford, Proquest LLC, 1980.
[21] Z. Sela. Diophantine geometry over groups VII: The elementary theory of a hyperbolic group. *Proc. Lond. Math. Soc.*, 99(1):217–273, 02 2009.
[22] J. P. Serre. Le probléme des groupes de congruence pour SL2. *Annals of Math.*, 92(3):489–527, 1970.
[23] J. P. Serre. *Trees.* Translated from the French original by John Stillwell. Corrected 2nd printing of the 1980 English translation. Springer Monographs in Mathematics. Springer-Verlag, Berlin x+142 pp, 2003.
[24] A. Shalev. Applications of some zeta functions in group theory. *Zeta functions in algebra and geometry, Contemp. Math*, 566:331–344, 2012.
[25] J. H. Silverman. The Markoff equation $x^2 + y^2 + z^2 = axyz$ over quadratic imaginary fields. *J. Number Theory*, 35(1):72–104, 1990.
[26] J. G. Thompson. Power maps and completions of free groups and of the modular group. *Jour. of Algebra*, 191(1):252–264, 1997.
[27] J. Whang. Nonlinear descent on moduli of local systems. *Israel Jour. of Math.*, 240, 10 2017.
[28] M. J. Wicks. Commutators in free products. *Jour. London Math. Soc.*, s1-37(1):433–444, 1962.
[29] J. S. Wilson. *Profinite groups.* London Mathematical Society Monographs. New Series, 19. The Clarendon Press, Oxford University Press, New York xii+284 pp, 1998.

Oklahoma State University
Stillwater, OK 74078, USA
ghosh@okstate.edu

Technion - Israel Institute of Technology (Haifa Israel)
chenm@technion.ac.il

Institute for Advanced Study and Princeton University
Princeton, NJ 08540, USA
sarnak@math.ias.edu