Math. Proc. Camb. Phil. Soc. (2026), **180**, 15–34
doi:10.1017/S0305004125101333
First published online 8 August 2025

On congruence subgroups generated by two parabolic rational matrices

BY CARL-FREDRIK NYBERG-BRODDA
June E. Huh Centre for Mathematical Challenges (KIAS), 85 *Hoegi-ro, Dongdaemun-gu* 02455 *Seoul, Republic of Korea.*
e-mail: cfnb@kias.re.kr

(*Received* 15 *April* 2024*; accepted* 22 *April* 2025)

Abstract

We study the freeness problem for multiplicative subgroups of $\mathrm{SL}_2(\mathbb{Q})$. For $q = r/p$ in $\mathbb{Q} \cap (0, 4)$, where p is prime and $\gcd(r, p) = 1$, we initiate the study of the algebraic structure of the group Δ_q generated by

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } Q_q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}.$$

We introduce the conjecture that $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$, the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ consisting of all matrices with upper right entry congruent to 0 mod r and diagonal entries congruent to 1 mod r. We prove this conjecture when $r \leq 4$ and for some cases when $r = 5$. Furthermore, conditional on a strong form of Artin's conjecture on primitive roots, we also prove the conjecture when $r \in \{p - 1, p + 1, (p + 1)/2\}$. In all these cases, this gives information about the algebraic structure of $\Delta_{r/p}$: it is isomorphic to the fundamental group of a finite graph of virtually free groups, and has finite index $J_2(r)$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$, where $J_2(r)$ denotes the Jordan totient function.

2020 Mathematics Subject Classification: 30F35, 30F40 (Primary);
20E05, 11J70 (Secondary)

1. *Background*

Consider the following problem: given a set of matrices, what can be said about the multiplicative (semi)group $\mathcal{H}$ generated by them? Can one decide whether some given matrix lies in $\mathcal{H}$? Can one decide whether $\mathcal{H}$ is free, or even finitely presented? It should come as no surprise that this type of problem, in full generality, is undecidable. For example, Markov [**24**] proved already in 1947 that the problem of whether a given matrix can be expressed as a product of some other given matrices, i.e. the membership problem, is undecidable for $\mathrm{SL}_4(\mathbb{Z})$. This was one of the first undecidability results in mathematics, and demonstrates the inherent difficulty of problems of this type. In special cases, one can often do much more.

When studying the matrix group $\mathrm{SL}_n(\mathbf{R})$ for some ring $\mathbf{R}$, there are two degrees of freedom: the size of n, and the complexity of $\mathbf{R}$. Even for $n = 4$, most algorithmic problems become intractable for $\mathbf{R} = \mathbb{Z}$, as indicated by Markov's result; on the other hand, the group $\mathrm{SL}_3(\mathbb{Z})$ is still rather mysterious, with many open problems (e.g. coherence, see

© The Author(s), 2025. Published by Cambridge University Press on behalf of Cambridge Philosophical Society.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

below). The freeness problem for subgroups of $\mathrm{SL}_3(\mathbb{Z})$ is highly non-trivial. By contrast, the group $\mathrm{SL}_2(\mathbb{Z})$ is virtually free and therefore comparatively much simpler to understand. Extending this to a larger ring, we find the group $\mathrm{SL}_2(\mathbb{Q})$, and, as a particular case, the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$ for a fixed prime p. Here, similar problems remain as for $\mathrm{SL}_3(\mathbb{Z})$, and the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is the starting point for this paper.

The problem central to this paper is the following: given two matrices in $\mathrm{SL}_2(\mathbb{Q})$, do they generate a free group? We will consider a very special case of this problem: given a non-zero rational $q \in \mathbb{Q}$, is the group Δ_q generated by the two matrices

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } Q_q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$$

free? If not, what is its algebraic structure?

The problem of representing free groups by matrices of the type above is a classical topic in combinatorial group theory, and has a long and complex history (the *semigroup* analogue has also been studied [**5**, **10**]). There is much to say about this fascinating history; a full treatment will appear elsewhere. However, a starting point is work by a group of three Soviet students supervised by V. A. Tartakovskii in Leningrad in the late 1930s: Kh. A. Doniyakhi [**11**], D. I. Fuchs-Rabinovich [**13**], and I. N. Sanov. The former two studied representing free groups by matrices (inspired by results by Magnus [**23**, section 5, p. 72]), while Sanov instead focussed on the Burnside problem, resolving it for exponent 4 [**32**]. All three students were drafted in 1941, following the invasion of the Soviet Union. Only Sanov survived the war. Now the sole torchbearer of this line of inquiry, in 1947 he would return to the matrix problem, and proved his now-famous theorem that the group generated by the two matrices

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

is free on those generators [**33**]. This article inspired a 1955 note by Brenner [**4**], who showed that if $|q| \geq 4$, the group Δ_q is free. Hence, we will restrict our attention to the case of $q \in \mathbb{Q}$ with $|q| < 4$, which by symmetry means we need only consider $q \in \mathbb{Q} \cap (0, 4)$. We remark that if one instead considers complex parameters $c \in \mathbb{C}$, then Δ_c becomes intricately connected with the *Riley slice* [**20**], although this remarkable slice is outside the scope of this paper.

Our problem is then: *is* $\Delta_q = \langle A, Q_q \rangle$ ever a free group for $q \in \mathbb{Q} \cap (0, 4)$? This problem was first addressed directly by Lyndon and Ullman [**22**], and it remains open to this day; it is problem 15.83 of the Kourovka Notebook [**25**], attributed to Merzlyakov, owing to his extensive studies of the problem, e.g. [**27**, **28**], cf. also [**25**, problem 15.84]. There are many known rationals q for which the group Δ_q is *not* free, with the best-known results to date being due to Kim and Koberda [**21**], but not a single value for when it is free. Farbman [**12**] and Kim and Koberda [**21**] explicitly conjecture that the answer to this question is **no**, i.e. that the group Δ_q is never free, but it remains open in general even to find a dense subset of $\mathbb{Q} \cap (0, 4)$ consisting of rational numbers which give rise to non-free Δ_q. Even the problem of whether Δ_q is finitely presented is an open problem. Lyndon and Ullman suspected that the group structure of Δ_q may be as an amalgam of two free groups. If the main conjecture of this paper is true, then this will show that the conjectures of Farbman and Kim and Koberda are true, and that Lyndon and Ullman's suspicion is very close to the truth (see section 2).

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

The theory and machinery of arithmetic matrix groups is sufficiently rich to place the non-freeness conjecture for Δ_q in a broader context. One particular instance of this is the Greenberg–Shalom Conjecture. This conjecture is rather technical, and we shall not state it; but if it is true, then it would have a number of remarkable consequences, surveyed recently in [7]. For our purposes, the two most important consequences are that if $r/p \in \mathbb{Q} \cap (0, 4)$ with $\gcd(r, p) = 1$, then:

(1) $\Delta_{r/p}$ is **not** free.
(2) $\Delta_{r/p}$ has finite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$.

Both problems remain open. The second implies the first, as $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is not virtually free. Whereas the first question has been extensively studied, the second remains essentially unexplored (although cf. [1]). Related to these questions is the following very natural question, which has essentially seen no study beyond the question of freeness:

Question 1.1 What is the algebraic structure of $\Delta_{r/p}$?

In this paper we will tackle both the finite index question and 1·1 We will identify a very compelling conjecture regarding this structure. Specifically, we conjecture, and prove in many cases, that $\Delta_{r/p}$ is equal to $\overline{\Gamma}_1^{(p)}(r)$, the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ generated by all matrices with diagonal entries congruent to $1 \pmod r$ and upper right entry congruent to $0 \pmod r$. Explicitly, we conjecture:

CONJECTURE 1·1. *For all $r/p \in \mathbb{Q} \cap (0, 4)$ with $\gcd(r, p) = 1$, the group $\Delta_{r/p}$ is equal to the congruence subgroup $\overline{\Gamma}_1^{(p)}(r)$ of $\mathrm{SL}_2(\mathbb{Z}[1/p])$. In particular, $\Delta_{r/p}$ is not free, has index $J_2(r)$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$, and is isomorphic to the fundamental group of a finite graph of groups with virtually free vertex groups (and is hence finitely presented).*

Here $J_2(r)$ denotes the Jordan totient function counting the number of generators of $(\mathbb{Z}/r\mathbb{Z})^2$. We will verify the conjecture in some cases; in section 6, we prove:

THEOREM 6·3 *Let $r/p \in \mathbb{Q} \cap (0, 4)$ with p prime, $\gcd(r, p) = 1$. If either*:

(i). $r \in \{1, 2, 3, 4\}$; or
(ii). $r = 5$ and $p \not\equiv -1, 1 \pmod{11}$,

then Conjecture 1.2 holds for $\Delta_{r/p}$. Furthermore, if p is arbitrary and

$$r \in \{p - 1, p + 1, \frac{p + 1}{2}\},$$

the last case assuming p is odd, then assuming a strong form of Artin's conjecture on primitive roots (Conjecture 5·3) for p holds, then Conjecture 1·1 holds for $\Delta_{r/p}$.

Our work can be seen as support for two consequences of the Greenberg–Shalom Conjecture. Doubtlessly, the conjecture can be proved in many more cases with analogous

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

Table 1. *Some computational evidence in favour of the main conjecture (Conjecture 1·1). Each box contains the index of $\Delta_{r/p}$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$, computed using GAP. In each instance, we also verified that $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$. The blank (grey) boxes correspond to values $r/p \geq 4$. The red crosses X correspond to integers r/p, and in those cases $\Delta_{r/p}$ has infinite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$.*

	$p=2$	$p=3$	$p=5$	$p=7$	$p=11$	$J_2(r)$
$r=1$	1	1	1	1	1	1
$r=2$	✗	3	3	3	3	3
$r=3$	8	✗	8	8	8	8
$r=4$	✗	12	12	12	12	12
$r=5$	24	24	✗	24	24	24
$r=6$	✗	✗	24	24	24	24
$r=7$	48	48	48	✗	48	48
$r=8$		48	48	48	48	48
$r=9$		✗	72	72	72	72
$r=10$		72	✗	72	72	72
$r=11$		120	120	120	✗	120
$r=12$			96	96	96	96
$r=13$			168	168	168	168
$r=14$			144	✗	144	144
$r=15$			✗	192	192	192
$r=16$			192	192	192	192
$r=17$			288	288	288	288
$r=18$			216	216	216	216
$r=19$			360	360	360	360
$r=20$				288	288	288
$r=21$				✗	440	440
$r=22$				360	✗	360
$r=23$				528	528	528
$r=24$				384	384	384
$r=25$				600	600	600
$r=26$				504	504	504
$r=27$				684	684	684

techniques as in this paper. We have also verified Conjecture 1·1 computationally for many small values of r/p, including for all values $r/p \leq 4$ when $p \in \{2, 3, 5, 7\}$. This is presented in Table 1. We also introduce the notion of a *strong* relation number, which is to $\Delta_{r/p}$ having finite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$ what being a relation number is to $\Delta_{r/p}$ not being free.

Finally, studying the algebraic structure of 2-generated subgroups of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is also relevant for the *coherence* problem, i.e. whether or not every finitely generated subgroup is finitely presented. This is open; however, for prime p the Greenberg–Shalom conjecture implies a positive answer to this question [**7**, theorem 6·2]. For n with at least two distinct prime factors p and q, Baumslag [**30**, p. 734] showed that $\mathrm{SL}_2(\mathbb{Z}[1/n])$ is incoherent, since the group generated by

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} p/q & 0 \\ 0 & q/p \end{pmatrix}$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

is not finitely presented. Thus, understanding the structure of 2-generated subgroups of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ seems a worthwhile task; for example, it is not known to the author whether every 2-generated subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is finitely presented. Our main conjecture (Conjecture 1·1) implies that the answer to this question is yes at least in the case of the 2-generated groups $\Delta_{r/p}$.

2. SL_2

For a ring $\mathbf{R}$, we denote by $\mathrm{SL}_2(\mathbf{R})$ the ring of all 2×2-matrices with entries in $\mathbf{R}$ and with determinant 1. We will only consider the multiplicative structure of $\mathrm{SL}_2(\mathbf{R})$ in this paper, and refer to it as a group.

2·1. *Generators and relations*

Throughout this paper, we will consider $\mathrm{SL}_2(\mathbb{Z})$ defined abstractly by the group presentation

$$\mathrm{SL}_2(\mathbb{Z}) = \mathrm{Gp}\langle a, b \mid b^2 = (ab)^3, b^4 = 1\rangle. \tag{2·1}$$

We will, however, seamlessly pass between this presentation and considering $\mathrm{SL}_2(\mathbb{Z})$ as a matrix group, via the isomorphism induced by

$$a \mapsto A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad b \mapsto B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Throughout remove, we will retain this notation for the matrices A and B.

Giving generators and relations for $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is more difficult, but two such descriptions are known: the first, described by Serre [**35**, II.1.4] comes via the action of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ on a tree:

$$\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) \cong \mathrm{SL}_2(\mathbb{Z}) *_{\Gamma_0^{\mathbb{Z}}(p)} \mathrm{SL}_2(\mathbb{Z}) \tag{2·2}$$

where the inclusion map is specified in [**35**, corollary II.1.2] (we will not use it). Here $\Gamma_0^{\mathbb{Z}}(p)$ is used to denote the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices with bottom left entry congruent to 0 (mod p). Second, Behr and Mennicke [**2**] provide a presentation for all p. For $p = 2, 3$, the presentation is

$$\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) \cong \mathrm{Gp}\langle a, b, u_p \mid (ab)^3 = (u_p b)^2 = (b u_p a^p)^3 = b^2, b^4 = 1, u_p^{-1} a u = a^{p^2}\rangle.$$

The generators a and b correspond to A and B above, and u_p corresponds to

$$U_p = \begin{pmatrix} p & 0 \\ 0 & 1/p \end{pmatrix}.$$

Throughout this paper, we will retain the notation U_p for this matrix. To see that A, B, U_p generate $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is easy, cf. [**26**, p. 204]. However, we also note that *any* non-trivial power of U_p will generate $\mathrm{SL}_2(\mathbb{Z}[1/p])$ together with A and B, as an easy multiplication shows that

$$U_p = U_p^k A^{p^{k-1}} U_p^{-k} B A^{p^{k+1}} U_p^{-k} B A^{p^{k-1}} B^{-1} \tag{2·3}$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

for any non-zero $k \in \mathbb{Z}$. We will also make consistent use of the following relations, which allow us to "push" U_p-type letters to the left.

$$B^i U_p = U_p^{(-1)^i} B^i, \qquad AU_p = U_p A^{p^2}. \tag{2·4}$$

2·2. *Congruence subgroups*

In this section, we will collect some known results about congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}[1/p])$.

Let $r \geq 1$, and consider the natural surjection $\pi_r^{\mathbb{Z}}\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/r\mathbb{Z})$ resp. (when $\gcd(p, r) = 1$) the map $\pi_r^{(p)}\colon \mathrm{SL}_2(\mathbb{Z}[1/p]) \to \mathrm{SL}_2(\mathbb{Z}/r\mathbb{Z})$ in each case defined by reducing each entry modulo r. The kernel of such a map is called a *principal congruence subgroup* (of level r) of $\mathrm{SL}_2(\mathbb{Z})$ resp. $\mathrm{SL}_2(\mathbb{Z}[1/p])$, and will here be denoted $\ker \pi_r^{\mathbb{Z}} = \Gamma^{\mathbb{Z}}(r)$ resp. $\ker \pi_r^{(p)} = \Gamma^{(p)}(r)$. Jordan proved in the *Traité* [19, p. 95, Thèoreme 123] that

$$|\mathrm{SL}_2(\mathbb{Z}/r\mathbb{Z})| = rJ_2(r) \sim \frac{r^3}{\zeta(3)}, \tag{2·5}$$

where $J_2(r)$ denotes the *Jordan totient function*, being the number of pairs (a,b) with $1 \leq a, b \leq r$ with $\gcd(a, b, r) = 1$, and $\zeta(3)$ is Apéry's constant. In particular, (2.5) also gives the index of the rth principal congruence subgroup $\Gamma^{\mathbb{Z}}(r)$ in $\mathrm{SL}_2(\mathbb{Z})$ (resp. the index of $\Gamma^{(p)}(r)$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$). The sequence of values of $J_2(r)$ begins

$$1, 3, 8, 12, 24, 24, 48, 48, 72, 72, 120, 96, \ldots$$

being OEIS sequence A007434. Clearly, for p prime $J_2(p) = p^2 - 1$.

It is well known that not every subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$ contains some $\Gamma^{\mathbb{Z}}(r)$ (indeed, most do not), i.e. $\mathrm{SL}_2(\mathbb{Z})$ does not have the *Congruence Subgroup Property*. By contrast, a theorem of Serre [34] and Mennicke [26][1] shows that $\mathrm{SL}_2(\mathbb{Z}[1/p])$ has this property for all p. If $\mathcal{H} \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$ (or $\mathrm{SL}_2(\mathbb{Z})$) is a congruence subgroup containing $\Gamma^{\mathbb{Z}}(r)$, then we say that $\mathcal{H}$ is an r-congruence subgroup. We define some important congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}[1/p])$. Let $r \geq 1$ and $\gcd(r, p) = 1$. Then we let

$$\overline{\Gamma}_1^{\mathbb{Z}}(r) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 1 \pmod{r}, b \equiv 0 \pmod{r} \right\}$$

and analogously for $\overline{\Gamma}_1^{(p)}(r)$, i.e. $\overline{\Gamma}_1^{\mathbb{Z}}(r)$ (resp. $\overline{\Gamma}_1^{(p)}(r)$) is the pre-image under $\pi_r^{\mathbb{Z}}$ (resp. $\pi_r^{(p)}$) of the group of lower unitriangular matrices in $\mathrm{SL}_2(\mathbb{Z}/r\mathbb{Z})$. Since that group is cyclic of order r, it follows that

$$[\,\mathrm{SL}_2(\mathbb{Z}[\tfrac{1}{p}]) : \overline{\Gamma}_1^{(p)}(r)] = [\,\mathrm{SL}_2(\mathbb{Z}) : \overline{\Gamma}_1^{\mathbb{Z}}(r)] = J_2(r). \tag{2·6}$$

The structures of $\overline{\Gamma}_1^{(p)}(r)$ and $\overline{\Gamma}_1^{\mathbb{Z}}(r)$ are quite different, however. It is well known that for $r \geq 4$ the group $\overline{\Gamma}_1^{\mathbb{Z}}(r)$ is free; indeed, denoting its rank by n, a simple Euler characteristic argument (see [8, IX.8]) yields $\chi(\mathrm{SL}_2(\mathbb{Z})) = 1 - n/J_2(r)$ and since $\chi(\mathrm{SL}_2(\mathbb{Z})) = \zeta(-1) = -1/12$, we have that $n = 1 + J_2(r)/12$. By contrast, $\overline{\Gamma}_1^{(p)}(r)$ is never free

1 Mennicke's proof is incomplete, as it relies on an incorrect computation of the Schur multiplier of $\mathrm{SL}_2(\mathbb{Z}/r\mathbb{Z})$. The argument is corrected in [3, §5].

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

(as $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is not virtually free), but by general Bass–Serre theory the decomposition (2) implies that $\overline{\Gamma}_1^{(p)}(r)$ is the fundamental group of a finite graph of groups with virtually free vertex groups. We will also prove that $\overline{\Gamma}_1^{(p)}(r)$ can sometimes (conjecturally always) be generated by three elements in §5.

3. *The group* $\Delta_{r/p}$

For any prime p and $r \in \mathbb{Z}$ such that p and r are coprime. When $r/p \in \mathbb{Q} \cap (0,4)$, we will say that r/p is *admissible*. Let

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad Q_{r/p} = \begin{pmatrix} 1 & r/p \\ 0 & 1 \end{pmatrix}.$$

Let $\Delta_{r/p} = \langle A, Q_{r/p} \rangle \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$. If r/p is not admissible, then $\Delta_{r/p}$ is free [**4**, **33**]. On the other hand, there is no known example of an admissible number for which the group $\Delta_{r/p}$ is free; this was noted already by Lyndon and Ullman [**22**] in 1969, and Kim and Koberda [**21**] conjecture that *every* admissible rational number gives rise to a non-free $\Delta_{r/p}$. Let us say that r/p is a *relation* number if $\Delta_{r/p}$ is not free (on two generators). We mention a useful necessary and sufficient condition for r/p to be a relation number: that there exist some non-trivial product of the matrices A and $Q_{r/p}$, involving both A and $Q_{r/p}$ non-trivially, which equals an upper triangular matrix. Some $Q_{r/p}$-conjugate of this matrix will then commute with $Q_{r/p}$, proving non-freeness (cf. [**21**, lemma 2·1]).

There are many known examples of rational relation numbers. We refer the reader to Kim and Koberda [**21**] and Gilman [**14**] for extensive references, see also [**6**, **18**, **36**]. Kim and Koberda, in particular, prove that r/p is a relation number for all $r \leq 27$, except possibly $r = 24$. The main difficulty in proving theorems of this type is that the shortest length of a relation (in the sense of the syllable length of the product of A and $Q_{r/p}$ that is required for a product to equal 1) grows very rapidly as $r/p \to 4$. There is also no known subset of $\mathbb{Q} \cap (0,4)$ in which the relation numbers are dense. Furthermore, there is no known example of a sequence of distinct relation numbers converging to 3 or to 4. By contrast, it is easy to prove that the algebraic relation numbers (defined analogously) are dense in (0,4), see e.g. [**9**, corollary 1]. It is also easy to construct a series of rational relation numbers converging to $2 + \sqrt{2} = 3.414....$ For example, consider the sequence

$$\frac{3}{1}, \frac{7}{2}, \frac{41}{12}, \frac{239}{70}, \frac{1393}{408}, \frac{8119}{2378} \ldots \longrightarrow 2 + \sqrt{2} \tag{3·1}$$

consisting entirely of principal convergents to $2 + \sqrt{2}$, i.e. 2 added to the solutions to the Pell equation $X^2 + 2Y^2 = 1$. Then it is not hard to prove that the nth entry q_n of the sequence will be such that $Q_{q_n}^{a(n)}(A^{-1}Q_{q_n})^3 A^{-1} Q_{q_n}^{a(n)}$ is upper triangular, where $a(1) = 0$, $a(2) = 2$ and recursively $a(n) = 34a(n-1) - a(n-2) - 8$ for $n \geq 3$. Thus the numbers in (3·1) are all rational relation numbers.

In spite of the extensive literature on the freeness problem, going back more than fifty years, there has been essentially no research done regarding the algebraic structure of the group $\Delta_{r/p}$. This paper aims to fill that gap. In section 6, we will describe the structure explicitly in many cases, and prove that in these cases the group $\Delta_{r/p}$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$, and in particular that $\Delta_{r/p}$ has finite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$. Indeed, we will show in many cases that $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$, as defined in section 2. When this equality

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

holds, $\Delta_{r/p}$ splits as the fundamental group of a finite graph of groups with virtually free vertex groups. This sort of decomposition for $\Delta_{r/p}$ was predicted already by Lyndon and Ullman in 1969 (cf. [22, p.1401]). We remark that the inclusion $\Delta_{r/p} \leq \overline{\Gamma}_1^{(p)}(r)$ is trivially true; both A and $Q_{r/p}$ clearly lie in $\overline{\Gamma}_1^{(p)}(r)$. This leads us directly to Conjecture 1·1. We will deal with one easy case of the conjecture, first, namely when $r = 1$.

PROPOSITION 3·1. *The group generated by A and $Q_{1/p}$ has index 1 in* $\mathrm{SL}_2(\mathbb{Z}[1/p])$. *That is,* $\Delta_{1/p} = \overline{\Gamma}_1^{(p)}(1) = \mathrm{SL}_2(\mathbb{Z}[1/p]) \cong \mathrm{SL}_2(\mathbb{Z}) *_{\Gamma_0^{\mathbb{Z}}(p)} \mathrm{SL}_2(\mathbb{Z})$.

Proof. This is a simple consequence of $B = A^{-1} Q_{1/p}^{\,p} A^{-1}$ and $U_p = B^{-1} Q_{1/p} A^{-p} Q_{1/p}$. Hence, $\mathrm{SL}_2(\mathbb{Z}[1/p]) = \langle A, B, U_p \rangle = \langle A, Q_{1/p} \rangle$.

The generators in Proposition 3·1, which appear to be new, can be used to give a new and minimal presentation of $\mathrm{SL}_2(\mathbb{Z}[1/2])$, see [31]. A particular consequence of Conjecture 1·1 is that $\Delta_{r/p}$ has index $J_2(r)$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$. Since $J_2(1) = 1$, we have now verified at least this trivial instance of the index formula. The conjecture can, of course, also be verified computationally using the presentation for $\mathrm{SL}_2(\mathbb{Z}[1/p])$ given in [2]. The results of this for small values of r/p is presented in Table 1. This is obviously very compelling computational evidence in favour of the conjecture.

4. *A sufficient criterion for congruence subgroups*

Throughout this section, fix a prime p. Let $\mathcal{H} \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$. We say that $\mathcal{H} \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$ is a *weak congruence subgroup* if $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. In particular, $\mathrm{SL}_2(\mathbb{Z})$ is a weak congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$. A (right) coset $\mathcal{H}W$ of $\mathcal{H}$ is an *integral* coset if there is some $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $\mathcal{H}W = \mathcal{H}M$. We will say that $\mathcal{H}$ has an *integral right coset transversal* (in $\mathrm{SL}_2(\mathbb{Z}[1/p])$), or simply that $\mathcal{H}$ is a *coset-integral* subgroup (of $\mathrm{SL}_2(\mathbb{Z}[1/p])$), if $\mathcal{H}$ has a complete right coset transversal consisting entirely of integer cosets. That is, $\mathcal{H}$ is a coset-integral subgroup if and only if $\mathrm{SL}_2(\mathbb{Z}[1/p]) = \mathcal{H} \cdot \mathrm{SL}_2(\mathbb{Z})$ as sets.

As noted by Mennicke [26, p.220], U_p is a redundant generator modulo $\ker \pi_r^{(p)}$ for any $r \in \mathbb{N}$ with $\gcd(r, p) = 1$. Specifically, we have

$$U_p = A^{p^{-1}} B A^p B A^{p^{-1}} B^{-1} \mod \ker \pi_r^{(p)}. \tag{4·1}$$

Hence, using (4·1) together with the normality of $\ker \pi_r^{(p)}$, we observe that every congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is coset-integral. In particular, it follows directly from the congruence subgroup property that the converse, when restricted to weak congruence subgroups, is also true:

LEMMA 4·1. *Let $\mathcal{H}$ be a weak congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z}[1/p])$. *Then $\mathcal{H}$ has only finitely many integral cosets. In particular, $\mathcal{H}$ is a congruence subgroup if and only if $\mathcal{H}$ is an coset-integral subgroup.*

LEMMA 4·2. *Let $\mathcal{H}$ be a weak congruence subgroup in* $\mathrm{SL}_2(\mathbb{Z}[1/p])$. *Then for all $M \in \mathrm{SL}_2(\mathbb{Z})$ and all $t \in \mathbb{Z}$, there exists $N \in \mathrm{SL}_2(\mathbb{Z})$ and $\varepsilon \in \{-1, 1\}$ such that*

$$\mathcal{H} M U^t = \mathcal{H} U^{\varepsilon t} N.$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

Proof. For ease of notation, we will only consider the case $t = 1$, the other cases being entirely analogous. Let $M = A^{i_1}B^{j_1}\cdots A^{i_k}B^{j_k} \in \mathrm{SL}_2(\mathbb{Z})$. We prove the claim by induction on k. If $k = 0$, there is nothing to prove; we can take $\varepsilon = 1, N = \mathbf{1}_{2\times 2}$. Suppose that $k \geq 1$. Then

$$\mathcal{H}M = \mathcal{H}A^{i_1}B^{j_1}\cdots A^{i_k}B^{j_k}U_p = \mathcal{H}A^{i_1}B^{j_1}\cdots A^{i_k}U_p^{(-1)^{j_k}}B^{j_k} \tag{4·2}$$

by (2·4). If $(-1)^{j_k} = 1$, then as $A^{i_k}U_p = U_pA^{p^2i_k}$, the claim follows by induction. So suppose $(-1)^{j_k} = -1$. In the case that $k = 1$, then (4·2) becomes $\mathcal{H}A^{i_1}U_p^{-1}$. Since $\mathcal{H}$ is a weak congruence subgroup, say $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z})$ is an r-congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with $\gcd(p, r) = 1$, it follows that $A^{rm} \in \mathcal{H}$ for all $m \in \mathbb{Z}$. Since $\gcd(r, p^2) = 1$, r is an (additive) generator of $\mathbb{Z}/p^2\mathbb{Z}$, so there is some $m \in \mathbb{Z}$ such that $rm + i_1 \equiv 0 \pmod{p^2}$. Choose such an m, and let $rm + i_1 = sp^2$, where $s \in \mathbb{Z}$. Then

$$\mathcal{H}A^{i_1}U_p^{-1} = \mathcal{H}A^{rm}A^{i_1}U_p^{-1} = \mathcal{H}A^{sp^2}U_p^{-1} = \mathcal{H}U_p^{-1}A^s,$$

again using (2·4). Thus we are done in this case. Assume, then, that j_{k-1} is non-zero, for otherwise we would be done by induction.

For all $m \in \mathbb{Z}$, right multiplication by $B^{j_{k-1}}A^{rm}B^{-j_{k-1}}$, this being an element of $\Gamma^{\mathbb{Z}}(r)$, which is contained in the normal core of $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z})$, will fix any right coset of $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z})$. Therefore, right multiplication by $B^{j_{k-1}}A^{rm}B^{-j_{k-1}}$ also fixes any integral right coset of $\mathcal{H}$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$. Consequently, picking m such that $rm + i_k = sp^2$ for some $s \in \mathbb{Z}$, we have

$$\begin{aligned}\mathcal{H}A^{i_1}B^{j_1}\cdots A^{i_k}U_p^{-1}B^{j_k} &= \mathcal{H}A^{i_1}B^{j_1}\cdots A^{j_{k-1}}(B^{j_{k-1}}A^{rm}B^{-j_{k-1}})B^{j_{k-1}}A^{i_k}U_p^{-1}B^{j_k}\\ &= \mathcal{H}A^{i_1}B^{j_1}\cdots A^{j_{k-1}}B^{j_{k-1}}A^{sp^2}U_p^{-1}B^{j_k}\\ &= \mathcal{H}A^{i_1}B^{j_1}\cdots A^{j_{k-1}}B^{j_{k-1}}U_p^{-1}A^sB^{j_k}\end{aligned}$$

Notice that in pushing our $U_p^{\pm 1}$ to the left, we have only changed its sign. By induction, we are done.

LEMMA 4·3. *Let $\mathcal{H}$ be a weak congruence subgroup in $\mathrm{SL}_2(\mathbb{Z}[1/p])$. If $U_p^k \in \mathcal{H}$ for some non-zero $k \in \mathbb{Z}$, then every right coset of $\mathcal{H}$ is integral.*

Proof. Let $W = W(A, B, U_p)$ be a word in A, B, U_p and their inverses. By (2·3), there is no loss of generality to assume that $W = W(A, B, U_p^k)$ is a word in A, B, U_p^k. If W contains no occurrence of $U_p^{\pm k}$, then there is nothing to show, as $\mathcal{H}W$ is integral by definition. Suppose instead that W contains at least one occurrence of $U_p^{\pm k}$ and write $W \equiv MU_p^{\pm k}W'$, where $M \in \mathrm{SL}_2(\mathbb{Z})$ and $W' = W'(A, B, U_p^k)$ contains one fewer occurrences of $U_p^{\pm k}$. Then by Lemma 4·2 there exists some $N \in \mathrm{SL}_2(\mathbb{Z})$ and some $\varepsilon \in \{-1, 1\}$ such that

$$\mathcal{H}W = \mathcal{H}MU_p^{\pm k}W' = \mathcal{H}U_p^{\varepsilon k}NW' = \mathcal{H}NW'.$$

Now *NW*' contains one less occurrence of U_p^k than W, so by induction on the number of occurrences of $U_p^{\pm k}$ in W, the claim follows.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

Thus, by combining Lemma 4·1 and Lemma 4·3, we find:

PROPOSITION 4·4. *Let $\mathcal{H} \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$. Then $\mathcal{H}$ is a congruence subgroup if and only if it is a weak congruence subgroup and $U_p^k \in \mathcal{H}$ for some non-zero $k \in \mathbb{N}$.*

Proof. ($\Longrightarrow$) This follows directly from the fact that congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$.

($\Longleftarrow$) Suppose $\mathcal{H}$ and $k \in \mathbb{N}$ are as given. Then by Lemma 4·3 we have that $\mathcal{H}$ is coset-integral, so by Lemma 4·1 $\mathcal{H}$ is a congruence subgroup.

COROLLARY 4·4. *Let $\mathcal{H} \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$. If $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z})$ is an r-congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $U_p^k \in \mathcal{H}$, for some non-zero $k \in \mathbb{Z}$, then*

$$[\,\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) : \mathcal{H}] = [\,\mathrm{SL}_2(\mathbb{Z}) : \mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z})] \leq rJ_2(r).$$

Proof. The first equality follows directly: ($\geq$) is always true, since $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z}) \leq \mathcal{H}$, and ($\leq$) follows from the fact that any congruence subgroup is coset-integral. Finally, the index of $\Gamma^{\mathbb{Z}}(r)$ in $\mathrm{SL}_2(\mathbb{Z})$ is $rJ_2(r) = |\mathrm{SL}_2(\mathbb{Z}/r\mathbb{Z})|$.

In the case that $\mathcal{H} \cap \mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})$, then we can choose $r = 1$, and since $rJ_2(r) = 1$ we find that

$$\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) = \langle \mathrm{SL}_2(\mathbb{Z}), U_p^k \rangle = \langle A, B, U_p^k \rangle,$$

for all non-zero k, as observed already in (2·3) (note, however, that (2·3) was used in the proof of Corollary 4·4). In other words, we find the interesting observation that there does not exist any group $\mathcal{H}$ such that $\mathrm{SL}_2(\mathbb{Z}) < \mathcal{H} < \mathrm{SL}_2(\mathbb{Z}[1/p])$.

Recall the definition of $\sigma_p(r)$ as the multiplicative order of p mod r. Then in particular we have:

THEOREM 4·6. *Let $\mathcal{H} \leq \mathrm{SL}_2(\mathbb{Z}[1/p])$ be any subgroup such that (i) $\overline{\Gamma}_1^{\mathbb{Z}}(r) \leq \mathcal{H}$ and (ii) $U_p^{k\sigma_r(p)} \in \mathcal{H}$ for some non-zero $k \in \mathbb{Z}$. Then $\overline{\Gamma}_1^{(p)}(r) \leq \mathcal{H}$.*

We will now use this result to verify that $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$ for $r \leq 4$, and use some number-theoretic arguments to give a conjectural generating set for $\overline{\Gamma}_1^{(p)}(r)$.

5. *Generating $\overline{\Gamma}_1^{(p)}(r)$*

In this section, we will give a generating set for the congruence subgroup $\overline{\Gamma}_1^{(p)}(r)$ of $\mathrm{SL}_2(\mathbb{Z}[1/p])$, when $\gcd(r,p) = 1$ and $r \leq 4$. Then, conditional on a slightly strengthened form of Artin's conjecture on primitive roots, we will give a generating set for all r with $\gcd(r,p) = 1$. First, the following is a restatement of the results of §4, specifically of Theorem 4·5:

THEOREM 5·1. *Let p be any prime, and $1 \leq r \leq 4$ with $\gcd(r,p) = 1$. Then the group*

$$\mathcal{H} = \left\langle A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, Q_{r/p} = \begin{pmatrix} 1 & r/p \\ 0 & 1 \end{pmatrix}, U_p^{\sigma_p(r)} = \begin{pmatrix} p^{\sigma_p(r)} & 0 \\ 0 & p^{-\sigma_p(r)} \end{pmatrix} \right\rangle$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

is equal to $\overline{\Gamma}_1^{(p)}(r)$*, where* $\sigma_p(r)$ *denotes the multiplicative order of p mod r (being equal to either 1 or 2).*

Proof. It is well known that $\overline{\Gamma}_1^{\mathbb{Z}}(r)$ is generated by A and $Q_{r/p}^p = BA^rB^{-1}$ if (and only if!) $r \leq 4$. The result then follows from Corollary 4·5, as we clearly have $\mathcal{H} \leq \overline{\Gamma}_1^{(p)}(r)$.

We will now give a conjectural generating set for $\overline{\Gamma}_1^{(p)}(r)$ for arbitrary r with $\gcd(r,p) = 1$. Let us recall Artin's conjecture on primitive roots:

CONJECTURE 5·2 (Artin). *Let m be any integer which is not a square nor* -1*. Then there are infinitely many primes q such that m is a primitive root mod q.*

The conjecture remains open even for $m = 2$; for a survey, see [**29**]. Let us consider the following strengthening of Artin's conjecture and Dirichlet's theorem:

CONJECTURE 5·3 (Residual Artin's Conjecture). *Let m be any integer which is not a square nor* -1*. Let* $a, b \in \mathbb{Z}$ *be such that* $\gcd(a,b) = 1$*. If the arithmetic progression* $a\mathbb{Z} + b$ *contains infinitely many primes q such that m is not a quadratic residue mod q, then* $a\mathbb{Z} + b$ *contains infinitely many primes q such that m is primitive mod q.*

Note that one obvious ("local") obstruction to m being primitive mod q is if m is a quadratic residue mod q. For example, 2 is a quadratic residue mod q if and only if $q \equiv \pm 1$ mod 8. Hence, 2 is never primitive mod q if $q \in 8\mathbb{Z} \pm 1$. However, Conjecture 5·3 says that there are infinitely many primes $q \equiv 3 \pmod 8$ such that 2 is primitive mod q, and likewise for $q \equiv 5 \pmod 8$. More generally, whether or not m is a quadratic residue mod q is always determined by a congruence condition on q mod km for some $k \in \mathbb{Z}$. Hence, by Dirichlet's theorem on primes in arithmetic progressions, Conjecture 5·3 implies the following: let m be any integer which is not a square nor -1, and let $a, b \in \mathbb{Z}$ be non-zero with $\gcd(a,b) = 1$ and $\gcd(a,m) = 1$. Then the arithmetic progression $a\mathbb{Z} + b$ contains infinitely many primes q such that m is primitive mod q. We will now use it in this form.

THEOREM 5·4. *Let p be any prime. Assume the strengthened form of Artin's conjecture on primitive roots (Conjecture* 5·3*) holds for* p*. Then for every* $r \in \mathbb{Z}$ *with* $\gcd(r,p) = 1$ *and for every non-zero* $k \in \mathbb{Z}$ *we have that the group*

$$\mathcal{H}_k = \left\langle A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, Q_{r/p} = \begin{pmatrix} 1 & r/p \\ 0 & 1 \end{pmatrix}, U_p^k = \begin{pmatrix} p^k & 0 \\ 0 & p^{-k} \end{pmatrix} \right\rangle$$

contains $\overline{\Gamma}_1^{(p)}(r)$. In particular, $[\mathrm{SL}_2(\mathbb{Z}[1/p]) : \mathcal{H}_k] \leq J_2(r)$.

Proof. Throughout, we will let $Q_r = Q_{r/p}^p$. Let $M_0 = \left(\begin{smallmatrix} a_0 & b_0 r \\ * & * \end{smallmatrix}\right) \in \overline{\Gamma}_1^{(p)}(r)$. We begin with some housekeeping. First, it is no loss of generality to assume that $a_0, b_0 \in \mathbb{Z}$, for we can always left multiply and conjugate M_0 by a sufficiently high power of U_p^k to ensure this. Then we have $\gcd(a_0, b_0) = p^n$ for some $n \in \mathbb{N}$. Hence, since $\gcd(r,p) = 1$, right multiplying by a sufficiently large power of Q_r can be used to ensure that $\gcd(b_0, p) = 1$ and hence also that b_0 is odd. Fix such a $b = b_0$.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

Suppose first that r is not divisible by 4. Then, as right multiplying M_0 by A^n transforms the upper left entry to $a_n = a_0 + nbr$, and since b is odd and $\gcd(r, 4) \leq 2$, we can by Dirichlet's theorem on arithmetic progressions ensure a_n is an odd prime congruent to 3 (mod 4), and since we assume Conjecture 5·3, we may also assume p is primitive mod a_n. Then p^2 generates the multiplicative subgroup of quadratic residues mod a. Furthermore, the multiplicative subgroup of quadratic residues mod a has odd order as $a \equiv 3 \pmod 4$, and hence, by making n sufficiently large, we may assume p^{2k} also generates this subgroup. Fix an n such that all the above holds, and let $a = a_n$. Now since $a \equiv 3 \pmod 4$, we have $(-1/a) = -1$. This fixes our a and b; we write $M = \left(\begin{smallmatrix} a & br \\ * & * \end{smallmatrix}\right)$, and of course $M_0 \in \mathcal{H}_k$ if and only if $M \in \mathcal{H}_k$. We now prove this last statement. Conjugating our matrix M by U_p^k gives

$$U_p^k \begin{pmatrix} a & br \\ * & * \end{pmatrix} U_p^{-k} = \begin{pmatrix} a & p^{2k}br \\ * & * \end{pmatrix}.$$

Since p^{2k} generates the subgroup of quadratic residues mod a, which has index 2 in $(\mathbb{Z}/a\mathbb{Z})^\times$, it follows that $p^{2k\ell} \equiv (b/a) \pmod a$ for some $\ell \in \mathbb{Z}$, and hence conjugating by a sufficiently high power will transform M into

$$\begin{pmatrix} a & \left(\frac{b}{a}\right) r \\ * & * \end{pmatrix} = \begin{pmatrix} a & \pm r \\ * & * \end{pmatrix}, \tag{5·1}$$

since $\gcd(a, b) = 1$. Since $M_0, M \in \overline{\Gamma}_1^{(p)}(r)$, we have $a \equiv 1 \pmod r$, and hence we can now transform the matrix in (5·1) using the Euclidean algorithm and right multiplication by A, Q_r, to obtain

$$\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s/p^n & 1 \end{pmatrix}, \quad s, n \in \mathbb{Z}.$$

Conjugating this matrix by a sufficiently high power of U_p^k, if necessary, transforms it into a power of A, and we are done.

Finally, suppose that r is divisible by 4. Then the first part of our approach fails, for we will always have $a \equiv 1 \pmod 4$. On the other hand, we will therefore always have $-a \equiv 3 \pmod 4$, and thus proceeding in the same manner as before, we can transform our matrix M_0 into

$$\begin{pmatrix} -a & \left(\frac{b}{a}\right) r \\ * & * \end{pmatrix} = \begin{pmatrix} -a & \pm r \\ * & * \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix},$$

where the last step is again effected by conjugation by U_p^k. Arguing as before, we again find that $M_0 \in \mathcal{H}_k$, which completes the proof.

As a corollary, we obtain a three-generator generating set for the congruence subgroup $\overline{\Gamma}_1^{(p)}(r)$ by noticing that $U_p^{k\sigma_p(r)}$ always lies in $\overline{\Gamma}_1^{(p)}(r)$ for all non-zero $k \in \mathbb{Z}$, where $\sigma_p(r)$ denotes the multiplicative order of p mod r:

COROLLARY 5·5. *Let p be a prime. Assume the strengthened form of Artin's conjecture on primitive roots (Conjecture* 5.3) holds for p. Then for any r with $\gcd(p, r) = 1$ and any

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

non-zero $k \in \mathbb{Z}$ we have

$$\overline{\Gamma}_1^{(p)}(r) = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & r/p \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} p^{k\sigma_p(r)} & 0 \\ 0 & p^{-k\sigma_p(r)} \end{pmatrix} \right\rangle = \langle A, Q_{r/p}, U_p^{k\sigma_p(r)} \rangle,$$

where $\sigma_p(r)$ denotes the multiplicative order of p in $\mathbb{Z}/r\mathbb{Z}$.

Notice also that neither the statement of Theorem 5·4 nor that of Corollary 5·4 contains the restriction $0 \leq r/p \leq 4$. Furthermore, the generating set in Corollary 5·4 is close to the generating set for $\Delta_{r/p}$ – it simply has one more generator $U_p^{\sigma_p(r)}$. Conjecture 1·1 amounts to saying that this generator is redundant when $0 < r/p < 4$. When $r/p \geq 4$, the group $\Delta_{r/p}$ is free, so in this case $U_p^{k\sigma_p(r)}$ is never redundant.

Remark 5·6. Artin's conjecture on primitive roots is not known to hold unconditionally for any fixed prime p (but it holds for infinitely many primes [**15**]). Nevertheless, much is known. Heath–Brown [**16**] has proved that there are at most two primes for which the conjecture fails. It would not be unreasonable to assume that this also holds true for the residue-wise Artin's conjecture (our Conjecture 5·3). If this is true, then we may interpret Corollary 5·4 as saying: *for all but at most two primes p*, the three matrices $A, Q_{r/p}, U_p^{k\sigma_p(r)}$ generate $\overline{\Gamma}_1^{(p)}(r)$. Hooley [**17**] has shown that Artin's conjecture follows from the Generalized Riemann Hypothesis. It seems plausible that the same is also true for Conjecture 5·3.

6. *Verifying conjecture* 1·1

For a prime p and some $r \in \mathbb{N}$ with $0 < r/p < 4$, and $\gcd(r, p) = 1$, recall (§3) the definition of $\Delta_{r/p}$ as the subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ generated by the two matrices

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } Q_{r/p} = \begin{pmatrix} 1 & r/p \\ 0 & 1 \end{pmatrix}.$$

It is clear from the definition of $\overline{\Gamma}_1^{(p)}(r)$ in §2 that $\Delta_{r/p} \leq \overline{\Gamma}_1^{(p)}(r)$. In this section, we will prove the converse inclusion for some values of r and p. By Corollary 5·4, to prove this (conditional on Conjecture 5·3) it suffices to verify the following:

$$U_p^{k\sigma_p(r)} \in \Delta_{r/p} \tag{6·1}$$

for some non-zero k, where $\sigma_p(r)$ is the multiplicative order of p mod r. Notice that, a *fortiori*, if one can verify (6·1), then one has found a non-trivial product of the generators A and $Q_{r/p}$ equalling an upper triangular matrix in $\Delta_{r/p}$. This already implies (as is well known, §3) that $\frac{r}{p}$ is a relation number. This is thus a very difficult problem in general. However, by Corollary 5·4 (and conditional on Conjecture 5·3) verifying (6·1) also shows that $\Delta_{r/p}$ has index $J_2(r)$ inside $\mathrm{SL}_2(\mathbb{Z}[1/p])$, which is significantly stronger than $\Delta_{r/p}$ being non-free.

We first verify Conjecture 1·1 (unconditionally) for small r, using Theorem 5·1:

PROPOSITION 6·1. *Let p be a prime, and let* $\gcd(r, p) = 1$. *If* $r \in \{1, 2, 3, 4\}$, *then*

$$\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r). \tag{6·2}$$

In particular, in these cases $[\mathrm{SL}_2(\mathbb{Z}[1/p]) : \Delta_{r/p}] = J_2(r)$.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

Proof. The case of $r = 1$ was handled already in Proposition 3·1. By Theorem 5·1, we now have to verify (6·1), i.e. that $U_p^{k\sigma_p(r)}$ lies in $\Delta_{r/p}$ for some non-zero k. In particular, we guide our search by looking for $U_p^{\sigma_p(r)}$, as this always lies in $\overline{\Gamma}_1^{(p)}(r)$. Throughout, we will write Q for $Q_{r/p}$.

(i) If $r = 2$, then $\sigma_p(r) = 1$, and $U_p \in \Delta_{r/p}$ as x‘

$$U_p = \begin{pmatrix} p & 0 \\ 0 & 1/p \end{pmatrix} = Q^s A^{\frac{p-1}{2}} Q^{-1} A^{-\frac{p(p-1)}{2}}.$$

Note that the condition $\gcd(r, p) = 1$ (i.e. p is odd) makes all exponents above integral.

(ii) If $r = 3$, then $\sigma_p(r)$ depends on the congruence class of $p \pmod 3$, being either 1 or 2:

(a) if $p \equiv 1 \pmod 3$, then $\sigma_p(3) = 1$, and $U_p \in \Delta_{3/p}$, as

$$U_p = \begin{pmatrix} p & 0 \\ 0 & \frac{1}{p} \end{pmatrix} = Q^{\frac{p(p-1)}{3}} A Q^{-\frac{p-1}{3}} A^{-p};$$

(b) if $p \equiv 2 \pmod 3$, then $\sigma_p(3) = 2$, and $U_p^2 \in \Delta_{3/p}$ as

$$-U_p = \begin{pmatrix} -p & 0 \\ 0 & -\frac{1}{p} \end{pmatrix} = Q^{\frac{p(p+1)}{3}} A^{-1} Q^{\frac{p+1}{3}} A^{-p}.$$

(iii) If $r = 4$, then we again split depending on the congruence class of $p \pmod 4$, which is either 1 or 3. If $p \equiv 1 \pmod 4$, then $\sigma_p(r) = 1$, so we should have $U_p \in \Delta_{4/p}$. If $p \equiv 3 \pmod 4$, then $\sigma_p(r) = 2$, so we should have $U_p^2 \in \Delta_{4/p}$. We verify this:

(a) if $p \equiv 1 \pmod 4$, then $U_p \in \Delta_{4/p}$, as $U_p = Q^p A^{\frac{p-1}{4}} Q^{-1} A^{-\frac{p(p-1)}{4}}$;

(b) if $p \equiv 3 \pmod 4$, then $-U_p \in \Delta_{4/p}$, as $-U_p = Q^{-p} A^{\frac{p+1}{4}} Q^{-1} A^{\frac{p(p+1)}{4}}$. In particular, we have $U_p^2 \in \Delta_{4/p}$.

Thus, in all cases we have verified (6·1), so we are done.

It seems feasible to prove that $\overline{\Gamma}_1^{\mathbb{Z}}(5) \leq \Delta_{5/p}$ for all primes p coprime with 5. We can prove it directly in most cases, using arguments completely analogous to those of Theorem 5·4 (and bypassing Artin's conjecture).

PROPOSITION 6·2. *Let $p \neq 5$ be a prime such that $p \not\equiv -1, 1 \pmod{11}$. Then*

$$\Delta_{5/p} = \overline{\Gamma}_1^{(p)}(r). \tag{6·3}$$

In particular, in these cases $[\mathrm{SL}_2(\mathbb{Z}[1/p]) : \Delta_{r/p}] = J_2(r)$.

Proof. It is well known that $\overline{\Gamma}_1^{\mathbb{Z}}(5)$ is generated by $A, Q_{5/p}^p$, together with a third matrix, which can be taken as

$$M_5 := \begin{pmatrix} 11 & 20 \\ -5 & -9 \end{pmatrix}.$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

The group of quadratic residues mod 11 has order 5, and is hence generated by any non-trivial quadratic residue; since $p \not\equiv -1, 1 \pmod{11}$, it follows that $p^2 \not\equiv 1 \pmod{11}$, so p^2 generates the quadratic residues mod 11. Since $\sigma_p(5) \leq 4$ for all p, it follows that $p^{2\sigma_p(5)k}$ generates the quadratic residues mod 11 for any $k \not\equiv 0 \pmod 5$. Thus, arguing as in the proof of Theorem 5·4, we have that $M_5 \in \Delta_{5/p}$, and so also $\overline{\Gamma}_1^{\mathbb{Z}}(5) \leq \Delta_{5/p}$.

Hence, by Corollary 4·5, it remains to verify that some power of $U_p^{\sigma_p(r)}$ lives in $\Delta_{r/p}$. We do this now. We must split based on the congruence class $\pmod 5$. First, the case of $p = 2$ is easily dealt with, since $\sigma_2(5) = 4$ and we have

$$-U_2^2 = A^2 Q A^{-1} Q A^{-1} Q^{-2}$$

so $U_2^4 \in \Delta_{5/2}$. Now let p be any odd prime. Then p is one of $\{1, 3, 7, 9\}$ modulo 10.

(i) If $p \equiv 1 \pmod{10}$, then we have

$$U_p^2 = A^p Q^{\frac{p-1}{5}} A^{-p-1} Q^{-\frac{p-1}{5}} A Q^{-\frac{(p+1)p(p-1)^2}{5}}.$$

(ii) If $p \equiv 3 \pmod{10}$, then the matrix

$$A^p Q^{\frac{2(p-3)}{5}+1} A^{\frac{p-3}{2}+1} Q^{-\frac{p-3}{5}-1} A$$

is upper triangular with $-p^2$ and $-p^{-2}$ on the diagonal and with upper right entry a multiple of $5p^{-2}$. In particular, right multiplying it by a suitable (rather large) multiple of Q will give $-U_p^2$, and thereby also U_p^4.

(iii) If $p \equiv 7 \pmod{10}$, then the matrix

$$A^p Q^{-\frac{2(p-7)}{5}-3} A^{-\frac{p-7}{2}-3} Q^{-\frac{p-7}{5}-1} A$$

is also upper triangular with $-p^2$ and $-p^{-2}$ on the diagonal and with upper right entry a multiple of $5p^{-2}$. Again, we obtain $-U_p^2$, and hence also U_p^4.

(iv) If $p \equiv 9 \pmod{10}$, then the matrix

$$A^p Q^{-\frac{(p-9)}{5}-2} A^{p+1} Q^{-\frac{(p-9)}{5}-2} A$$

is upper triangular as previously; and we find $-U_p^2$ and U_p^4 as before.

This completes the proof of the result.

A more detailed analysis can doubtlessly be used to eliminate the condition that $p \not\equiv -1, 1 \pmod{11}$ in Proposition 6·2. Next, conditional on the strengthened Artin's conjecture, we are able to verify the conditions of Corollary 5·4 in some other particular cases, this time being infinite families with arbitrarily large numerators.

THEOREM 6·3 *Let p be a prime. Assume the strengthened form of Artin's conjecture on primitive roots (Conjecture 5.3) holds for p. If one of the following hold*:

(i) $r = p - 1$;

(ii) $r = p + 1$;

(iii) $r = \frac{p+1}{2}$ (and $p \neq 2$);

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

then the group $\Delta_{r/p}$ equals $\overline{\Gamma}_1^{(p)}(r)$. In particular, $\Delta_{r/p}$ has index $J_2(r)$ in $\mathrm{SL}_2(\mathbb{Z}[1/p])$.

Proof. Throughout this proof, we will let $Q = Q_{r/p}$, where the r is always as given in the individual subcases.

If $r = p - 1$, then since $\sigma_p(p-1) = 1$ it suffices, in view of Corollary 5·4, to verify that $U_p \in \Delta_{(p-1)/p}$. But this is easy to verify: $U_p = Q^p A Q^{-1} A^{-p}$.

If $r = p + 1$, then since $\sigma_p(p+1) = 2$, it suffices to verify that $U_p^2 \in \Delta_{r/p}$, and

$$U_p^2 = \begin{pmatrix} p^2 & 0 \\ 0 & 1/p^2 \end{pmatrix} = Q^{p^3-p^2-p} A Q^{-1} A^p Q A^{-1} Q A^{-p}.$$

Finally, if $r = p + 1/2$, we first single out the case $p = 3$. In this case, $\sigma_p(r) = \sigma_3(2) = 1$, and $U_p = Q^{-3} A^{-1} Q A^3$. Suppose now that $p > 3$. Then $\sigma_p(r) = 2$, and as $-U_p = Q^{-2p} A Q^{-2} A^p$, it follows that $U_p^2 \in \Delta_{r/p}$.

The rational numbers appearing in Theorem 6·3 are well known to be relation numbers, and Theorem 6·3 also (conditionally) recovers this result.

6·1. *Strong relation numbers*

We will now give another corollary of the methods of this paper. As mentioned in §3, to prove that $\Delta_{r/p}$ is not free it suffices to find *some* upper (or lower) triangular matrix as a non-trivial product of A and $Q_{r/p}$. We now introduce a new condition on r/p which strengthens this (although, as we shall conjecture, this is not actually a strengthening). Let $0 < r/p < 4$ with $\gcd(r, p) = 1$, i.e. let r/p be admissible. Then we say that r/p is a *strong* relation number if there exists some non-trivial product in A and $Q_{r/p}$ which equals an upper (or lower) triangular matrix in which the diagonal elements are not 1. For example, the number $3/2$ is a strong relation number, as

$$A^2 Q_{3/2}^{-1} A = \begin{pmatrix} -1/2 & -3/2 \\ 0 & -2 \end{pmatrix}.$$

To have r/p be a strong relation number is a necessary and sufficient condition for $\Delta_{r/p}$ having finite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$. More precisely, we have:

THEOREM 6·4. *Let p be prime and $\gcd(p, r) = 1$. Assume the strengthened form of Artin's conjecture on primitive roots (Conjecture 5·3) holds for p. Then the following are equivalent* :

(i) r/p is a strong relation number;

(ii) $U_p^{\sigma_p(r)} \in \Delta_{r/p}$;

(iii) $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$;

(iv) $[\mathrm{SL}_2(\mathbb{Z}[1/p]) : \Delta_{r/p}] = J_2(r)$.

Proof. Let us suppose that r/p is a strong relation number, i.e. that

$$M = \begin{pmatrix} p^k & b \\ 0 & p^{-k} \end{pmatrix}$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

lies in $\Delta_{r/p}$ for some non-zero k and $b \in \mathbb{Z}[1/p]$. Then $Q_{r/p} M Q_{r/p}^{-1} = U_p^k$. Since $\Delta_{r/p} \leq \overline{\Gamma}_1^{(p)}(r)$, it follows that k must be a multiple of the multiplicative order of $p \pmod r$. By Corollary 5·4, the result follows.

We mention one of the curious consequences of the (still conjectural, in general) equality $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$. This is the fact that it implies that $\Delta_{r/p^k} = \Delta_{r/p}$ for all $k \geq 1$, as the generator Q_{r/p^k} is an element of $\overline{\Gamma}_1^{(p)}(r)$. This can be observed in many cases without any theory; for example, $\Delta_{7/3} = \Delta_{7/3^k}$, as one checks that

$$Q_{7/3^k} = \begin{pmatrix} 1 & 7/3^k \\ 0 & 1 \end{pmatrix} = A^{3^k} Q_{7/3}^{-1} A^{3^{k-1}} Q_{7/3}^{-1} A^{3^k}$$

for all $k \geq 1$. Finding such equalities is very difficult in general, as it involves finding a non-trivial product of A and $Q_{r/p}$ equalling an upper triangular matrix. Nevertheless, it provides targets for *which* upper triangular matrices to generate.

EXAMPLE 6·5 *Assume Conjecture 5·3 holds. We will prove that* $\Delta_{8/3}$ *has finite index in* $\mathrm{SL}_2(\mathbb{Z}[1/3])$ *by proving that* $8/3$ *is a strong relation number. This is direct:*

$$A^6 Q_{8/3}^{-1} A Q_{8/3}^{-1} A = \begin{pmatrix} 1/9 & 16/9 \\ 0 & 9 \end{pmatrix}.$$

Hence $8/3$ *is a strong relation number, so by Theorem 6·4 we have that* $\Delta_{8/3}$ *has index* $J_2(8) = 48$ *in* $\mathrm{SL}_2(\mathbb{Z}[1/3])$. *This can be verified computationally, see Table 1.*

Finally, we list the conjectures about $\Delta_{r/p}$ made (explicitly or implicitly) in this article. Recall that an *admissible* rational r/p is one where $0 \leq r/p \leq 4$.

CONJECTURE 6·6. *For all admissible* $r, p \in \mathbb{Z}$ *with* $\gcd(r, p) = 1$, *the following hold*:

(i) r/p is a relation number;
(ii) $\Delta_{r/p}$ has finite index in $\mathrm{SL}_2(\mathbb{Z}[1/p])$ (and is a congruence subgroup);
(iii) $\Delta_{r/p} = \overline{\Gamma}_1^{(p)}(r)$, and $[\mathrm{SL}_2(\mathbb{Z}[1/p]) : \Delta_{r/p}] = J_2(r)$;
(iv) $U_p^{\sigma_p(r)} \in \Delta_{r/p}$, where $\sigma_p(r)$ is the multiplicative order of p mod r;
(v) r/p is a strong relation number;
(vi) $\Delta_{r/p} = \Delta_{r/p^k}$ for all $k \geq 1$;
(vii) $\mathrm{SL}_2(\mathbb{Z}[1/p]) = \Delta_{r/p} \cdot \mathrm{SL}_2(\mathbb{Z})$.

With the exception of (i) and (ii), all the conjectures are original to this article. I. Smilga (personal communication) has informed the author that he has a proof of Conjecture (vii), which will appear in forthcoming work.

Remark 6·7. Let us make some remarks on the group generated by the two matrices

$$X_\mu = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad Y_\mu = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

Let us write $\diamondsuit_\mu = \langle X_\mu, Y_\mu \rangle$. Chang, Jennings and Ree [9] proved that $\diamondsuit_\mu \cong \Delta_{\mu^2}$. This isomorphism is not, however, an equality as subsets of $\mathrm{SL}_2(\mathbb{C})$. If $\mu = r/p$, then similar reasoning as in this paper about $\diamondsuit_{r/p}$ should give similar conjectures as for $\Delta_{r/p}$. For example, it seems as if

$$\left[\mathrm{SL}_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) : \diamondsuit_{r/p}\right] = J_2(r^2)$$

and that $\diamondsuit_{r/p}$ consists of the preimage of the matrices in $\mathrm{SL}_2(\mathbb{Z}/r^2\mathbb{Z})$ whose diagonal entries are congruent to 1 mod r (not r^2), and whose off-diagonal elements are congruent to 0 mod r. Of course, there are r^2 such matrices.

Lyndon and Ullman [22] in fact seem to have been close to this fact. On [22, p. 1402], they consider the group $\diamondsuit_{3/2}$, and mention that the group is contained in the principal congruence subgroup $\Gamma^{(2)}(3)$, which they denote $\mathbf{U}(3)$, in $\mathrm{SL}_2(\mathbb{Z}[1/2])$, but that it does not appear to coincide with it. This is correct; however, on the next line, they write that the group $\diamondsuit_{3/2}$ contains $\left(\begin{smallmatrix} 8 & 0 \\ 0 & 1/8 \end{smallmatrix}\right)$. This is not correct. Indeed, it contradicts the preceding statement: $8 \equiv 2 \pmod 3$, so $\left(\begin{smallmatrix} 8 & 0 \\ 0 & 1/8 \end{smallmatrix}\right)$ cannot possibly be an element of $\Gamma^{(2)}(3)$. On the other hand, it is not hard to verify that

$$\begin{pmatrix} -8 & 0 \\ 0 & -1/8 \end{pmatrix} = X_{3/2}^{12}(Y_{3/2}X_{3/2}^{-1})^2 X_{3/2}^{-1} Y_{3/2}^{-2} \in \diamondsuit_{3/2},$$

so it is clear that a minus sign is simply missing from the assertion in Lyndon and Ullman. It is also not difficult to prove Lyndon and Ullman's assertion that $\diamondsuit_{3/2}$ is a proper subgroup of $\Gamma^{(2)}(3)$, and indeed $[\Gamma^{(2)}(3):\diamondsuit_{3/2}] = 3$. Representatives for these three cosets of $\diamondsuit_{3/2}$ in $\Gamma^{(2)}(3)$ are easy to construct: they can be taken as 1, $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 1/4 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 16 & 0 \\ 0 & 1/16 \end{smallmatrix}\right)$. We do not develop this theory further here, but doing this, one is led to entirely analogous conjectures as for $\Delta_{r/p}$.

Acknowledgements. I would like to thank Sang-hyun Kim (KIAS) for introducing me to the freeness problem for $\Delta_{r/p}$ and for many helpful discussions at every stage of this project. I also wish to thank G. Arzhantseva (Univ. Vienna) for very useful remarks and discussions about the history of the freeness problem for $\Delta_{r/p}$, and A. L. Talambutsa (Steklov Institute) for providing me with copies of the very inaccessible articles by Sanov [33] and Fuchs-Rabinovich [13]. The research was carried out while the author was supported by the Mid-Career Researcher Program (RS-2023-00278510) through the National Research Foundation funded by the government of Korea, and by the KIAS Individual Grant (MG094701) at Korea Institute for Advanced Study.

REFERENCES

[1] A. S. DETINKO, D. L. FLANNERY. A. H. FREENESS and *s*-arithmeticity of rational Möbius groups. *Preprint*: ArXiv:2203.17201 (2022).
[2] H. BEHR and J. MENNICKE. A presentation of the groups PSL(2, *p*). *Canadian J. Math.* **20** (1968), 1432–1438.
[3] F. R. BEYL. The Schur multiplicator of SL (2, $\mathbf{Z}/m\mathbf{Z}$) and the congruence subgroup property. *Math. Z.* **191** (1986), 23–42.
[4] J. L. BRENNER. Quelques groupes libres de matrices. *C. R. Acad. Sci. Paris* **241** (1955), 1689–1691.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

[5] J. L. BRENNER and A. CHARNOW. Free semigroups of 2×2 matrices. *Pacific J. Math.* **77** (1978), 57–69.
[6] J. L. BRENNER, R. A. MACLEOD, and D. D. OLESKY. Non-free groups generated by two 2×2 matrices. *Canadian J. Math.* **27** (1975), 237–245.
[7] N. BRODY, D. FISHER, M. MJ, and W. VAN LIMBEEK. Greenberg longer Shalom's commensurator hypothesis and applications. ArXiv:2308.07785 (2023).
[8] K. S. BROWN 1982. *Cohomology of Groups*, Graduate Texts in Math. vol 87 (Springer-Verlag, new YOuk-Berlin, 1982)
[9] B. CHANG, S. A. JENNINGS, and R. REE. On certain pairs of matrices which generate free groups. *Canadian J. Math.* **10** (1958), 279–284.
[10] A. CHARNOW. A note on torsion free groups generated by pairs of matrices. *Canad. Math. Bull.* **17** (1974/75), 747–748.
[11] K. A. DONIYAKHI. Linear representation of the free product of cyclic groups. *Leningrad State Univ. Annals [Uchenye Zapiski] Math. Ser.* **10** (1940), 158–165.
[12] S. P. FARBMAN. Non-free two-generator subgroups of $SL_2(\mathbf{Q})$. *Publ. Mat.* **39** (1995), 379–391.
[13] D. I. FUCHS-RABINOVICH. On a certain representation of a free group. *Leningrad State Univ. Annals [Uchenye Zapiski] Math. Ser.* **10** (1940), 154–157.
[14] J. GILMAN. The structure of two-parabolic space: parabolic dust and iteration. *Geom. Dedicata* **131** (2008), 27–48.
[15] R. GUPTA and M. R. MURTY. A remark on Artin's conjecture. *Invent. Math.* **78** (1984), 127–130.
[16] D. R. HEATH-BROWN. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)* **37** (1986), 27–38.
[17] C. HOOLEY. On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220.
[18] Y. A. IGNATOV. Rational nonfree points of the complex plane. In *Algorithmic Problems in the Theory of Groups and Semigroups (Russian)*, (Tulsk. Gos. Ped. Inst., Tula, 19860 , pp. 72-80, 127. 1986
[19] C. JORDAN . *Traité des Substitutions et des équations Algébriques*. (Gauthier-Villars, 1870)
[20] L. KEEN and C. SERIES. The Riley slice of Schottky space. *Proc. London Math. Soc. (3)* 69 (1994), 72–90.
[21] S. H. KIM and T. KOBERDA. Non-freeness of groups generated by two parabolic elements with small rational parameters. *Michigan Math. J.* 71 (2022), 809–833.
[22] R. C. LYNDON and J. L. ULLMAN. Groups generated by two parabolic linear fractional transformations. *Canadian J. Math.* **21** (1969), 1388–1403.
[23] W. MAGNUS. Untersuchungen über einige unendliche diskontinuierliche Gruppen. *Math. Ann.* **105** (1931), 52–74.
[24] A. MARKOV. On certain insoluble problems concerning matrices. *Doklady Akad. Nauk SSSR (N.S.)* **57** (1947), 539–542.
[25] V. D. MAZUROV and E. I. KHUKHRO. *Unsolved problems in Group Theory, the Kourovka Notebook (no. 20)*, (2023).
[26] J. MENNICKE. On Ihara's modular group. *Invent. Math.* **4** (1967), 202–228.
[27] Y. I. MERZLJAKOV. Matrix representations of free groups. *Dokl. Akad. Nauk SSSR* **238** (1978), 527–530.
[28] Y. I. MERZLYAKOV. Linear groups. In *Algebra, Topology, Geometry, Vol. 16 (Russian)*. Itogi Nauki i Tekhniki, **247**. (Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow. 1978), pp. 35-89.
[29] P. MOREE. Artin's primitive root conjecture—a survey. *Integers* **12** (2012), 1305–1416.
[30] M. F. NEWMAN, editor. *Proceedings of the Second International Conference on the Theory of Groups*. Lecture Notes in Math. Vol. 372. (Springer-Verlag, Berlin-New York, 1974. Held at the Australian National University, Canberra, (August 13–24, 1973), With an introduction by B. H. Neumann.
[31] C.-F. NYBERG-BRODDA. The abelianisation of $SL_2(\mathbb{Z}[\frac{1}{m}])$. *J. Algebra* **660** (2024), 614–618.
[32] I. N. SANOV. Solution of Burnside's problem for exponent 4. *Leningrad State Univ. Annals [Uchenye Zapiski] Math. Ser.* **10** (1940), 166–170.
[33] I. N. SANOV. A property of a representation of a free group. *Doklady Akad. Nauk SSSR (N.S.)* **57** (1947), 657–659.
[34] J.-P. SERRE. Le problème des groupes de congruence pour SL2. *Ann. of Math. (2)* **92** (1970), 489–527.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press

[35] J.-P. SERRE. *Trees*. (Springer-Verlag, Berlin-New York 1980). Translated from the French by John Stillwell.

[36] I. SMILGA. New sequences of non-free rational points. *C. R. Math. Acad. Sci. Paris* **359** (2021), 983–989.

https://doi.org/10.1017/S0305004125101333 Published online by Cambridge University Press