ALGORITHMS FOR ARITHMETIC GROUPS WITH THE CONGRUENCE SUBGROUP PROPERTY

A. S. DETINKO, D. L. FLANNERY, AND A. HULPKE

Dedicated to the memory of Ákos Seress

ABSTRACT. We develop practical techniques to compute with arithmetic groups $H \leq SL(n, \mathbb{Q})$ for $n > 2$. Our approach relies on constructing a principal congruence subgroup in $H$. Problems solved include testing membership in $H$, analyzing the subnormal structure of $H$, and the orbit-stabilizer problem for $H$. Effective computation with subgroups of $GL(n, \mathbb{Z}_m)$ is vital to this work. All algorithms have been implemented in GAP.

In [8, 9, 10] we established methods for computing with finitely generated linear groups over an infinite field, based on the use of congruence homomorphisms. These have been applied to test virtual solvability and answer questions about solvable-by-finite (SF) linear groups.

Computing with finitely generated linear groups that are not SF is a largely unexplored topic. These groups comprise a wide class in which certain algorithmic problems are undecidable [6, Section 3]. We might be more confident of progress if we restrict ourselves to arithmetic subgroups of linear algebraic groups. Decision problems for such groups were investigated by Grunewald and Segal [17]; see also [7]. We note renewed activity focussed on deciding arithmeticity [32].

This paper is a revision of [11], which provides a starting point for computation with semisimple arithmetic groups that have the congruence subgroup property (CSP). A prominent example is $\Gamma_n = SL(n, \mathbb{Z})$, $n \geq 3$. Recall that $H \leq SL(n, \mathbb{Q})$ is arithmetic if $\Gamma_n \cap H$ has finite index in both $H$ and $\Gamma_n$ (in particular, finite index subgroups of $\Gamma_n$ are arithmetic). Each arithmetic group $H \leq SL(n, \mathbb{Q})$ contains a principal congruence subgroup $\Gamma_{n,m}$ for some $m$, namely the kernel of the congruence homomorphism $\Gamma_n \rightarrow SL(n, \mathbb{Z}_m)$ induced by natural surjection $\mathbb{Z} \rightarrow \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ [3, 27]. So if we know that $\Gamma_{n,m} \leq H$ then we can transfer much of the computing to $SL(n, \mathbb{Z}_m)$, for which efficient machinery is available [20]. We give a method to construct $\Gamma_{n,m}$ in $H$. This implies that membership testing and other fundamental problems are decidable.

We pay special attention to subnormality and the orbit-stabilizer problem. Aside from their computational importance, these were the earliest questions considered for arithmetic groups. The study of subnormal subgroups of $\Gamma_n$ originated in the late 19th century and led up to formulation of the Congruence Subgroup Problem. In turn, the solution of that problem used knowledge of $\Gamma_n$-orbits in $\mathbb{Q}^n$ [21, §17].

The paper is organized as follows. Section 1 covers background on arithmetic groups: basic facts; material about principal congruence subgroups (their generating sets, maximality); and subnormal structure. Section 2 details relevant theory of matrix groups over $\mathbb{Z}_m$ and computing in $GL(n, \mathbb{Z}_m)$. In Section 3 we give a suite of algorithms for arithmetic groups in $\Gamma_n$. After verifying decidability, we describe computing a maximal principal congruence subgroup; membership testing; and aspects of subnormality, e.g., testing whether an arithmetic group $H \leq \Gamma_n$ is subnormal or normal, and constructing the normal closure of a subgroup of $\Gamma_n$. In Section 4 we solve the orbit-stabilizer problem for arithmetic groups in $\Gamma_n$ acting on $\mathbb{Q}^n$. Our solution draws on a comprehensive description of orbits and stabilizers for a principal congruence subgroup acting on $\mathbb{Z}^n$. Section 5 shows how to extend results from $\Gamma_n$ to $SL(n, \mathbb{Q})$. Finally, we examine the performance of our GAP [16] implementation of the algorithms.
We remark that the scope of this paper may be widened to other groups with the CSP, such as $\text{Sp}(2m, \mathcal{O}_P)$ or $\text{SL}(n, \mathcal{O}_P)$ for $m \geq 2$ and $n > 2$, where $\mathcal{O}_P$ is the ring of integers of a number field $\mathbb{P}$ that is not totally imaginary [3].

1. **Arithmetic Subgroups of $\text{SL}(n, \mathbb{Q})$: Background**

1.1. **Preliminaries.** Let $R$ be a commutative ring with 1, and $I \subseteq R$ be an ideal. The natural surjection $R \to R/I$ induces a congruence homomorphism $\varphi_I : \text{Mat}(n, R) \to \text{Mat}(n, R/I)$. Let $G_n = \text{GL}(n, R)$ and $\Gamma_n = \text{SL}(n, R)$. The kernel of $\varphi_I$ on $\Gamma_n$ or $G_n$ is a principal congruence subgroup (PCS) of level $I$. Such a subgroup of $\Gamma_n$ will be denoted $\Gamma_{n,I}$. We set $\Gamma_{n,R} = \Gamma_n$. If $R = \mathbb{Z}$ then $R/I = \mathbb{Z}_m$ for some non-negative integer $m$, and the subscript ‘$I$’ is replaced by ‘$m$’.

For computational purposes, $\Gamma_n$ and $G_n$ should be finitely generated, and proper quotients of $R$ should be finite. The latter is true if $R = \mathcal{O}_P$ or $R$ is the univariate polynomial ring $\mathbb{F}_q[x]$ over the finite field $\mathbb{F}_q$ of size $q$. These are two major types of ambient ring $R$ encountered when computing with finitely generated linear groups.

Define $t_{ij}(a) = 1 + e_{ij}(a)$, where $e_{ij}(a) \in \text{Mat}(n, R)$ has $a$ in position $(i, j)$ and zeros everywhere else. The matrices $t_{ij}(a)$ for distinct $i, j$ are transvections. The subgroup $E_{n,I} = \langle t_{ij}(a) : a \in I, 1 \leq i, j \leq n, i \neq j \rangle$ of $\Gamma_{n,I}$ is the elementary group of level $I$. We write $e_{ij}, t_{ij}, E_n$ for $e_{ij}(1), t_{ij}(1), E_{n,R}$ respectively.

**Lemma 1.1.**

(i) For all $i \neq j$, $[t_{ij}(a), t_{ji}(b)] = 1 + e_{ij}(a^2b) - e_{ji}(ab^2) + e_{ii}(ab + a^2b^2) - e_{jj}(ab)$. 
(ii) If $i, j, k$ are pairwise distinct then $[t_{ij}(a), t_{jk}(b)] = t_{ik}(ab)$ and $[t_{ij}(a), t_{ki}(b)] = t_{kj}(-ab)$.
(iii) If $i \neq l$ and $j \neq k$ then $t_{ij}(a)$ commutes with $t_{kl}(b)$.

**Proposition 1.2.** In each of the following situations, $\Gamma_n = E_n$: (i) $n \geq 2$ and $R$ is Euclidean or semi-local; (ii) $n \geq 3$ and $R$ is a Hasse domain of a global field.

**Proof.** See [19] 4.3.9, pp. 172–173. \hfill \Box

**Remark 1.3.** $\mathcal{O}_P$ is a Hasse domain of a global field, $\mathbb{F}_q[x]$ is Euclidean, and $\mathbb{Z}_m$ is semi-local.

**Proposition 1.2** implies that $\varphi_n$ maps $\text{SL}(n, \mathbb{Z})$ onto $\text{SL}(n, \mathbb{Z}_m)$. However, $\varphi_I : \text{GL}(n, R) \to \text{GL}(n, R/I)$ may not be surjective.

**Proposition 1.4.** Let $R = \mathcal{O}_P$ or $\mathbb{F}_q[x]$. If $n > 2$ or $R = \mathcal{O}_P$ then $E_n$, $\Gamma_n$, and $G_n$ are finitely generated. None of the groups $E_2, \Gamma_2$, or $G_2$ is finitely generated when $R = \mathbb{F}_q[x]$.

**Proof.** If $n \geq 3$ then $\Gamma_n = E_n$ is finitely generated by [19] 4.3.11, p. 174; hence so too is $G_n$, by [19] 1.2.17, p. 29] and Dirichlet’s unit theorem. See [19] 4.3.16, p. 175] and subsequent comments for the remaining claims. \hfill \Box

The notation $A \leq_f B$ means that $A$ is of finite index in the group $B$. For $n \geq 3$, $\Gamma_n = \text{SL}(n, \mathbb{Z})$ has the congruence subgroup property: $H \leq_f \Gamma_n$ is equivalent to $H$ containing some $\Gamma_{n,m}$ [3, 27]. On the other hand, $\Gamma_2$ does not have the CSP [35 §1.1].

1.2. **Generators of congruence subgroups.** Let $R = \mathbb{Z}$. We first discuss generating sets for $G_n$ and $\Gamma_n$, and thus for their homomorphic images $\overline{\Gamma_n} = \text{GL}(n, \mathbb{Z}_m), \overline{\Gamma_n} = \text{SL}(n, \mathbb{Z}_m)$.

By **Lemma 1.1**(ii), the transvections $t_{12}, \ldots, t_{1n}, t_{21}, \ldots, t_{n1}$ constitute a generating set for $\Gamma_n = E_n$. In fact $\Gamma_n$ has a generating set of minimal size 2: $t_{12}$ and 

$$
\begin{pmatrix}
0 & 1_{n-1} \\
(-1)^{n-1} & 0
\end{pmatrix},
$$




see [31, p. 107]. Adding the diagonal matrix diag(−1, 1, . . . , 1) produces a generating set for $G_n$ of size 3 (better still, it is known that $G_n$ is 2-generated). Similarly, two generators of $\Gamma_n$, together with all diagonal matrices diag(α, 1, . . . , 1) as α runs over a generating set for the unit group $\mathbb{Z}_m^*$ of $\mathbb{Z}_m$, generate $\Gamma_n$. If $m = 2$ or an odd prime power then $G_n$ is 2-generated. For all $k \geq 3$, $\text{GL}(n, \mathbb{Z}_{2^k})$ is 4-generated, and $\text{GL}(n, \mathbb{Z}_4)$ is 3-generated.

The normal closure of $A$ in $B$ is denoted $A^B$. Let $(k, l)$ be the permutation matrix obtained by swapping rows $k$ and $l$ of $1_n$.

**Lemma 1.15.** For any $i \neq j$, $E_{n,m}^{\Gamma_n} = \langle t_{ij}(m) \rangle^{\Gamma_n}$.

**Proof.** Put $N = \langle t_{ij}(m) \rangle^{\Gamma_n}$. We prove that $t_{kl}(m) \in N$ for all $k \neq l$. By Lemma 1.1(ii),

$$t_{kj}(m) = t_{ij}(m)t_{ij}(-m)^t_{kj}, \quad k \neq j, i;$$

so $t_{kj}(m) \in N$. Then $t_{kl}(m) = [t_{kj}(m), t_{jl}] \in N$ if $k, l \neq j$. Since $t_{kl}(m) = t_{lk}(-m)^{(k,l)d}$ where $d = \text{diag}(1, . . . , 1, -1, 1, . . . , 1)$ with $-1$ in position $k$, this concludes the proof. □

**Proposition 1.16.** If $n \geq 3$ and $i \neq j$ then $\Gamma_{n,m} = \langle t_{ij}(m) \rangle^{\Gamma_n} = E_{n,m}^{\Gamma_n}$ (hence $\Gamma_{n,m} = E_{n,m}^{G_n}$).

**Proof.** See [3], [4], or [27]. □

**Remark 1.7.** For $n, m > 1$, $E_{n,m}$ is not normal in $\Gamma_n$.

**Remark 1.8.** $E_{n,m_1} \leq E_{n,m_2} \iff \Gamma_{n,m_1} \leq \Gamma_{n,m_2} \iff m_2 \mid m_1$.

A PCS in $\Gamma_n$ for $n \geq 3$ is the image under $\varphi_m$ of a PCS in $\Gamma_n$.

**Corollary 1.9.** Let $I$ be an ideal of $\mathbb{Z}_m$, so $\mathbb{Z}_m/I \cong \mathbb{Z}_a$ for some divisor $a$ of $m$. If $n \geq 3$ then the kernel $\Gamma_{n,a}$ of $\varphi_I$ on $\Gamma_n = \text{SL}(n, \mathbb{Z}_m)$ is

$$\{1_n + ax \in \Gamma_n \mid x \in \text{Mat}(n, \mathbb{Z}_m)\} = \varphi_m(\Gamma_{n,a}) = E_{n,a}^{\Gamma_n}.$$

Furthermore, $\Gamma_{n,a} = \langle t_{ij}(a) \rangle^{\Gamma_n} = \langle t_{ij}(a) \rangle^{\Gamma_n}$ for any $i$ and $j \neq i$.

**Proposition 1.10.** If $n \geq 3$ then $\Gamma_{n,m}$ has generating set

$$\{t_{ij}(m)^g \mid 1 \leq i < j \leq n, g \in \Sigma\}$$

where

$$\Sigma = \{1_n, (k, l), 1_n - 2e_{kk} - 2e_{k+1,k+1} + e_{k+1,k} \mid 1 \leq k < l \leq n\}.$$  

**Proof.** See [36]. □

We emphasize that the number of generators in (1) does not depend on $m$. The minimal size of a generating set for $\Gamma_{n,m}$ is unknown. However, by Lemma 2.10 below, this size can be no less than $n^2 - 1$. As Professor A. Lubotzky has pointed out to us, [33, Theorem 1] and Lemma 2.10 imply that $\Gamma_{n,m}$ has a generating set of size $n^2 + 2$. In [23] it is conjectured that $\Gamma_{n,m}$ for $n \geq 3$ contains a 2-generator subgroup of finite index (cf. [22, p. 412]). This conjecture has been settled affirmatively (see [26]), so $\Gamma_{n,m}$ is $(n^2 + 1)$-generated.

Let min$(H)$ denote the minimal size of a generating set of $H$. Although min$(H)$ can be arbitrarily large [36, pp. 355–356], we have

**Lemma 1.11.** Suppose that $n \geq 3$ and $\Gamma_{n,m} \leq H \leq \Gamma_n$. Then min$(H)$ is bounded above by a function of $n, m$ only.

**Proof.** This is clear from Proposition 1.10 and the fact that $|H : \Gamma_{n,m}| \leq |\text{SL}(n, \mathbb{Z}_m)|$. □
1.3. Constructing a PCS in an arithmetic subgroup. Let \( n \geq 3 \). Our overall strategy rests on knowing some \( \Gamma_{n,m} \) in the arithmetic group \( H \leq \Gamma_n \). We show that such a PCS can always be constructed.

**Proposition 1.12.** \( \Gamma_{n,m^2} \leq E_{n,m} \), so \( |\Gamma_n : E_{n,m}| \) is finite.

**Proof.** Let \( p_{ij} = t_{ij}(m) \) and \( s_{ij} = t_{ij}(m^2) \). Then \( \Gamma_{n,m^2} \) is generated by the \( s_{ij} \) for \( i < j \) and their conjugates as in Proposition [1,10]. Our goal is to prove that these all lie in \( E_{n,m} \), i.e., that they can be expressed as words in the \( p_{ij} \). Since \( s_{ij}^{(k,l)} = p_{ij}^{m'} \) where \( i' = i^{(k,l)} \) and \( j' = j^{(k,l)} \), it suffices to look at conjugation by \( c_i = 1_n - 2e_\mu - 2e_{l+1,l+1} \) for \( l < n \). Furthermore, if \( l, l+1 \notin \{i,j\} \) then \( s_{ij} \) and \( c_l \) commute: thus it suffices to consider conjugation of \( s_{ij} \) by \( c_i, c_{i-1}, c_j, c_{j-1} \).

First we suppose that the conjugating element has subscript \( i \) or \( i-1 \). For \( j = i+1 \) and \( \alpha \notin \{i,i+1\} \),

\[
s_{ij}^\alpha = p_{ai}^{-1}p_{pa}^{-1}p_{ja}^{-1}p_{ja}p_{pa} = [p_{ja}^{-1}p_{ai}, p_{ja}p_{ia}].
\]

If \( j \neq i+1 \) we have

\[
s_{ij}^{c_{i-1}} = (p_{i+1,j})^{m-1}p_{i,i+1}p_{i+1,j}p_{i+1,j}^{-1}.
\]

For \( j \neq i-1 \),

\[
s_{ij}^{c_{i-1}} = p_{i,i-1}p_{i-1,i}^{-1}p_{i-1,j}^{-1}p_{i-1,j} = [p_{i,i-1}, p_{i-1,j}],
\]

while \( s_{i,i-1} \) and \( c_{i-1} \) commute.

Now suppose that the subscript of the conjugating element is \( j \) or \( j-1 \). For \( j \neq i+1 \),

\[
s_{ij}^{c_{j-1}} = p_{j-1,j}^{-1}p_{i,j}^{-1}p_{j-1,j}^{-1}p_{i,j}^{-1} = [p_{j+1,j}, p_{i,j+1}],
\]

If \( j = i+1 \) then \( c_{j-1} = c_i \) and (2) applies.

If \( i \neq j+1 \) then

\[
s_{ij}^{c_j} = p_{j+1,j}^{-1}p_{i,j+1}^{-1}p_{i,j+1} = [p_{j+1,j}, p_{i,j+1}],
\]

and if \( i = j+1 \), again as noted above, \( s_{ij} = s_{i,i-1} \) and \( c_j = c_{i-1} \) commute. \( \square \)

The group \( \Gamma_n \) has a (finite) presentation \( \langle t_{ij}, 1 \leq i, j \leq n, i \neq j \mid R \rangle \) where \( R \) consists of all commutator relations \( [t_{ij}, t_{km}] = 1, [t_{ij}, t_{jk}] = t_{ik} \) from Lemma [1.1](ii) and (iii), with a single extra relation \( (t_{12}t_{21}^{-1})^4 = 1 \) [29 Corollary 10.3].

**Lemma 1.13.** Given \( H \leq_f \Gamma_n \) we can find an elementary group in \( H \).

**Proof.** Express each generator of \( H \) as a product of transvections (for which see, e.g., [21] p. 99]). Then the Todd-Coxeter procedure with input \( \Gamma_n \) and \( H \) terminates, returning \( m = |\Gamma_n : H| \). So for all \( i, j \) and known \( l \) we have \( t_{ij}(l) = t_{ij}(1)^l \in H \) \( (l = \lcm\{1, \ldots, m\}) \) say. Hence \( E_{n,l} \leq H \). \( \square \)

Using Proposition [1.12] we rescue one item (slightly generalized) from the proof of Lemma [1.13]

**Lemma 1.14.** If \( |\Gamma_n : H| \leq m \) then \( \Gamma_{n,l^2} \leq H \) where \( l = \lcm\{1, \ldots, m\} \).

**Proposition 1.12** and **Lemma 1.13** yield the promised

**Corollary 1.15.** Construction of a PCS in \( H \leq_f \Gamma_n \) is decidable.
1.4. Maximal congruence subgroups. In this subsection \( n \geq 3 \) and \( G_n = \text{GL}(n, \mathbb{Z}) \).

**Lemma 1.16.** Let \( m_1, m_2 \) be positive integers, \( m = \gcd(m_1, m_2) \), and \( l = \text{lcm}(m_1, m_2) \). Then

1. \( \Gamma_{n, m_1} \Gamma_{n, m_2} = \Gamma_{n, m} \).
2. \( \Gamma_{n, m_1} \cap \Gamma_{n, m_2} = \Gamma_{n, l} \).

**Proof.** (i) For \( x \in \Gamma_n \) and integers \( a, b \) such that \( am_1 + bm_2 = m \),

\[
(i_{ij}(m)^x = (i_{ij}(m_1)^x)^a \cdot (i_{ij}(m_2)^x)^b \in \Gamma_{n, m_1} \Gamma_{n, m_2}.
\]

Thus \( \Gamma_{n, m} = \Gamma_{n, m_1} \Gamma_{n, m_2} \) by Proposition 1.6.

(ii) Certainly \( \Gamma_{n, l} \leq \Gamma_{n, m_1} \cap \Gamma_{n, m_2} \). The reverse containment is just the Chinese Remainder Theorem. \( \square \)

**Corollary 1.17.** If \( H \leq_f G_n \) then \( H \) contains a unique maximal PCS (of \( \Gamma_n \)): there is a positive integer \( m \) such that \( \Gamma_{n, m} \leq H \), and \( \Gamma_{n, k} \leq H \Rightarrow \Gamma_{n, k} \leq \Gamma_{n, m} \).

**Remark 1.18.** If \( H \) has maximal PCS \( \Gamma_{n, m} \) and \( \gcd(k, m) = 1 \) then \( \varphi_k(H) = \text{SL}(n, \mathbb{Z}_k) \). Hence we know \( \nu \) such that \( \varphi_p(H) = \text{SL}(n, p) \) for all primes \( p > \nu \); cf. the query raised at the foot of [24, p. 126].

**Remark 1.19.** Although \( H \) similarly contains a unique maximal elementary subgroup \( E_{n, m} \), the \( \Gamma_n \)-normal closure of \( E_{n, m} \) need not be the maximal PCS in \( H \), nor even be in \( H \).

**Remark 1.20.** Lemma 1.14 provides an upper bound on \( m \) such that \( \Gamma_{n, m} \) is the maximal PCS of an arithmetic group in \( \Gamma_n \); cf. [25, Proposition 6.1.1, p. 115].

**Lemma 1.21.** Each subgroup of \( \overline{G}_n = \text{GL}(n, \mathbb{Z}_m) \) contains a (perhaps trivial) unique maximal PCS of \( \overline{\Gamma}_n = \text{SL}(n, \mathbb{Z}_m) \). In more detail, suppose that \( \Gamma_{n, m} \leq H \leq \Gamma_n \) and \( \Gamma_{n, r} \) is the maximal PCS in \( H \); then \( \Gamma_{n, r} = \varphi_m(\Gamma_{n, r}) \) is the maximal PCS in \( \overline{H} = \varphi_m(H) \).

**Proof.** Since \( \Gamma_{n, m} \leq \Gamma_{n, r} \), we have that \( r \) divides \( m \), and so \( \Gamma_{n, r} \) is a PCS in \( \overline{H} \). Corollary 1.9 tells us that each PCS in \( \overline{H} \) has the form \( \overline{\Gamma}_{n, k} = \varphi_m(\Gamma_{n, k}) \) for some \( k \mid m \). Moreover \( \Gamma_{n, k} \leq H \), because \( H \) contains \( \ker \varphi_m \). Hence \( \Gamma_{n, r} \) is as claimed. \( \square \)

1.5. Subnormal structure. Let \( Z_{n, l} \) denote the full preimage of the center (scalar subgroup) of \( \text{GL}(n, R/I) \) in \( G_n = \text{GL}(n, R) \) under \( \varphi_l \). As per [37, p. 166], the level \( \ell(h) \) of \( h = (h_{ij}) \in G_n \) is the ideal of \( R \) generated by

\[
\{ h_{ij} \mid i \neq j, 1 \leq i, j \leq n \} \cup \{ h_{ii} - h_{jj} \mid 1 \leq i, j \leq n \}.
\]

Then \( \ell(A) := \sum_{a \in A} \ell(a) \) for \( A \subseteq G_n \). So \( \ell(A) \) is the smallest ideal \( I \) such that \( A \subseteq Z_{n, l} \). When \( R \) is a principal ideal ring we write \( b \) in place of \( I = bR \). For \( R = \mathbb{Z} \) or \( \mathbb{Z}_m \), \( \ell(A) \) may be defined unambiguously as the non-negative integer or integer modulo \( m \) that generates \( \ell(A) \); e.g., \( \ell(Z_{n, k}) = \ell(\Gamma_{n, k}) = k \).

**Lemma 1.22.** If \( H = \langle S \rangle \leq G_n \) then \( \ell(H) = \ell(S) \).

**Proof.** It is evident from the definitions that \( \ell(S) \subseteq \ell(H) \) and \( \ell(ab) \subseteq \ell(a) + \ell(b) \) for \( a, b \in G_n \). Since \( \ell(a) = \ell(a^{-1}) \) by [37, Lemma 1], \( \ell(H) \subseteq \ell(S) \) as required. \( \square \)

From now on in this subsection, \( n \geq 3 \) and \( R = \mathbb{Z} \) or \( \mathbb{Z}_m \). We write \( H \models G \) to denote that \( H \leq G \) is subnormal. The defect of \( H \) is the least \( d \) such that there exists a series \( H = H_0 \leq H_1 \leq \cdots \leq H_{d-1} \leq H_d = G \).
Lemma 2.1. \( m - \chi(H) \leq H \leq Z_{n,k} \)

(i) The inclusion holds then \( d \leq e + 1 \) where \( d \) is the defect of \( H \), and the least possible \( e \) is bounded above by a function of \( n \) and \( d \) only.

Proof. See [37] Corollary 3].

Although non-scalar subnormal subgroups of \( \text{GL}(n, \mathbb{Z}) \) have finite index, this is not true for \( n = 2 \); the normal closure of \( E_{2,m} \) in \( \text{SL}(2, \mathbb{Z}) \) has infinite index for \( m > 5 \) [27, p. 31].

Theorem 1.24. Let \( H \) be a subgroup of \( G_n \) of level \( l \geq 1 \), with maximal PCS \( \Gamma_{n,r} \). Then \( H \) sn \( G_n \) if and only if \( r \mid l^e \) for some \( e \). In that event, the defect of \( H \) is bounded above by \( e' + 1 \) where \( e' \) is the least such \( e \).

Proof. If \( H \) is subnormal then \( lR \subseteq kR \) and \( \Gamma_{n,k} \leq \Gamma_{n,r} \) for \( k, e \) as in Theorem 1.23 so \( k \mid l \) and \( r \mid k^e \). Conversely, if \( r \mid l^e \) then \( H \) satisfies (7) with \( k = l \).

Lemma 1.25 ([37], p. 165). \( Z_{n,t}/\Gamma_{n,t} \) is nilpotent of class at most \( e \).

We now consider normality.

Lemma 1.26. If \( \Gamma_{n,l} \leq H \leq Z_{n,l} \) then \( H \leq G_n \) and \( l = \ell(H) = \text{the level of the maximal PCS in } H \).

Proof. We first observe that \( l = \ell(\Gamma_{n,l}) \geq \ell(H) \geq \ell(Z_{n,l}) \). Let \( \Gamma_{n,r} \) be the maximal PCS in \( H \). Then \( r \mid l \) and \( r \mid l \) because \( \Gamma_{n,r} \leq Z_{n,l} \).

Lemma 1.27. Suppose that \( H \leq G_n \) has level \( l \). Then

(i) \( \Gamma_{n,l} \leq H^G_n \leq Z_{n,l} \).
(ii) \( H^G_n = \langle H, \Gamma_{n,l} \rangle \).

Proof. (i) The inclusion \( H^G_n \leq Z_{n,l} \) is clear. If \( h \in H \) has level \( a \) then \( t_{1,2}(a) \in \langle h \rangle^G_n \) by Theorems 1 and 4 of [5]. As a consequence, \( t_{1,2}(l) \in H^G_n \). Now this part is assured by Proposition 1.6 and Corollary 1.9.

(ii) Let \( L = \langle H, \Gamma_{n,l} \rangle \). Since \( L \leq G_n \) (Lemma 1.26), \( H^G_n \leq L \). Also \( L \leq H^G_n \) by (i).

Corollary 1.28. \( H \leq G_n \) if and only if \( \ell(H) \) is the level of the maximal PCS in \( H \).

Proposition 1.29. Lemma 1.27 remains true with \( G_n \) replaced by \( \Gamma_n = \text{SL}(n, R) \). That is, \( H_{\Gamma_n} = H^G_n \), and so \( H \leq \Gamma_n \) is normal in \( \Gamma_n \) precisely when it is normal in \( G_n \).

2. Matrix groups over \( \mathbb{Z}_m \)

2.1. Relevant theoretical results. Let \( m = p_1^{k_1} \cdots p_t^{k_t} \) where the \( p_i \) are distinct primes and \( k_i \geq 1 \). We define a ring isomorphism \( \chi : \mathbb{Z}_m \to \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{k_t}} \) by \( \chi(a) = (a_1, \ldots, a_t) \) where \( 0 \leq a \leq m - 1, 0 \leq a_i \leq p_i^{k_i} - 1 \), and \( a_i \equiv a \mod p_i^{k_i} \).

Lemma 2.1.

(i) \( \chi \) extends to an isomorphism of \( \text{Mat}(n, \mathbb{Z}_m) \) onto \( \oplus_{i=1}^t \text{Mat}(n, \mathbb{Z}_{p_i^{k_i}}) \), which restricts to isomorphisms \( \text{GL}(n, \mathbb{Z}_m) \to \times_{i=1}^t \text{GL}(n, \mathbb{Z}_{p_i^{k_i}}) \) and \( \text{SL}(n, \mathbb{Z}_m) \to \times_{i=1}^t \text{SL}(n, \mathbb{Z}_{p_i^{k_i}}) \).

(ii) Let \( I = \langle a \rangle \) be an ideal of \( \mathbb{Z}_m \), and let \( I_i \) be the ideal of \( \mathbb{Z}_{p_i^{k_i}} \), generated by \( a_i \equiv a \mod p_i^{k_i} \). Denote by \( K_I, K_{I_i} \) the kernels of \( \varphi_I, \varphi_{I_i} \) on \( \text{GL}(n, \mathbb{Z}_m), \text{GL}(n, \mathbb{Z}_{p_i^{k_i}}) \) respectively. Then

\[ \chi(K_I) = \times_{i=1}^t K_{I_i} \quad \text{and} \quad \chi(K_I \cap \text{SL}(n, \mathbb{Z}_m)) = \times_{i=1}^t (K_{I_i} \cap \text{SL}(n, \mathbb{Z}_m)) \]
For $i \geq 1$,
\[
M_{p,i} = \{ h \in \text{GL}(n, \mathbb{Z}_{p^k}) \mid h \equiv 1_n \mod p^i \}, \quad N_{p,i} = \text{SL}(n, \mathbb{Z}_{p^k}) \cap M_{p,i}
\]
are normal subgroups of $\text{GL}(n, \mathbb{Z}_{p^k})$.

Lemma 2.2 (Cf. Corollary [1.9]). If $I$ is the ideal of $\mathbb{Z}_{p^k}$ generated by $p^i$, then $\varphi_I : \text{GL}(n, \mathbb{Z}_{p^k}) \to \text{GL}(n, \mathbb{Z}_{p^i})$ and $\varphi_I : \text{SL}(n, \mathbb{Z}_{p^k}) \to \text{SL}(n, \mathbb{Z}_{p^i})$ are surjective, with kernels $M_{p,i}$, $N_{p,i}$ respectively.

The notation $M_{p,i}$, $N_{p,i}$ supersedes our earlier notation for principal congruence subgroups in this special case. Let $d_j(a) = n + ae_{j,j} \in \text{Mat}(n, \mathbb{Z}_m)$.

Lemma 2.3. Suppose that $i < j \leq 2i$ and $j \leq k$. Then $M_{p,i}/M_{p,j} \cong \mathbb{C}_p^{n^2}$ and $N_{p,i}/N_{p,j}$ has a subgroup isomorphic to $\mathbb{C}_p^{n^2-1}$.

Proof. Treating $\text{Mat}(n, \mathbb{Z}_{p^{i-1}})$ as an additive group, we confirm that $\theta_j : M_{p,i} \to \text{Mat}(n, \mathbb{Z}_{p^{i-1}})$ defined by $\theta_j(1_n + p^i x) = \varphi_{p^{i-1}}(x)$ is a homomorphism with kernel $M_{p,j}$. Now $t_{ri}(p^i) \in N_{p,i}$ and $d_i(p^i) \in M_{p,i}$, so $\theta_j$ is surjective. Since $N_{p,i}$ contains $1_n + p^i(e_{rr} - e_{r+1,r+1} + e_{r,r+1} - e_{r+1,r})$, the second assertion follows too.

Lemma 2.4. $[M_{p,i}, M_{p,j}] = [N_{p,i}, N_{p,j}] = N_{p,i+j}$.

Proof. (Cf. Lemma [1.25]) Let $a = 1_n + p^i x \in M_{p,i}$ and $b = 1_n + p^j y \in M_{p,j}$. For some $z$, and $x, y$ such that $a^{-1} = 1_n + p^i \bar{x}$ and $b^{-1} = 1_n + p^j \bar{y}$, we have
\[
[a, b] = (1_n + p^i x + p^j \bar{y} + p^{i+j} \bar{x} \bar{y})(1_n + p^j y + p^i \bar{x} \bar{y} + p^{i+j} x y) = 1_n + p^i(x + \bar{x}) + p^j(y + \bar{y}) + p^{i+j} x y + p^{i+j} z = 1_n + p^{i+j} z.
\]
Therefore $[M_{p,i}, M_{p,j}] \leq M_{p,i+j} \cap \text{SL}(n, \mathbb{Z}_{p^k}) = N_{p,i+j}$. Also $t_{21}(p^{i+j}) = [t_{25}(p^i), t_{31}(p^j)] \in [N_{p,i}, N_{p,j}] \leq \text{SL}(n, \mathbb{Z}_{p^k})$; thus $N_{p,i+j} \leq [N_{p,i}, N_{p,j}]$ by Corollary [1.9].

Lemma 2.5.

(i) $|M_{p,i}| = p^{n^2(k-i)}$.

(ii) $|\text{GL}(n, \mathbb{Z}_{p^k})| = |\text{GL}(n, p)| \cdot p^{n^2(k-1)}$.

Proof. Lemma 2.3 takes care of (i). By Lemma 2.2 we then get (ii).

Corollary 2.6. If $2i > k$ then $M_{p,i}$ is abelian of exponent $p^{k-i}$.

The next two corollaries use Lemma 2.1. Let $a = p_1^{j_1} \cdots p_t^{j_t}$ where $0 \leq j_i \leq k_i$. Note that $a_i \equiv a \mod p_i^{k_i}$ generates the ideal $(p_i^{j_i})$ of $\mathbb{Z}_{p_i^{k_i}}$. Set $M_{p_i,0} = \text{GL}(n, \mathbb{Z}_{p_i^{k_i}})$ and $N_{p_i,0} = \text{SL}(n, \mathbb{Z}_{p_i^{k_i}})$.

Corollary 2.7.

(i) $|\text{GL}(n, \mathbb{Z}_m)| = \prod_{i=1}^t \left( |\text{GL}(n, p_i)| \cdot p_i^{n^2(k_i-1)} \right)$.

(ii) The PCS of $\text{GL}(n, \mathbb{Z}_m)$ of level $a$ has order $\prod_{i=1}^t |M_{p_i, j_i}|$.

Lemma 2.8.

(i) $|\text{SL}(n, \mathbb{Z}_{p^k})| = |\text{SL}(n, p)| \cdot p^{(n^2-1)(k-1)}$.

(ii) For $i \geq 1$, $N_{p,i}/N_{p,i+1} \cong \mathbb{C}_p^{n^2-1}$ and $|N_{p,i}| = p^{(n^2-1)(k-i)}$.

Proof. The unit group of $\mathbb{Z}_{p^k}$ has order $(p-1)p^{k-1}$, so Lemma 2.5(ii) gives (i). By Lemma 2.3 $|N_{p,j}/N_{p,j+1}| \geq p^{n^2-1}$. Thus, if $|N_{p,j}/N_{p,j+1}| = p^{n^2-1}$ for some $j$ then $|N_{p,j}| > p^{(n^2-1)(k-1)}$, which contradicts (i) by Lemma 2.2.
Corollary 2.9.

(i) \(|\text{SL}(n, \mathbb{Z}_m)| = \prod_{i=1}^{t} (|\text{SL}(n, p_i)| \cdot p_i^{(n^2-1)(k_i-1)})\).

(ii) The PCS of \(\text{SL}(n, \mathbb{Z}_m)\) of level \(a\) has order \(\prod_{i=1}^{t} |N_{p_i,j_i}|\).

Define subsets

\[ S_c = \{t_{rs}(c), 1_n + c(e_uu + e_{u,u+1} - e_{u+1,u} - e_{u+1,u+1}) \mid r \neq s, 1 \leq r, s \leq n, 1 \leq u \leq n - 1\} \]

of \(\text{SL}(n, \mathbb{Z}_m)\) and

\[ T_c = \{t_{rs}(c), d_1(c), \ldots, d_n(c) \mid r \neq s, 1 \leq r, s \leq n\} \]

of \(\text{Mat}(n, \mathbb{Z}_m)\). We see that \(T_c \leq \text{GL}(n, \mathbb{Z}_m)\) if and only if \(1 + c\) is a unit of \(\mathbb{Z}_m\).

Lemma 2.10. Suppose that \(1 \leq i < k\).

(i) \(N_{p,i}\) has minimal size generating set \(S_{p,i}\), so \(\min(N_{p,i}) = n^2 - 1\).

(ii) Unless \(p = 2, k \geq 3\), and \(i = 1\), \(\min(M_{p,i}) = n^2\) and \(M_{p,i}\) has minimal size generating set \(T_{p,i}\).

(iii) \(M_{2,1}\) for \(k \geq 3\) has minimal size generating set \(T_2 \cup \{\text{diag}(-1, 1, \ldots, 1)\}\) of size \(n^2 + 1\).

Proof. In the proof of Lemma 2.3 we saw that \(N_{p,i} = \langle S_{p,i}, N_{p,2i} \rangle\). Since \(N_{p,i}\) is nilpotent with derived group \(N_{p,2i}\) by Lemma 2.4, we have \(N_{p,i} = \langle S_{p,i} \rangle\). So \(\min(N_{p,i}) = \min(N_{p,i}/N_{p,i+1}) = n^2 - 1\) by Lemma 2.3(ii).

The rest of the proof is along similar lines. Note that \(M_{p,i} = \langle T_{p,i}, M_{p,2i} \rangle\), and \(M_{p,2i}/N_{p,2i}\) is trivial when \(2i \geq k\), or cyclic of order \(p^{k-2i}\) generated by the coset of \(d_1(p^{2i})\) otherwise. Also \(1 + p^{2i} \in \langle 1 + p^i \rangle \leq \mathbb{Z}_p^{2i}\) unless \(p = 2, k \geq 3,\) and \(i = 1\); whereas \(5 \in \langle -1, 3 \rangle = \mathbb{Z}_p^2\) for \(k \geq 3\).

Therefore \(M_{p,i} = \langle T_{p,i}, N_{p,2i} \rangle = \langle T_{p,i} \rangle\) in (ii). Since \(|T_{p,i}| = n^2\) and \(M_{p,i}/M_{p,i+1}\) has rank \(n^2\), this proves (ii). The verification of (iii) is left as an exercise. \(\square\)

Proposition 2.11. Let \(H, K\) be non-trivial principal congruence subgroups of level \(a = p_1^{j_1} \cdots p_t^{j_t} \neq m\) in \(\text{GL}(n, \mathbb{Z}_m), \text{SL}(n, \mathbb{Z}_m)\) respectively, where \(1 \leq j_i \leq k_i\) for all \(i\). Then

(i) \(\min(H) = n^2\); unless \(k_2 \geq 3\) and the Sylow 2-subgroup of \(\chi(H)\) is \(M_{2,1}\), in which case \(\min(H) = n^2 + 1\).

(ii) \(\min(K) = n^2 - 1\).

Proof. If \(X, Y\) are groups of coprime order with generating sets \(\{x_1, \ldots, x_r\} \subseteq X\) and \(\{y_1, \ldots, y_r\} \subseteq Y\) of minimal size, where \(r_1 \leq r_2\), then \(\min(X \times Y) = r_2\). Indeed

\[ X \times Y = \langle (x_i, y_i), (1, y_j) : 1 \leq i \leq r_1; r_1 + 1 \leq j \leq r_2 \rangle. \]

The result follows from Lemmas 2.1(ii) and 2.10. \(\square\)

Remark 2.12.

(i) If \(j_i = 0\) for any \(i\) then a full \(\text{GL}(4\text{-generated})\) or \(\text{SL}(2\text{-generated})\) appears as a factor in \(H\) or \(K\).

(ii) The proof of Proposition 2.11 shows how to construct minimal size generating sets for \(H\) and \(K\) with the aid of Lemma 2.10. Note that we get a generating set for a PCS \(\text{SL}(n, \mathbb{Z}_m)\) by \(\text{GL}(n, \mathbb{Z}_m)\) modulo \(p\) in Proposition 1.10.

2.2. Computing in \(\text{GL}(n, \mathbb{Z}_m)\). As above, suppose that \(m \geq 2\) has prime factorization \(\prod_{i=1}^{t} p_i^{k_i}\). Let \(\chi\) be the isomorphism introduced just before Lemma 2.1. We identify \(H \leq \text{GL}(n, \mathbb{Z}_m)\) with \(\chi(H)\).

To compute with \(H\), we use composition tree methods and the data structure from [20]. The latter consists of an effective homomorphism into \(\times_{i=1}^{t} \text{GL}(n, p_i)\) whose kernel \(K\) is the solvable radical of \(H\), and a polycyclic generating sequence (PCGS) for \(K\). Data structures for the images of the
projections of $H$ modulo $p_i^{k_i}$ can be combined into a data structure for $H$. We therefore assume that $m = p^k$.

Clearly $H/K$ is isomorphic to a quotient of $\varphi_p(H) \leq \mathrm{GL}(n, p)$, and a PCGS for $\varphi_p(H)$ gives the initial terms of a PCGS for $K$; the rest are found by reductions modulo $p^e$ (cf. Subsection 2.1). As we have seen, if $M$ is the kernel of reduction modulo $p^e$ and $N$ the kernel of reduction modulo $p^{e+1}$, then $M/N$ is described by matrices $1 + p^e x$ for $x \in \mathrm{Mat}(n, p)$, which multiply by addition of their $x$-parts. A PCGS for the elementary abelian group $M/N$ can be determined easily by linear algebra.

2.3. Subnormal structure. Let $n \geq 3$. We adhere to previous notation and conventions.

Let $\ell$ be a function that returns $\ell(H)$ for a subgroup $H = \langle S \rangle$ of $G_n = \mathrm{GL}(n, \mathbb{Z}_m)$; see Lemma 1.22.

\texttt{MaxPCS}(H)

Input: $H \leq G_n$.

Output: a generating set for a maximal PCS of $\Gamma_n = \mathrm{SL}(n, \mathbb{Z}_m)$ in $H$.

1. $l := \ell(H)$.
2. If $l = 0$ then return $1_n$,
   then return a generating set $L$ for the PCS of level $a$ in $\Gamma_n$ as given by Proposition 2.11, where $a$ is minimal subject to $a$ dividing $m$, $l$ dividing $a$, and $L \subseteq H$.

Step (2) requires membership testing. As an application of \texttt{MaxPCS}, we have

\texttt{IsSpecialLinear}(H)

Input: $H \leq \Gamma_n$.

Output: true if $H = \Gamma_n$; false otherwise.

If $\ell(\text{MaxPCS}(H)) = 1$ then return true
else return false.

The following reiterates Theorem 1.24.

\texttt{IsSubnormal}(H)

Input: $H \leq G_n$.

Output: true and an upper bound $d$ on the defect of $H$ if $H \trianglerighteq G_n$; false otherwise.

1. $l_1 := \ell(H), l_2 := \ell(\text{MaxPCS}(H))$.
2. If $\nmid l_2|l_1$ then return false,
   then return true and $d := e' + 1$ where $e' :=$ the least $e$ such that $l_2|l_1$.

\textit{Remark} 2.13. Let $H \leq \Gamma_n$. Obviously $H \trianglerighteq \Gamma_n$ if and only if $H \trianglerighteq G_n$. The defect of $H$ as a subnormal subgroup of $\Gamma_n$ is either equal to or one less than its defect as a subgroup of $G_n$.

\texttt{NormalClosure}(H) returns the normal closure of $H$ in $G_n$ according to Lemma 1.27. \texttt{IsNormal} tests whether $H \trianglelefteq G_n$, returning true if and only if $l_2 = l_1$ (Corollary 1.28).

By Proposition 1.29, \texttt{NormalClosure} also returns the normal closure in $\Gamma_n$ of $H \leq \Gamma_n$, and \texttt{IsNormal} tests whether $H \trianglelefteq \Gamma_n$.

We can list the subnormal subgroups of $G_n$ in $H$.

\texttt{NormalSubgroups}(H, l)

Input: $H \leq G_n$ and a positive integer $l$.

Output: all normal subgroups of $G_n$ in $H$ of level $l$. 

Proposition 1.10. Given a finite generating set.

Let \( L \) := a list of all subgroups of \( \varphi_I(H) \cap \varphi_I(\mathbb{Z}_{n,l}) \).

(3) Return the full preimage of \( L \) in \( H \) under \( \varphi_I \).

We sketch a more general method. Let \( \mathcal{L}_{a,b} \) be the list of all \( K \) such that \( \Gamma_{n,b} \leq K \leq H \cap \mathbb{Z}_{n,a} \).

(1) \( r := \text{Level}(\text{MaxPCS}(H)) \).

(2) If \( r \) does not divide \( l \) then return \( \emptyset \).

(3) \( \mathcal{L} := \) a list of all subgroups of \( \varphi_I(H) \cap \varphi_I(\mathbb{Z}_{n,l}) \).

(4) Return the full preimage of \( \mathcal{L} \) in \( H \) under \( \varphi_I \).

3. Computing with arithmetic groups in \( \text{SL}(n, \mathbb{Z}) \)

3.1 Decidability. An arithmetic subgroup \( H \) of an algebraic \( \mathbb{Q} \)-group \( G \leq \text{GL}(n, \mathbb{C}) \) is ‘explicitly given’ if (i) an upper bound on \( |G_Z : H| \) is known, and (ii) membership testing in \( H \) is possible; i.e., for any \( g \in G_Z \) it can be decided whether \( g \in H \) \cite[pp. 531–532]{17}. Conditions (i) and (ii) were assumed in \cite{17} to prove decidability of algorithmic problems for \( H \). As the next lemma shows, these conditions are equivalent to knowing a PCS in \( H \). Such a PCS can always be found: see Corollary 1.15.

Lemma 3.1. Let \( H \leq \Gamma_n \). The following are equivalent.

(i) A positive integer \( m \) such that \( \Gamma_{n,m} \leq H \) is known.

(ii) An upper bound on \( |\Gamma_n : H| \) is known, and testing membership of \( x \in \Gamma_n \) in \( H \) is decidable.

Proof. (i) \( \Rightarrow \) (ii). \( |\Gamma_n : H| \leq |\text{SL}(n, \mathbb{Z}_m)| \), and \( x \in H \) if and only if \( \varphi_m(x) \in \varphi_m(H) \).

(ii) \( \Rightarrow \) (i). Suppose that \( |\Gamma_n : H| \leq r \). For \( g \in \Sigma \) as in Proposition 1.10 and each pair \( i, j \), after no more than \( r \) rounds we are guaranteed to find positive integers \( r_{g,i,j} \leq r \) such that \( t_{ij}(r_{g,i,j})^y = (t_{ij}^y)^{g,i,j} \in H \). Thus, if \( m \) is any common multiple of the \( r_{g,i,j} \) then \( \Gamma_{n,m} \leq H \).

Proposition 3.2. If \( H \) is a finite index subgroup of \( \Gamma_n \) specified by a finite generating set then testing membership of any \( g \in \Gamma_n \) in \( H \) is decidable.

Proof. This follows from Corollary 1.15 and Lemma 3.1.

Of course, a key problem is (AT), arithmeticity testing: if \( H \) is a finitely generated subgroup of \( \Gamma_n \), determine whether \( |\Gamma_n : H| \) is finite. We are unaware of any proof that (AT) is decidable—although it seems not to be \cite{28}. Nonetheless, (AT) is decidable when \( G \) is solvable \cite{7}.

3.2 Algorithms for arithmetic groups. Now we design algorithms for \( H \leq \Gamma_n = \text{SL}(n, \mathbb{Z}), n \geq 3 \), given by a finite generating set.

By Corollary 1.15 (and the proof of Lemma 1.13), we have a procedure \( \text{LevelPCS}(H) \) that returns the level of a PCS in \( H \). It depends on representing elements of \( \Gamma_n \) as products of transvections. Once we know \( \text{LevelPCS}(H) = m \), say, then \( \text{GeneratorsPCS}(m) \) returns a generating set for \( \Gamma_{n,m} \) as in Proposition 1.10.

Let \( \overline{H} = \varphi_m(H) \leq \overline{\Gamma}_n = \text{SL}(n, \mathbb{Z}_m) \). Lemma 1.21 underpins the following, which finds the maximal PCS \( \Gamma_{n,r} \) in \( H \). (To improve efficiency we could substitute \( r \) for \( m \) in algorithms of this section.)

\[ \text{MaxPCS}(H, m) \]

Input: \( H \leq \Gamma_n \) such that \( \Gamma_{n,m} \leq H \).

Output: a generating set for the maximal PCS in \( H \).

(1) \( r := \text{Level}(\text{MaxPCS}(\overline{H})) \).

(2) Return \( \text{GeneratorsPCS}(r) \).
4. THE ORBIT-STABILIZER PROBLEM

Let $R$ be a commutative ring with 1, and let $H = \langle S \rangle \leq \text{GL}(n,R)$. This section addresses the orbit-stabilizer problem: for arbitrary $u, v \in R^n$,

1. decide whether there is $g \in H$ such that $gu = v$, and find a $g$ if it exists;
2. determine $\text{Stab}_H(u) = \{g \in H \mid gu = u\}$.

The element $g$ and a generating set for $\text{Stab}_H(u)$ should be written as words over $S \cup S^{-1}$. We solve (I) and (II) for $R = \mathbb{Q}$ and $H \leq \Gamma_n = \text{SL}(n,\mathbb{Z})$. Along the way, partial results for subgroups of $\Gamma_n = \text{SL}(n,\mathbb{Z}_m)$ are proved as well.

4.1. Preliminaries. Suppose that $\Gamma_{n,m} \leq H \leq \Gamma_n$. We denote images under $\varphi_m$ by overlining.

**Lemma 4.1.** Let $u, v \in \mathbb{Z}^n$, and let $K$ be the full preimage of $\text{Stab}_{\overline{\Gamma}}(\overline{u})$ in $H$. Then

1. $v \in H u$ if and only if $\overline{v} \in \overline{\Gamma} \overline{u}$ and $h v \in K u$ for any $h \in H$ such that $\overline{h} \overline{v} = \overline{u}$.
2. $\text{Stab}_H(u) = \text{Stab}_K(u)$.

**Proposition 4.2.** If we can solve the orbit-stabilizer problem for $\Gamma_{n,m}$ (acting on $\mathbb{Z}^n$), then we can solve it for $H$.

**Proof.** (Cf. [14, p. 255] and [15, Lemma 3.1].) First, note that $K$ permutes the $\Gamma_{n,m}$-orbits in $\mathbb{Z}^n$. Let $\{y_1, \ldots, y_k\}$ be a set of representatives for the $K$-orbit of $\Gamma_{n,m} u$. In the notation of **Lemma 4.1**

$$v \in H u \iff hv \in K u \iff hv, y_i u \text{ are in the same } \Gamma_{n,m} \text{-orbit for some } i.$$

Secondly, we can find (Schreier) generators $h_1, \ldots, h_s$ of $\text{Stab}_K(\Gamma_{n,m} u)$; and find $g_i \in \Gamma_{n,m}$ such that $g_i u = h_i u$, $1 \leq i \leq s$. Then

$$\text{Stab}_H(u) = \text{Stab}_K(u) = \langle g_1^{-1} h_1, \ldots, g_s^{-1} h_s, \text{Stab}_\Gamma(u) \rangle.$$
As suggested by Proposition 4.2 we first aim to solve the orbit-stabilizer problem for a PCS in $\Gamma_n$.

Let $u = (u_1, \ldots, u_n)^\top \in R^n$, and let $\langle u \rangle$ denote the ideal of $R$ generated by the $u_i$.

Lemma 4.3. $\langle xu \rangle = \langle u \rangle$ for any $x \in \text{GL}(n, R)$; thus, if $u$ and $v$ are in the same $\text{GL}(n, R)$-orbit then $\langle u \rangle = \langle v \rangle$.

A vector $u \in R^n$ such that $\langle u \rangle = R$ is said to be unimodular. By Lemma 4.3 $\text{GL}(n, R)$ permutes the unimodular vectors among themselves.

4.2. $\Gamma_n$-orbits in $\mathbb{Z}_m^n$. Suppose that $m$ has prime factorization $\prod p_i^{e_i}$, and write each $a \in \mathbb{Z}_m$ as $(a_1, \ldots, a_s), a_i \in \mathbb{Z}_{p_i^{e_i}}$.

Lemma 4.4. If $(u_1, \ldots, u_n)^\top \in \mathbb{Z}_m^n$ is unimodular then $u_1 + \sum_{i=2}^n b_i u_i$ is a unit of $\mathbb{Z}_m$ for some $b_2, \ldots, b_n \in \mathbb{Z}_m$.

Lemma 4.4 is proved in [21, p. 104]. We summarize the proof as follows.

Auxiliary1 ($u$)

Input: unimodular $u = (u_1, \ldots, u_n)^\top \in \mathbb{Z}_m^n$.

Output: $b_2, \ldots, b_n$ as in Lemma 4.4

(1) For $j = 1, \ldots, s$ do

let $k$ be the least index such that $p_j^{e_j} u_{kj} \not\equiv 0 \text{ mod } p_j^{e_j}$;

let $b_{kj} := 1$ and $b_{kj} := 0$ for $i \neq k$.

(2) Return $b_2 := (b_{21}, b_{22}, \ldots, b_{2s}), \ldots, b_n := (b_{n1}, b_{n2}, \ldots, b_{ns})$.

Lemma 4.5. If $u \in \mathbb{Z}_m^n$ is unimodular then $g u = (1, 0, \ldots, 0)^\top$ for some $g \in \Gamma_n$.

Proof. By Lemma 4.4

$$t_{12}(b_2) \cdots t_{1n}(b_n) u = (v_1, u_2, \ldots, u_n)^\top$$

where $v_1 = u_1 + \sum_{i=2}^n b_i u_i$ is a unit of $\mathbb{Z}_m$. Further,

$$t_{n1}(-v_1^{-1} u_n) \cdots t_{21}(-v_1^{-1} u_2)(v_1, u_2, \ldots, u_n)^\top = (v_1, 0, \ldots, 0)^\top.$$ 

Finally,

$$t_{21}(-1) t_{12}(1-v_1) t_{21}(v_1^{-1})(v_1, 0, \ldots, 0)^\top = (1, 0, \ldots, 0)^\top. \hfill \Box$$

Corollary 4.6. The set of all unimodular vectors is a $\Gamma_n$-orbit in $\mathbb{Z}_m^n$.

Proposition 4.7. Non-zero vectors $u, v \in \mathbb{Z}_m^n$ are in the same $\Gamma_n$-orbit if and only if $\langle u \rangle = \langle v \rangle$.

Proof. Suppose that $\langle u \rangle = \langle v \rangle$; so $u = a \tilde{u}$ and $v = a \tilde{v}$ for some $a$ dividing $m$, $1 \leq a < m$, and unimodular $\tilde{u}, \tilde{v}$. Now the result is apparent by Lemma 4.3 and Corollary 4.6.

Corollary 4.8. The map defined by $\Gamma_n u \mapsto \langle u \rangle$ is a bijection between the set of $\Gamma_n$-orbits in $\mathbb{Z}_m^n$ and the set of ideals of $\mathbb{Z}_m$.

4.3. Orbits in $\mathbb{Z}_m^n$.

4.3.1. $\Gamma_n$-orbits.

Lemma 4.9. Let $u = (u_1, \ldots, u_n)^\top \in \mathbb{Z}_m^n \setminus \{0\}$ and let $d$ be the gcd of the non-zero entries of $u$. Then $t u = (d, 0, \ldots, 0)^\top$ for some $t \in \Gamma_n$. 

Proof. (Cf. [34, Lemma 3, pp. 72–73].) Say the non-zero entries of \( u \) are \( u_{j_1}, \ldots, u_{j_l} \) where \( j_1 < \cdots < j_l \). If \( u_i = 0 \) then
\[
 t_{ji}(-1)t_{ij}(1)u = (u_1, \ldots, u_{i-1}, u_{j_1}, u_{j_1+1}, \ldots, u_{j_l-1}, 0, u_{j_l+1}, \ldots, u_n)^\top.
\]
So the lemma holds for \( l = 1 \), and we may assume that \( j_l = i \) and \( l \geq 2 \).

Formally, the proof is by induction on \( l \). We manufacture \( t \) by applying the Euclidean algorithm repeatedly to pairs of adjacent nonzero entries of \( u \). To begin, put \( r_0 = u_{l-1}, r_1 = u_l \); then for \( i \geq 0 \) and while \( r_{i+1} \neq 0 \), let \( q_i+1, r_{i+2} \) be the integers such that \( r_i = r_{i+1}q_i+1 + r_{i+2} \) and \( 0 \leq r_{i+2} < |r_{i+1}| \). If \( r_k \) is the last non-zero remainder then
\[
 t^*u = (u_1, \ldots, u_{l-2}, r_k, 0, 0, \ldots, 0)^\top
\]
where
\[
 t^* = \begin{cases} 
 t_{i,l-1}(-1)t_{i-1,l}(1)t_{l-1,i}(-q_k)\cdots t_{i,l-1}(-q_2)t_{l-1,i}(-q_1) & \text{if } k \text{ odd,} \\
 t_{i,l-1}(-q_k)\cdots t_{i,l-1}(-q_2)t_{l-1,i}(-q_1) & \text{if } k \text{ even.}
\end{cases}
\]
At the next stage we put \( r_0 = u_{l-2}, r_1 = r_k \), and repeat the above. Continuing in this fashion ultimately gives \( t \) as desired. \( \square \)

**Proposition 4.10** (cf. [34, Corollary 1, p. 73].) Vectors \( u, v \in \mathbb{Z}^n \) belong to the same \( \Gamma_n \)-orbit if and only if \( \langle u \rangle = \langle v \rangle \).

Proof. In the notation of Lemma 4.9 \( \langle u \rangle = d\mathbb{Z} \). \( \square \)

**Corollary 4.11.** There is a one-to-one correspondence between the set of \( \Gamma_n \)-orbits in \( \mathbb{Z}^n \) and the set of ideals of \( \mathbb{Z} \).

\( \text{OrbitGamma} \) accepts \( u \in \mathbb{Z}^n \setminus \{0\} \) and (as per the proof of Lemma 4.9) returns a pair \( (d, t) \) where \( t \in \Gamma_n, d \) is the gcd of all non-zero entries of \( u \), and \( tu = (d, 0, \ldots, 0)^\top \).

By Proposition 4.10, the next procedure solves the orbit problem for \( \Gamma_n \) acting on \( \mathbb{Z}^n \).

\[ \text{OrbitGamma}(u, v) \]
Input: \( u, v \in \mathbb{Z}^n \setminus \{0\} \).
Output: \( g \in \Gamma_n \) such that \( gu = v \), or false if \( u, v \) are not in the same \( \Gamma_n \)-orbit.

1. \((d_1, t_1) := \text{OrbitGamma}(u), \)
\((d_2, t_2) := \text{OrbitGamma}(v). \)
2. If \( d_1 \neq d_2 \) then return false,
   else return \( t_2^{-1}t_1 \).

4.3.2. \( \Gamma_{n,m} \)-orbits.

**Lemma 4.12** ([21, Lemma 2, p. 105].) Let \( u, v \in \mathbb{Z}^n \). Suppose that there is a non-empty subset \( I \subseteq \{1, \ldots, n\} \) such that \( u_i = v_i \) for \( i \in I \) and \( u_i \equiv v_i \mod m' \) for \( i \not\in I \), where \( m'\mathbb{Z} = \langle u_j : j \in I \rangle \). Then \( u, v \) are in the same \( \Gamma_{n,m} \)-orbit.

We outline the proof of Lemma 4.12 in the form of an algorithm.

\[ \text{Auxiliary2}(u, v, I) \]
Input: \( u, v \in \mathbb{Z}^n, I \) as in Lemma 4.12
Output: \( g \in \Gamma_{n,m} \) such that \( gu = v \).

1. For each \( i \in I \) and \( j \in \{1, \ldots, n\} \setminus I \), find \( c_{ji} \in \mathbb{Z} \) such that \( v_j = u_j + m\sum_{i \in I} c_{ji}u_i \).
2. Return \( g := \prod_{i \in I, j \not\in I} t_{ji}(mc_{ji}) \).
Theorem 4.13. Let $u, v \in \mathbb{Z}^n \setminus \{0\}$ where $\langle u \rangle = a\mathbb{Z}$. Then $u$ and $v$ are in the same $\Gamma_{n,m}$-orbit if and only if $\langle u \rangle = \langle v \rangle$ and $u_i \equiv v_i \mod{am}$, $1 \leq i \leq n$.

Proof. See the theorem on p. 101 of [21] for $n > 2$. Suppose that $n = 2$, $\langle u \rangle = \langle v \rangle$, and $u_i \equiv v_i \mod{am}$. Then $tu = (a, 0)^T$ and $tv = (a(1 + mr, ms))^T$ for some $t \in \Gamma_2$ and $r, s \in \mathbb{Z}$ such that $\langle 1 + mr, ms \rangle = \mathbb{Z}$, say $x(1 + mr) + yms = 1$. Consequently $h^t u = v$ where

$$h = \begin{pmatrix} 1 - mrx & -mry \\ -ms & 1 + mr \end{pmatrix}. \quad \square$$

The procedure below incorporates the method for $n > 2$ in [21] pp. 105–106. Lines beginning ‘#’ contain explanatory comments.

OrbitGamma(u, v)

Input: $u, v \in \mathbb{Z}^n$, $n \geq 2$.
Output: $g \in \Gamma_{n,m}$ such that $gu = v$, or false if $u, v$ are not in the same $\Gamma_{n,m}$-orbit.

1. If OrbitGamma(u, v) = false then return false.
2. If $u_i \not\equiv v_i \mod{am}$ for some $i$, where $(a, t) := \text{Orbit1Gamma}(v)$, then return false, else $u := \frac{1}{a}tu$.

# $u$ is now unimodular, $u_1 \equiv 1 \mod{m}$, and $u_i \equiv 0 \mod{m}$ for $i > 1$.

3. Apply Auxiliary1 to find $b_3, \ldots, b_n \in \mathbb{Z}$ such that $c := u_2 + r \sum_{i=3}^{n} b_i u_i$ is coprime to $u_1$, where $u_1 = 1 - r$, $r \in m\mathbb{Z}$.

# $u$ unimodular $\implies (u_2, ru_3, \ldots, ru_n)^T$ unimodular mod $u_1$.

4. If $n \geq 3$ then

\begin{align*}
& s_1 := \text{Auxiliary2}(u, (u_1, c, u_3, \ldots, u_n)^T, \{3, \ldots, n\}), \\
& \# s_1, (u_1, c, u_3, \ldots, u_n)^T, \text{and } I = \{3, \ldots, n\} \text{ satisfy the hypotheses of Lemma 4.12} \\
& s_2 := \text{Auxiliary2}((u_1, c, u_3, u_4, \ldots, u_n)^T, (u_1, c, r, 0, \ldots, 0)^T, \{1, 2\}). \\
& \# \text{ Lemma 4.12 again, with } m' = \gcd(u_1, c) = 1.
\end{align*}

5. If $n = 2$ then $s := h$ as in the proof of Theorem 4.13.

else $s := s_3s_2s_1$ where $s_3 := t_{13}(-1)t_{31}(-r)t_{21}(-c)t_{13}(1)$.

# $s_3 \in \Gamma_{n,m}$ because $\Gamma_{n,m} \leq \Gamma_n$.

6. Return $g := s^t$.

# $s^t \in \Gamma_{n,m}$ and $s^t \frac{1}{a}tu = (1, 0, \ldots, 0)^T = t_{a}^{-1}v$ for the original input $u, v$.

4.4. Stabilizers in $\Gamma_n$ and $\Gamma_{n,m}$. Suppose that $\Gamma_{n,m} \leq H \leq \Gamma_n$ and $u \in \mathbb{Z}^n \setminus \{0\}$. As an arithmetic subgroup of an algebraic group, $\text{Stab}_H(u)$ is finitely generated [18, p. 744]. Indeed, $\text{Stab}_{\Gamma_n}(u) = \Lambda^t_n$ where $\text{Orbit1Gamma}(u) = (d, t)$ and $\Lambda^t_n$ is the affine group

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}. $$
Hence \( \text{Stab}_{\Gamma_n}(u) \) is generated by \( t_{12}(1)^t, \ldots, t_{1n}(1)^t, \text{diag}(1, x)^t, \) and \( \text{diag}(1, y)^t \), where \( x, y \) are the generators of \( \Gamma_{n-1} \) given in Subsection 1.2. Next,

\[
\text{Stab}_{\Gamma_n}(u) = \text{Stab}_{\Gamma_n}(u) \cap \Gamma_{n,m} = (\Lambda_n \cap \Gamma_{n,m})^t.
\]

Plainly \( \Lambda_n \cap \Gamma_{n,m} \) is generated by \( \text{diag}(1, x) \) as \( x \) ranges over a generating set of \( \Gamma_{n-1,m} \) (for which see Proposition 1.10), together with \( t_{12}(m), \ldots, t_{1n}(m) \). We denote by \( \text{Stab}_{\Gamma_n} \) the procedure that returns the set of \( t \)-conjugates of these matrices for input \( u \).

4.5. Solution of the orbit-stabilizer problem for arithmetic groups. With Proposition 4.2 and its proof in mind, we now describe the main algorithms of this section.

As \( \Gamma_{n,m} \triangleleft H \), the orbits of \( \Gamma_{n,m} \) form a block system for \( H \). All vectors in a block have the same reduction modulo \( m \) (but vectors with equal reduction may not be in the same block). We first check for equivalence of vectors under the action by \( \overline{H} = \varphi_m(H) \), and compute generators for stabilizers in \( \overline{H} \). Then we represent each \( \Gamma_{n,m} \)-orbit by a vector in \( \mathbb{Z}^n \) and use \( \text{Orbit}_{\Gamma_{n,m}} \) to test orbit equality. We shall write \( u \) for \( \Gamma_{n,m}u \); that is, \( u = v \) if and only if \( \text{Orbit}_{\Gamma_{n,m}}(u, v) \) is not false.

To determine stabilizers (and thereby eliminate surplus generators) in \( H \) we calculate the induced action of \( \overline{H} \) and then take preimages.

If \( h \in H \) stabilizes \( u \) then we put \( g_h = \text{Orbit}_{\Gamma_{n,m}}(u, hu) \). Hence \( \text{Stab}_H(u) \) is generated by \( \text{Stab}_{\Gamma_n}(u) \) together with the corrected elements \( g_h^{-1}h \).

We state the algorithms below.

\[
\text{Orbit}(u, v, S)
\]

Input: \( u, v \in \mathbb{Z}^n \setminus \{0\} \) and \( S \subseteq \Gamma_n \) such that \( \Gamma_{n,m} \leq H = \langle S \rangle \).

Output: \( h \in H \) such that \( hu = v \), if \( v \in Hw \); false otherwise.

1. Determine \( \text{Stab}_{\overline{H}}(\overline{\pi}) \) and \( \overline{H}_{\pi} \).
   If \( \overline{\pi} \not\in \overline{H}_{\pi} \) then return false,
   else select \( \overline{h_1} \in \overline{H} \) such that \( \overline{h_1}v = \overline{\pi} \) and replace \( v \) by \( \overline{h_1}v \).

2. Determine the \( K \)-orbit of \( \overline{\pi} \), where \( K \) is the full preimage of \( \text{Stab}_{\overline{H}}(\overline{\pi}) \) in \( H \).
   If \( \overline{\pi} \not\in K_{\pi} \) then return false,
   else select \( h_2 \in K \) such that \( h_2v = \overline{\pi} \) and replace \( v \) by \( h_2v \).

3. \( g := \text{Orbit}_{\Gamma_{n,m}}(u, v) \).

4. Return \( h_1^{-1}h_2^{-1}g \).

\[
\text{Stabilizer}(u, S)
\]

Input: \( u \in \mathbb{Z}^n \setminus \{0\} \) and \( S \subseteq \Gamma_n \) such that \( \Gamma_{n,m} \leq H = \langle S \rangle \).

Output: a generating set for \( \text{Stab}_H(u) \).

1. \( K := \) the full preimage of \( \text{Stab}_{\overline{H}}(\overline{\pi}) \) in \( H \).
2. \( L := \text{Stab}_K(u) \).
3. \( g_h := \text{Orbit}_{\Gamma_{n,m}}(u, hu) \) for each generator \( h \) of \( L \),
   \( A := \{ g_h^{-1}h \mid h \text{ a generator of } L \} \).
4. Return \( A \cup \text{Stab}_{\Gamma_{n,m}}(u) \).

4.6. Remarks on and refinements of the algorithms. The stabilizer calculations for \( \overline{\pi} \) and \( \overline{\pi} \) are done in \( \overline{H} \) via the data structure of Subsection 2.2. We use the solvable radical of \( \overline{H} \) to deal with orbits, as in [20]. Typically the main obstacle is that \( \overline{H}_{\pi} \) can be very long. To ameliorate this we take orbits of \( \varphi_r(u) \) for an increasing sequence of divisors \( r \) of \( m \).

A further refinement (as with any linear action) is given by the imprimitivity system arising from the relation of vectors being unit multiples of each other. Here \( \overline{H} \) acts on blocks projectively; i.e., as \( \overline{H} \mathbb{Z} / \mathbb{Z} \) where \( Z = \mathbb{Z}(\text{SL}(n, \mathbb{Z}_r)) = \{ a1_n \mid a \in \mathbb{Z}_r^* \} \). We implement this action by representing each
block by a normalized vector. For prime \( r \), this means scaling the vector so that its first nonzero entry is 1. If the original entry has a common divisor with \( r \) greater than 1, then a minimal associate will be different from 1 and will usually have a nontrivial stabilizer. This stabilizer is then used to minimize entries in subsequent positions.

4.7. Preimages under \( \varphi_m \). A basic operation when utilizing congruence homomorphisms is to find preimages: for \( b \in \Gamma_n \) find \( c \in \Gamma_n \) such that \( \varphi_m(c) = b \) (any preimage will do because \( \Gamma_{n,m} \leq H \)). We cannot simply treat \( b \) as an integer matrix; it need not have determinant 1 over \( \mathbb{Z} \).

Matrix group recognition \[11\] maintains a history of how each element of \( \overline{\Gamma} \) was obtained as a word in congruence images of generators of \( H \). Long product expressions tend to build up when constructing a composition tree for \( \overline{\Gamma} \) using pseudo-random products. Evaluating these expressions back in characteristic 0 leads to large matrix entries.

We could write \( b \) as a product of transvections in \( \Gamma_n \) and then form the same product over \( \mathbb{Z} \). Similarly, suppose that \( c \) has Smith Normal Form \( c_{L,C}D_{R} \) where \( c_L, c_R \in \Gamma_n \) and \( c_{L,R} = 1_n \). Thus \( c_{L,R} = \overline{\tau} = b \) and \( c_{L,R} \) is a suitable preimage. Still, these approaches sometimes produced larger matrix entries than in the following heuristic.

Let \( x \) be the transposed adjugate \( \det(c) \left(c^{-1}\right)^\top \). Adding 1 to \( c_{ij} \) for \( i \neq j \) adds \( x_{ij} \) to \( \det(c) \). If \( \det(c) \neq 1 \) and \( \det(c) + amx_{ij} \) is positive of smaller absolute value, then add \( am \) to \( c_{ij} \). Repeat with updated \( x \). If no such \( x_{ij} \) exists (all entries of \( x \) are larger in absolute value than \( \det(c) \)), then we can try to use instead the gcd of two entries of \( x \) in the same row or column. Eventually \( \det(c) = 1 \), or we must resort to the other methods.

5. Generalizing to any arithmetic group in \( \text{SL}(n, \mathbb{Q}) \)

Let \( H \leq \text{SL}(n, \mathbb{Q}) \) be arithmetic. We explain how to compute \( g \in \text{GL}(n, \mathbb{Q}) \) such that \( H^g \leq \Gamma_n \). Our algorithms may therefore be modified to accept any arithmetic group in \( \text{SL}(n, \mathbb{Q}) \); i.e., not necessarily given by a generating set of integer matrices.

Lemma 5.1. The following are equivalent, for a finitely generated subgroup \( H \) of \( \text{GL}(n, \mathbb{Q}) \).

- \( H \) has finite index in \( \Gamma_n \).
- \( H \) is \( \text{GL}(n, \mathbb{Q}) \)-conjugate to a subgroup of \( \text{GL}(n, \mathbb{Z}) \).
- There exists a positive integer \( d \) such that \( dH \subseteq \text{Mat}(n, \mathbb{Z}) \).
- \( \text{tr}(H) = \{ \text{tr}(h) \mid h \in H \} \subseteq \mathbb{Z} \).

Proof. See \[7\] Section 3 and \[2\] Theorem 2.4. \( \square \)

An integer \( d = d(H) \) as in Lemma 5.1 is a common denominator for \( H \). Suppose that \( H = \langle S \rangle \leq \text{SL}(n, \mathbb{Q}) \) is arithmetic. Hence \( d \) exists. Let \( A = \{ a_1, \ldots, a_{n^2} \} \subseteq H \) be a basis of the enveloping algebra \( \langle H \rangle_\mathbb{Q} \), and let \( c \) be a common multiple of the denominators of all entries in the \( a_i \). By the proof of \[2\] Theorem 2.4 we can take \( d = c \det([\text{tr}(a_i a_j)]_{i,j}) \). A basis \( A \) can be found by, e.g., a standard ‘spinning-up’ process. However, when we know \( m \) such that \( \Gamma_{n,m} \) is in the finite index subgroup \( H_Z \) of \( \Gamma_n \), we can write down \( A \) directly. Let \( b_k(m) \) be the block diagonal matrix with

\[
\begin{pmatrix}
1 + m & m \\
-m & 1 - m
\end{pmatrix}
\]

in rows/columns \( k, k + 1 \), and 1s elsewhere on the main diagonal. Then

\[
\{1_n, t_{ij}(m), b_k(m) \mid 1 \leq i, j \leq n, i \neq j, 1 \leq k \leq n - 1 \}
\]

is a basis \( A \subseteq H \) with \( c = 1 \).

With a common denominator \( d = d(H) \) in hand, we invoke BasisLattice from \[7\] Section 3 with input \( S, d \). If \( g \) is any matrix whose columns are the elements of BasisLattice \( S, d \) then \( g \in \text{GL}(n, \mathbb{Q}) \) and \( H^g \leq \Gamma_n \).
6. Implementation

Our algorithms have been implemented in GAP [16]. For matrix group recognition, we rely on the recog package [30] of Max Neunhöffer and Ákos Seress.

To demonstrate practicality, and the effect that input parameters (degree $n$, number of generators, size of matrix entries, index in $\Gamma_n$) have on performance, we ran experiments on a range of arithmetic groups. Except for the elementary groups (see Proposition 1.12), we chose a value of $m$ that exposed a nontrivial quotient but which we cannot yet prove to be maximal; that is, the groups all contain $\Gamma_{n,m}$.

In Table 1, ‘# gens’ is the number of generators outside $\Gamma_{n,m}$, and $l$ is the decadic logarithm of the largest generator entry. Times (in seconds on a 3.7GHz Quad-Core late 2013 Mac Pro with 32GB memory) are for computing the index in $\Gamma_n$.

| Group    | # gens | $n$  | $m$  | $l$          | Index in $\Gamma_n$ | Time |
|----------|--------|------|------|-------------|---------------------|------|
| $E_{4,12}$ | 12     | 4    | $24^3$ | 1           | $2^{353}115137.13$ | 0.8  |
| $E_{4,53}$ | 12     | 4    | 53   | 2           | $2^{95}7.13$           | 0.1  |
| $E_{4,3207}$ | 12    | 4    | $3^6$ | 4           | $2^{16}475.13$         | 2.2  |
| $E_{8,7}$ | 56     | 8    | 7    | 1           | $2^{22}3^57^{19}2943.1201$ | 13   |
| RAN$_1$ | 5      | 4    | $2^53^2$ | 21          | $2^{50}15^27$           | 1    |
| RAN$_2$ | 3      | 4    | $2^53^4$ | 21          | $2^{74}3057$            | 6    |
| RAN$_3$ | 2      | 4    | $2^55^211^2$ | 4          | $2^{45}3^417^23113$     | 9    |
| RAN$_4$ | 10     | 6    | $2^53^2$ | 4           | $2^{54}3^85^21313$      | 0.5  |
| $\beta_1$ | 3      | 3    | 5    | 1           | $2^{17}7$              | 0.3  |
| $\beta_2$ | 3      | 3    | $2^5$ | 1           | $2^{17}7$              | 0.3  |
| $\beta_3$ | 3      | 3    | $3^373$ | 2           | $2^{3}1131801$         | 2    |
| $\beta_4$ | 3      | 3    | $2^523$ | 2           | $2^{31}729$            | 2    |
| $\beta_5$ | 3      | 3    | 5$^367$ | 3           | $2^{43}2510133140$     | 14   |
| $\beta_6$ | 3      | 3    | $2^83^35$ | 3          | $2^{29}310713$         | 3    |
| $\beta_7$ | 3      | 3    | $7^31021$ | 3          | $2^{53}457109347821$   | 40   |
| $\rho_0$ | 3      | 3    | 1    | 1           | $2^{3}1513$            | 0.2  |
| $\rho_1$ | 3      | 3    | $3^4$ | 1           | $2^{3}1513$            | 0.2  |
| $\rho_2$ | 3      | 3    | 5    | 1           | $2^{43}5712913$        | 1    |
| $\rho_3$ | 3      | 3    | 13   | 1           | $2^{3}31261$           | 1    |
| $\rho_4$ | 3      | 3    | $3^7$ | 1           | $2^{43}1173319$        | 2    |
| $\rho_5$ | 3      | 3    | 19   | 2           | $2^{2}3^53127331$      | 3    |

Table 1. Runtimes for setting up the initial data structure

Each group RAN$_i$ is generated by $\Gamma_{n,m}$ and products of transvections of level dividing $m$ (see [http://www.math.colostate.edu/~hulpke/examples/arithmetic.html](http://www.math.colostate.edu/~hulpke/examples/arithmetic.html) for the explicit matrices). They seem to be different from any elementary group.

The $\beta_i$ and $\rho_k$ are $\Gamma_{n,m}$-closures of their namesakes from [22], p. 414. Apart from $\rho_1$, these are arithmetic [22] Theorems 3.1 and 4.1. We discovered that $\beta_7$ has larger index than the lower bound in [22].

For a second batch of examples we tested our orbit-stabilizer algorithms on groups $H$ from Table 1. Times in Table 2 are solely for Stabilizer$(u, S)$, and include the setup for $H$. Here $l_1$ is the length of $\overline{H}u$, and $l_2$ is the length of the orbit of $u = \Gamma_{n,m}u$ under the preimage of Stab$_\mathcal{T}(\overline{u})$. While the $u$ look rather specific, random choices of $u$ do not alter runtimes appreciably. The magnitude of $m$
likewise has minor impact; if $m$ is composite then the calculation of $\mathcal{T} \pi$ can be separated into orbits modulo divisors of $m$.

| Group | $m$            | $u$             | $l_1$   | $l_2$ | Time |
|-------|----------------|-----------------|---------|-------|------|
| $E_{4,12}$ | $2^33^2$       | $(1,0,0,0)$     | $2^63^4$ | 1     | 1    |
| $E_{4,12}$ | $2^33^2$       | $(3,3,9,9)$     | $2^8$   | $3^4$ | 1.6  |
| $E_{4,12}$ | $2^33^2$       | $(6,6,6,6)$     | $2^4$   | $2^43^4$ | 158  |
| RAN$_1$  | $2^53^2$       | $(0,0,0,1)$     | $2^{10}3^3$ | 1     | 1    |
| RAN$_1$  | $2^53^2$       | $(0,0,0,6)$     | $2^6$   | $2^43^3$ | 31   |
| RAN$_1$  | $2^53^2$       | $(0,0,0,12)$    | $2^3$   | $2^73^3$ | 2346 |
| RAN$_2$  | $2^53^4$       | $(0,0,0,1)$     | $2^{22}3^{10}$ | 1     | 6.5  |
| RAN$_2$  | $2^53^4$       | $(0,0,0,2)$     | $2^{18}3^{10}$ | 2     | 7.5  |
| RAN$_2$  | $2^53^4$       | $(0,0,0,3)$     | $2^{22}3^6$  | $3^4$ | 315  |
| RAN$_2$  | $2^53^4$       | $(0,0,0,6)$     | $2^{18}3^6$  | $2^23^4$ | -    |
| $\beta_{-2}$ | $2^6$        | $(1,0,0)$       | $2^{13}3$  | 1     | 0.6  |
| $\beta_{-2}$ | $2^6$        | $(4,0,0)$       | $2^73$    | $2^6$ | 1.1  |
| $\beta_{-2}$ | $2^6$        | $(8,0,0)$       | $2^43$    | $2^9$ | 32   |
| $\beta_3$ | $3^373$       | $(1,0,0)$       | $2^53^937^3$ | 1     | 2    |
| $\beta_3$ | $3^373$       | $(9,9,9)$       | $2^63^23^73$ | $3^6$ | 86   |
| $\beta_5$ | $5^3367$      | $(1,0,0)$       | $2^63^25^323^361^367$ | 1     | 16   |
| $\beta_5$ | $5^3367$      | $(0,0,5)$       | $2^63^25^323^361^367$ | $5^2$ | 17   |
| $\rho_1$  | $3^4$         | $(1,0,0)$       | $3^11$    | 1     | 0.3  |
| $\rho_1$  | $3^4$         | $(3,0,0)$       | $3^8$    | $3^3$ | 0.35 |
| $\rho_1$  | $3^4$         | $(9,0,0)$       | $3^5$    | $3^6$ | 61   |
| $\rho_1$  | $3^4$         | $(9,9,9)$       | $3^5$    | $3^6$ | 72   |

**Table 2.** Runtimes for stabilizer computations

What does have an impact is divisibility of entries in $u$ by divisors of $m$. The reason that this affects runtime appears to be twofold. First, we must compare representatives for $u$ using $\text{OrbitGamma}_m$. The number of comparisons is quadratic in orbit length. Moreover, integer entries grow quickly even for modest examples (it can happen that stabilizer elements have entries with 10–20 digits). As the auxiliary operations entail iterated gcd calculations and integer factorization, each equivalence test becomes relatively expensive.

We do not report on other procedures from Subsection 3.2 that are essentially computations in $\text{GL}(n,\mathbb{Z}_m)$.

**Postscript.** For developments in the area since the publication of [11] (including further experiments with groups from [22]), see, e.g., [12] [13].

**Acknowledgments.** The authors received support from Science Foundation Ireland grant 11/RFP.1/ MTH3212 (Detinko and Flannery) and Simons Foundation Collaboration Grant 244502 (Hulpke). We are grateful to Professors A. Lubotzky, C. F. Miller III, and T. N. Venkataramana for helpful advice. We also thank Steffen Kionke, who detected an error in Proposition 2.11 of [11].

**REFERENCES**

1. H. Bäärnhielm, D. F. Holt, C. R. Leedham-Green, and E.A. O’Brien, *A practical model for computation with matrix groups*, J. Symbolic Comput. 68 (2015), 27–60.

2. L. Babai, R. Beals, and D. N. Rockmore, *Deciding finiteness of matrix groups in deterministic polynomial time*, Proc. of International Symposium on Symbolic and Algebraic Computation ISSAC ’93 (ACM Press), 1993, pp. 117–126.
3. H. Bass, M. Lazard, and J-P. Serre, *Sous-groupes d’indice fini dans SL(n, $\mathbb{Z}$)*, Bull. Amer. Math. Soc. 70 (1964), 385–392.
4. H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for $SL_n$ ($n \geq 3$) and $Sp_{2n}$ ($n \geq 2$)*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 33, 59–137.
5. J. Brenner, *The linear homogeneous group, III*, Ann. of Math. (2) 71 (1960), no. 2, 210–223.
6. A. S. Detinko, B. Eick, and D. L. Flannery, *Computing with matrix groups over infinite fields*, London Math. Soc. Lecture Note Ser. 387, 256–270, 2011.
7. A. S. Detinko, D. L. Flannery, and W. de Graaf, *Integrality and arithmeticity of solvable linear groups*, J. Symbolic Comput. 68 (2015), part 1, 138–145.
8. A. S. Detinko, D. L. Flannery, and E. A. O’Brien, *Algorithms for the Tits alternative and related problems*, J. Algebra 344 (2011), 397–406.
9. A. S. Detinko, D. L. Flannery, and E. A. O’Brien, *Recognizing finite matrix groups over infinite fields*, J. Symbolic Comput. 50 (2013), 100–109.
10. A. S. Detinko, D. L. Flannery, and E. A. O’Brien, *Algorithms for linear groups of finite rank*, J. Algebra 393 (2013), 187–196.
11. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra 421 (2015), 234–259.
12. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing in arithmetic groups*, Math. Comp. 87 (2018), 967–986.
13. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for experimenting with Zariski dense subgroups*, Exp. Math., https://doi.org/10.1080/10586458.2018.1466217
14. J. D. Dixon, *The orbit-stabilizer problem for linear groups*, Canad. J. Math. 37 (1985), no. 2, 238–259.
15. B. Eick and G. Ostheimer, *On the orbit-stabilizer problem for integral matrix actions of polycyclic groups*, Math. Comp. 72 (2003), no. 243, 1511–1529.
16. The GAP Group, *GAP – Groups, Algorithms, and Programming*, http://www.gap-system.org
17. F. Grunewald and D. Segal, *Some general algorithms. I. Arithmetic groups*, Ann. of Math. (2) 112 (1980), no. 3, 531–583.
18. F. Grunewald and D. Segal, *Decision problems concerning $S$-arithmetic groups*, J. Symbolic Logic 50 (1985), no. 3, 743–772.
19. A. J. Hahn and O. T. O’Meara, *The classical groups and $K$-theory*, Grundlehren der Mathematischen Wissenschaften, vol. 291, Springer-Verlag, Berlin, 1989.
20. A. Hulpke, *Computing conjugacy classes of elements in matrix groups*, J. Algebra 387 (2013), 268–286.
21. J. Humphreys, *Arithmetic groups*, Lecture Notes in Mathematics, vol. 789, Springer, Berlin, 1980.
22. D. D. Long and A. W. Reid, *Small subgroups of $SL(3, \mathbb{Z})$*, Exp. Math. 20 (2011), no. 4, 412–425.
23. A. Lubotzky, *Dimension function for discrete groups*, London Math. Soc. Lecture Note Ser. 121, 254–262, 1986.
24. A. Lubotzky, *One for almost all: generation of $SL(n, \mathbb{Z})$ by subsets of $SL(n, \mathbb{Z})$*, Contemp. Math. 243, 125–128, 1999.
25. A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, Basel, 2003.
26. C. Meiri, *Generating pairs for finite index subgroups of $SL(n, \mathbb{Z})$*, J. Algebra 470 (2017), 420–424.
27. J. L. Mennicke, *Finite factor groups of the unimodular group*, Ann. of Math. (2) 81 (1965), 31–37.
28. C. F. Miller III, personal communication.
29. J. Milnor, *Introduction to algebraic $K$-theory*, Princeton Univ. Press, Princeton, NJ, 1971, Ann. of Math. Stud., no. 72.
30. M. Neunhöffer and Á. Seress, *A data structure for a uniform approach to computations with finite groups*, in ISSAC 2003, pp. 254–261. ACM, New York, 2006.
31. M. Newman, *Integral matrices*, Academic Press, New York, 1972, Pure and Applied Mathematics, Vol. 10.
32. P. Sarnak, *Notes on thin matrix groups*, in: Thin groups and superstrong approximation, Math. Sci. Res. Inst. Publ. 61, pp. 343–362. Cambridge Univ. Press, Cambridge, 2014.
33. R. Sharma and T. N. Venkataramana, *Generations for arithmetic groups*, Geom. Dedicata 114 (2005), 103–146.
34. D. A. Suprunenko, *Matrix groups*, Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI, 1976.
35. B. Sury, *The congruence subgroup problem*, J. Indian Inst. Sci. (4) 87 (2007), 457–465.
36. B. Sury and T. N. Venkataramana, *Generators for all principal congruence subgroups of $SL(n, \mathbb{Z})$ with $n \geq 3$*, Proc. Amer. Math. Soc. 122 (1994), no. 2, 355–358.
37. J. S. Wilson, *The normal and subnormal structure of general linear groups*, Proc. Cambridge Philos. Soc. 71 (1972), 163–177.