The congruence subgroup problem for $\mathrm{SL}_n(\mathbb{Z})$

Andrew Putman

Abstract

Following Bass–Milnor–Serre, we prove that $\mathrm{SL}_n(\mathbb{Z})$ has the congruence subgroup property for $n \geq 3$. This was originally proved by Mennicke and Bass–Lazard–Serre.

Let $\Gamma_n = \mathrm{SL}_n(\mathbb{Z})$. The congruence subgroup problem for Γ_n (solved independently by Mennicke [Me] and Bass–Lazard–Serre [BLS]) seeks to classify all finite-index subgroups of Γ_n. For $\ell \geq 2$, the **level ℓ principal congruence subgroup** of Γ_n, denoted $\Gamma_n(\ell)$, is the kernel of the homomorphism $\Gamma_n \to \mathrm{SL}_n(\mathbb{Z}/\ell)$ that reduces the entries in matrices modulo ℓ. Clearly $\Gamma_n(\ell)$ is finite-index in Γ_n. A subgroup G of Γ_n is a **congruence subgroup** if there exists some $\ell \geq 2$ such that $\Gamma_n(\ell) \subset G$. Mennicke and Bass–Lazard–Serre proved the following theorem.

Theorem A. *For $n \geq 3$, every finite-index subgroup of Γ_n is a congruence subgroup.*

Remark. This is false for $n = 2$. Indeed, $\mathrm{SL}_2(\mathbb{Z}) \cong (\mathbb{Z}/4) *_{\mathbb{Z}/2} (\mathbb{Z}/6)$ contains a free subgroup of finite index, and thus contains a veritable zoo of finite-index subgroups. Most of these are not congruence subgroups.

Bass–Milnor–Serre [BMiS] later generalized Theorem A to deal with finite-index subgroups of $\mathrm{SL}_n(\mathcal{O})$ for number rings $\mathcal{O}$; they proved that $\mathrm{SL}_n(\mathcal{O})$ satisfies a version of the congruence subgroup problem if and only if $\mathcal{O}$ has a real embedding. In this note, we will describe Bass–Milnor–Serre's proof, specialized to just prove Theorem A.

Acknowledgments. I want to thank Xiyan Zhong for pointing out some small mistakes in a previous version.

1 Reduction to a generating set

It turns out that the key to proving Theorem A is to construct (normal) generating sets for $\Gamma_n(\ell)$. For distinct $1 \leq i,j \leq n$, let $e_{ij} \in \Gamma_n$ denote the elementary matrix with 1's along the diagonal and at position (i,j), and 0's elsewhere. Observe that $e_{ij}^{\ell} \in \Gamma_n(\ell)$. Bass–Milnor–Serre proved the following theorem.

Theorem 1.1. *For $n \geq 3$ and $\ell \geq 2$, the group $\Gamma_n(\ell)$ is normally generated (as a subgroup of Γ_n) by $\{e_{ij}^{\ell} \mid 1 \leq i,j \leq n \text{ distinct}\}$.*

The remaining sections of this note will be devoted to the proof of Theorem 1.1, which will be completed in §5. Before we get to that, we will show how to derive Theorem A from it.

Proof of Theorem A. Let G be a finite-index subgroup of Γ_n. We wish to show that G contains $\Gamma_n(\ell)$ for some $\ell \geq 2$. Passing to a deeper finite-index subgroup, we can assume that G is a normal subgroup of Γ_n. For all distinct $1 \leq i, j \leq n$, the fact that G is finite-index in Γ_n implies that there exists some $\ell_{ij} \geq 1$ such that $e_{ij}^{\ell_{ij}} \in G$. Define ℓ to be the least common multiple of the ℓ_{ij}, so $e_{ij}^{\ell} \in G$ for all distinct $1 \leq i, j \leq n$. Since G is a normal subgroup of Γ_n, we deduce that G contains the normal closure of the set $\{e_{ij}^{\ell} \mid 1 \leq i, j \leq n \text{ distinct}\}$, which by Theorem 1.1 is $\Gamma_n(\ell)$. Thus G is a congruence subgroup, as desired. □

2 Reduction to 2×2 matrices

The first step in proving Theorem 1.1 is to construct a larger generating set for $\Gamma_n(\ell)$. Define $E\Gamma_n(\ell)$ to be the normal closure in Γ_n of $\{e_{ij}^{\ell} \mid 1 \leq i, j \leq n \text{ distinct}\}$. For $m < n$, we will regard $\Gamma_m(\ell)$ as a subgroup of $\Gamma_n(\ell)$ via the map

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.1}$$

The following lemma is the main result of this section.

Lemma 2.1. *For $n \geq 2$ and $\ell \geq 2$, the group $\Gamma_n(\ell)$ is generated by $\Gamma_2(\ell)$ and $E\Gamma_n(\ell)$.*

For the proof of Lemma 2.1, we need the following lemma.

Lemma 2.2. *For $n \geq 3$, let $a_1, \ldots, a_n \in \mathbb{Z}$ satisfy $\gcd(gcd)(a_1, \ldots, a_n) = 1$. Then there exist $c_2, \ldots, c_n \in \mathbb{Z}$ such that $\gcd(a_2 + c_2 a_1, \ldots, a_n + c_n a_1) = 1$.*

Remark. A ring R which satisfies the conclusion of Lemma 2.2 for $n \geq r$ is said to satisfy Bass's stable range condition SR_r. We remark that in this more general context, the condition $\gcd(a_1, \ldots, a_n) = 1$ should be interpreted as asserting that $Ra_1 + \cdots + Ra_n = R$. Lemma 2.2 says that $\mathbb{Z}$ satisfies SR_3.

Proof of Lemma 2.2. If any of the a_i are zero then this is trivial, so we can assume that $a_i \neq 0$ for all $1 \leq i \leq n$. In this case, it will turn out that we can find a single $c \in \mathbb{Z}$ such that $\gcd(a_2 + ca_1, a_3, \ldots, a_n) = 1$. Set $b = \gcd(a_3, \ldots, a_n)$, and let $p_1, \ldots, p_k$ be the distinct primes dividing b. For each $1 \leq i \leq k$, we know that p_i cannot divide both a_1 and a_2, so there exists some $\lambda_i \in \{0, 1\}$ such that

$$a_2 + \lambda_i a_1 \not\equiv 0 \pmod{p_i}.$$

By the Chinese remainder theorem, there exists some $c \in \mathbb{Z}$ such that

$$c \equiv \lambda_i \pmod{p_i}$$

for $1 \leq i \leq k$, which implies that

$$a_2 + ca_1 \not\equiv 0 \pmod{p_i}$$

for all $1 \leq i \leq k$. We conclude that $\gcd(a_2 + ca_1, b) = 1$, and thus that $\gcd(a_2 + ca_1, a_3, \ldots, a_n) = 1$. □

Proof of Lemma 2.1. By induction on n, it is enough to show that $\Gamma_n(\ell)$ is generated by $\Gamma_{n-1}(\ell)$ and $E\Gamma_n(\ell)$. Consider $M \in \Gamma_n(\ell)$. Let the bottom row of M be $(a_1, \ldots, a_n)$, so

$$a_1 \equiv \cdots \equiv a_{n-1} \equiv 0 \pmod{\ell} \qquad \text{and} \qquad a_n \equiv 1 \pmod{\ell}.$$

Also, $\gcd(a_1, \ldots, a_n) = 1$. Since $\ell \mid a_1$, we have $\gcd(\ell a_1, a_2, \ldots, a_n) = 1$. By Lemma 2.2, we can find $c_2, \ldots, c_n \in \mathbb{Z}$ such that $\gcd(a_2 + c_2 \ell a_1, \ldots, a_n + c_n \ell a_1) = 1$. For $2 \le i \le n$, set $a_i' = a_i + c_i \ell a_1$. By multiplying M on the right by elements of $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$, we can perform column operations to convert its bottom row into $(a_1, a_2', \ldots, a_n')$. Next, since $\ell \mid a_1$ we can multiply our matrix on the right by elements of $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$ to perform column operations and convert its bottom row into $(\ell, a_2', \ldots, a_n')$. The next step is the most subtle and is the reason why we need to take the normal closure of $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$. Write $a_n' = 1 + k\ell$. Multiplying our matrix on the right by e_{1n}^{k} (which does not necessarily lie in $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$) converts its last row to $(\ell, a_2', \ldots, a_{n-1}', 1)$. Multiplying our matrix on the right by elements of $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$, we can then perform column operations and convert its last row into $(0, \ldots, 0, 1)$. Multiplying our matrix on the right by e_{1n}^{-k} then does not change its last row, and using the fact that $E\Gamma_n(\ell)$ is the normal closure of $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$ we see that the resulting matrix is the result of multiplying our original matrix M on the right by an element of $E\Gamma_n(\ell)$. We now can multiply our matrix on the left by elements of $\{e_{ij}^{\ell} \mid 1 \le i, j \le n \text{ distinct}\}$ to perform row operations and convert its last column to $(0, \ldots, 0, 1)$. Our matrix now lies in $\Gamma_{n-1}(\ell) \subset \Gamma_n(\ell)$, as desired. □

3 The nature of the quotient

Define $Q_n(\ell) = \Gamma_n(\ell)/E\Gamma_n(\ell)$. The main result of this section is as follows.

Lemma 3.1. *For $n \ge 3$, the group $Q_n(\ell)$ is a finitely generated abelian group. Moreover, the action of Γ_n on $Q_n(\ell)$ induced by the conjugation action of Γ_n on $\Gamma_n(\ell)$ is trivial.*

Remark. Lemma 2.1 implies that elements of $Q_n(\ell)$ can be represented by 2×2 matrices; however, the condition $n \ge 3$ in Lemma 3.1 is necessary.

Proof of Lemma 3.1. Since $Q_n(\ell)$ is a quotient of the finitely generated group $\Gamma_n(\ell)$ (we remark that the group $\Gamma_n(\ell)$ is finitely generated since it is a finite-index subgroup of the finitely generated group Γ_n), it is itself finitely generated. The fact that $Q_n(\ell)$ is abelian will follow from the fact that the Γ_n-action on it is trivial since $\Gamma_n(\ell) \subset \Gamma_n$, so it is enough to prove this. The group Γ_n is generated by elementary matrices e_{ij}. Moreover, we have the easily-verified matrix identity $e_{ik} = [e_{ij}, e_{jk}]$ when $1 \le i, j, k \le n$ are distinct. Since $n \ge 3$, we see that Γ_n is actually generated by $\{e_{in}, e_{ni} \mid 1 \le i \le n-1\}$, so it is enough to prove that these generators act trivially on $Q_n(\ell)$. Lemma 2.1 implies that $Q_n(\ell)$ is generated by the image of $\Gamma_2(\ell)$, so it is enough to prove that for $1 \le i \le n-1$ and $M \in \Gamma_2(\ell)$, we have $[e_{in}, M] \in E\Gamma_n(\ell)$ and $[e_{ni}, M] \in E\Gamma_n(\ell)$. For $i \ge 3$, we have $[e_{in}, M] = [e_{ni}, M] = 1$, so we just have to deal with $i = 1$ and $i = 2$. All four of the necessary calculations are similar; we will give the details for e_{1n}, and in fact to simplify our notation we will assume that $n = 3$ (the general case will be clear from this). Write

$$M = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We then have

$$\begin{aligned}
[e_{13}, M] &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b & 0 \\ -c & a & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a & b & 1 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b & -1 \\ -c & a & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1-a \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

This clearly lies in $E\Gamma_n(\ell)$, as desired. □

4 Mennicke symbols

The goal of this section is to show how to generate $Q_n(\ell)$ in terms of "Mennicke symbols" and to compute some relations between these Mennicke symbols. The starting point is the following lemma.

Lemma 4.1. *Fix $n \geq 2$ and $\ell \geq 2$. Consider $a, b \in \mathbb{Z}$ which are relatively prime and satisfy*

$$a \equiv 1 \pmod{\ell} \qquad \text{and} \qquad b \equiv 0 \pmod{\ell}. \tag{4.1}$$

Then there exists some $M \in \Gamma_2(\ell)$ whose first row is (a, b). Moreover, if $M, M' \in \Gamma_2(\ell)$ are matrices whose first rows are (a, b), then the images of M and M' in $Q_2(\ell)$ are the same.

Proof. Since $\gcd(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Using (4.1), we see that when we reduce $ax + by = 1$ modulo ℓ we get that $x \equiv 1 \pmod{\ell}$. Setting $c = ay - y$ and $d = by + x$ and

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we get that

$$\det(M) = a(by + x) - b(ay - y) = (ax + by) + (aby - bay) = 1$$

and

$$c \equiv 1 \cdot y - y \equiv 0 \pmod{\ell} \quad \text{and} \quad d \equiv 0 \cdot y + x \equiv 1 \pmod{\ell},$$

i.e. that $M \in \Gamma_2(\ell)$. If

$$M' = \begin{pmatrix} a & b \\ c' & d' \end{pmatrix} \in \Gamma_2(\ell),$$

we get that

$$M(M')^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d' & -b \\ -c' & a \end{pmatrix} = \begin{pmatrix} ad' - bc' & -ab + ba \\ cd' - dc' & -cb + da \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ cd' - dc' & 1 \end{pmatrix}.$$

This is an element of $E\Gamma_2(\ell)$, so we get that M and M' have the same image in $Q_2(\ell)$. □

We can thus make the following definition. Assume that we have fixed $n \geq 3$ and $\ell \geq 2$. Consider $a, b \in \mathbb{Z}$ which are relatively prime and satisfy (4.1). Using Lemma 4.1, let $M \in \Gamma_2(\ell)$ have first row (a, b). The **Mennicke symbol** $[a, b]_\ell$ is the image of M in $Q_n(\ell)$. By Lemma 4.1, this does not depend on the choice of M. When we say that some $[a, b]_\ell$ is a Mennicke symbol, we are saying implicitly that a and b are relatively prime and satisfy (4.1).

Remark. The usual convention is to reverse the order of a and b in a Mennicke symbol, but we find the above ordering a little less confusing.

Remark. In all our calculations, we will manipulate matrices which either are 2×2 or 3×3 matrices; these are included in $\mathrm{SL}_n(\mathbb{Z})$ via (2.1).

The following follows immediately from Lemmas 4.1 and 3.1.

Corollary 4.2. *Fix $n \geq 2$ and $\ell \geq 2$. Then $Q_n(\ell)$ is a finitely generated abelian group generated by the set of Mennicke symbols $[a, b]_\ell$.*

Even though $Q_n(\ell)$ is an abelian group, we will continue to write it multiplicatively; in particular, its unit will be written 1.

There are infinitely many distinct Mennicke symbols, so since $Q_n(\ell)$ is a finitely generated abelian group there must be many relations between different Mennicke symbols. The following lemma gives some relations. We remark that Mennicke symbols are usually defined abstractly via the relations in this lemma.

Lemma 4.3. *Fix $n \geq 3$ and $\ell \geq 2$, and let $[a, b]_\ell$ be a Mennicke symbol. We then have the following.*

- *$[a, b]_\ell = [a, b + ta]_\ell$ for $t \in \ell\mathbb{Z}$.*
- *$[a, b]_\ell = [a + tb, b]_\ell$ for $t \in \mathbb{Z}$.*
- *$[a, bb']_\ell = [a, b]_\ell [a, b']_\ell$ whenever $[a, b']_\ell$ is a Mennicke symbol.*

Proof. In all of the calculations in this proof, the reader should keep in mind that elements of $E\Gamma_n(\ell)$ are trivial in $Q_n(\ell)$. Choose a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_2(\ell)$$

The first relation follows from the calculation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+ta \\ c & d+tc \end{pmatrix};$$

here the second matrix lies in $E\Gamma_n(\ell)$ whenever $t \in \ell\mathbb{Z}$.

The second relation is more complicated since we need it for $t \in \mathbb{Z}$, not merely for $t \in \ell\mathbb{Z}$. Observe that

$$\begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix}\begin{pmatrix} a+bt & b \\ c+dt & d \end{pmatrix} = \begin{pmatrix} a+bt & b \\ * & * \end{pmatrix},$$

where $*$ are integers. Lemma 3.1 says that the action of Γ_n on $Q_n(\ell)$ induced by conjugation is trivial, so this calculation shows that $[a,b]_\ell = [a+tb,b]_\ell$.

The third and final relation is the most complicated of the three, and will take a little work. Moreover, we will have to go up to 3×3 matrices. Choose a matrix

$$\begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}$$

that lies in $\Gamma_2(\ell)$. Lemma 3.1 says that the action of Γ_n on $Q_n(\ell)$ induced by conjugation is trivial, so $[a,b']_\ell$ can be represented by the matrix

$$\begin{aligned}
&\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} a & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}\\
=&\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} a & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}\\
=&\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} -b' & 0 & a \\ -d' & 0 & c' \\ 0 & -1 & 0 \end{pmatrix}\\
=&\begin{pmatrix} d' & 0 & -c' \\ 0 & 1 & 0 \\ -b' & 0 & a \end{pmatrix}
\end{aligned}$$

It follows that $[a,b]_\ell[a,b']_\ell$ is represented by the matrix

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} d' & 0 & -c' \\ 0 & 1 & 0 \\ -b' & 0 & a \end{pmatrix} = \begin{pmatrix} ad' & b & -ac' \\ * & * & * \\ -b' & 0 & a \end{pmatrix},$$

where the $*$ are integers. Multiplying this on the left or right by elementary matrices in $E\Gamma_3(\ell)$, we can perform (certain) row and column operations without changing the image in $Q_n(\ell)$. The sequence of operations we perform is as follows; the "r" or "c" above the arrows indicates whether it is a row or column operation. We remark that the 1 in the upper left hand corner of the second matrix appears because $ad' - b'c' = 1$.

$$\begin{pmatrix} ad' & b & -ac' \\ * & * & * \\ -b' & 0 & a \end{pmatrix} \xrightarrow{r} \begin{pmatrix} 1 & b & 0 \\ * & * & * \\ -b' & 0 & a \end{pmatrix} \xrightarrow{r} \begin{pmatrix} 1 & b & 0 \\ * & * & * \\ 0 & bb' & a \end{pmatrix} \xrightarrow{c} \begin{pmatrix} 1 & 0 & 0 \\ * & * & * \\ 0 & bb' & a \end{pmatrix} \xrightarrow{r} \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & bb' & a \end{pmatrix}$$

Next, we can conjugate by any element of $\mathrm{SL}_3(\mathbb{Z})$ without changing the image in $Q_n(\ell)$. Conjugating by a permutation matrix (with determinant +1), our matrix becomes

$$\begin{pmatrix} a & bb' & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which represents $[a, bb']_\ell$, as desired. □

5 Killing Mennicke symbols

Theorem 1.1 is equivalent to the assertion that $Q_n(\ell) = 0$ for all $n \geq 3$ and $\ell \geq 2$. By Corollary 4.2, this is equivalent to the assertion that $[a, b]_\ell = 0$ for all Mennicke symbols $[a, b]_\ell$, which will be the main result of this section (see Lemma 5.3 below). The proof of this will only use the relations from Lemma 4.3. Since we will use these relations constantly, we will not refer explicitly to this lemma in our proofs. Throughout this section, we will fix $n \geq 3$ and $\ell \geq 2$.

We begin with the following observation.

Lemma 5.1. *Let $[a, b]_\ell$ be a Mennicke symbol such that $b \equiv \pm 1 \pmod{a}$. Then $[a, b]_\ell = 1$.*

Proof. Write $b = \pm 1 + ka$ for some $k \in \mathbb{Z}$. Since $b \equiv 0 \pmod{\ell}$, we have

$$[a, b]_\ell = [a, b - ab]_\ell = [a, b(1-a)]_\ell = [a, (\pm 1 + ka)(1-a)]_\ell = [a, \pm(1-a) + ka(1-a)]_\ell.$$

Since $1 - a \equiv 0 \pmod{\ell}$, this equals

$$[a, \pm(1-a)]_\ell = [1, \pm(1-a)]_\ell.$$

Again using the fact that $1 - a \equiv 0 \pmod{\ell}$, this equals $[1, 0]_\ell = 1$, as desired. □

This has the following corollary. Recall that the *Euler totient function* is the function ϕ that takes a nonzero integer a to the number of units in $\mathbb{Z}/a$. If $a, a' \in \mathbb{Z}$ are relatively prime, then the Chinese remainder theorem says that $\mathbb{Z}/aa' \cong \mathbb{Z}/a \oplus \mathbb{Z}/a'$, so $\phi(aa') = \phi(a)\phi(a')$. Moreover, if p is prime and $k \geq 1$, then $\phi(p^k) = p^k - p^{k-1}$. It follows that if $a = \pm p_1^{k_1} \cdots p_m^{k_m}$ is the prime factorization of a, then

$$\phi(a) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_m^{k_m} - p_m^{k_m - 1}).$$

Corollary 5.2. *Let $[a, b]_\ell$ be a Mennicke symbol. Then $[a, b]_\ell^{\phi(a)} = 1$.*

Proof. Since $\gcd(a,b) = 1$, the integer b projects to an element of the group of units of $\mathbb{Z}/a$, and thus $b^{\phi(a)}$ projects to the identity in $\mathbb{Z}/a$, i.e. $b^{\phi(a)} \equiv 1 \pmod{a}$. Applying Lemma 5.1, we see that

$$[a,b]_\ell^{\phi(a)} = [a,b^{\phi(a)}]_\ell = 1. \qquad \square$$

This corollary implies that $Q_n(\ell)$ is a *finite* abelian group. We now come to the main result of this section.

Lemma 5.3. *Let $[a,b]_\ell$ be a Mennicke symbol and let p be prime. Then p does not divide the order of $[a,b]_\ell$. Consequently, $[a,b]_\ell = 1$.*

Proof. We will accomplish this in three steps.

Step 1. *The order of $[a,b]_\ell$ is a power of 2.*

Since $\gcd(a,b) = 1$, Dirichlet's theorem on primes in arithmetic progressions implies that there exists some prime p such that $p \equiv a \pmod{b}$, and thus $[a,b]_\ell = [p,b]_\ell$. Corollary 5.2 implies that the order of $[a,b]_\ell = [p,b]_\ell$ divides $\phi(p) = p-1$. Let $q_1,\dots,q_m$ be the odd prime factors of $p-1$. Both b and all the q_i are coprime to p, so by Dirichlet's theorem there exists a prime p_1 such that

$$p_1 \equiv -p \pmod{bq_1q_2\cdots q_m}.$$

A final application of Dirichlet's theorem yields a prime p_2 such that

$$p_2 \equiv -1 \pmod{bq_1q_2\cdots q_m}.$$

We have

$$p_1p_2 \equiv (-p)(-1) \equiv p \pmod{b},$$

so $[p,b]_\ell = [p_1p_2,b]_\ell$. Corollary 5.2 implies that the order of $[a,b]_\ell = [p,b]_\ell = [p_1p_2,b]_\ell$ divides

$$\phi(p_1p_2) = (p_1-1)(p_2-1).$$

For $1 \le i \le m$, we have

$$(p_1-1)(p_2-1) \equiv (-p-1)(-1-1) \equiv 2(p+1) \pmod{q_i}.$$

Since q_i is an odd prime which divides $p-1$, it cannot divide $2(p+1)$. We deduce that q_i does not divide $(p_1-1)(p_2-1)$, and thus cannot divide the order of $[a,b]_\ell = [p,b]_\ell = [p_1p_2,b]_\ell$. Since the q_i are all the odd prime factors of $p-1$ and we proved above that the order of $[a,b]_\ell$ divides $p-1$, we deduce that the only prime that can divide the order of $[a,b]_\ell$ is 2, as desired.

Step 2. *If either $a \equiv 3 \pmod{4}$ or $b \not\equiv 0 \pmod{4}$, then $[a,b]_\ell = 1$.*

We first find some $a' \in \mathbb{Z}$ such that $[a',b]_\ell$ is a Mennicke symbol satisfying $[a',b]_\ell = [a,b]_\ell$ and such that $a' \equiv 3 \pmod{4}$. If $a \equiv 3 \pmod{4}$, then we can take $a' = a$. Assume now that $a \not\equiv 3 \pmod{4}$. If $b \equiv 1 \pmod{4}$ or $b \equiv 3 \pmod{4}$, then we can find some $k \in \mathbb{Z}$ such that $a + kb \equiv 3 \pmod{4}$, and we can take $a' = a + kb$. Finally, if $b \equiv 2$

(mod 4), then since $\gcd(a,b) = 1$ we must have a odd, and thus $a \equiv 1 \pmod 4$. We can therefore take $a' = a + b$.

Since $a' \equiv 3 \pmod 4$ and $\gcd(a', b) = 1$, we have $\gcd(a', 4b) = 1$. Dirichlet's theorem on primes in arithmetic progressions thus implies that there exists some prime p such that $p \equiv a' \pmod{4b}$. We then have $[p,b]_\ell = [a',b]_\ell = [a,b]_\ell$ and $p \equiv 3 \pmod 4$. The number $\frac{p-1}{2}$ is thus odd. We have

$$b^{\frac{p-1}{2}} \equiv \pm 1 \pmod p,$$

so using Lemma 5.1 we have

$$[a,b]_\ell^{\frac{p-1}{2}} = [p,b]_\ell^{\frac{p-1}{2}} = [p, b^{\frac{p-1}{2}}]_\ell = 1.$$

This implies that the order of $[a,b]_\ell$ divides the odd number $\frac{p-1}{2}$, and thus that the order of $[a,b]_\ell$ is odd. Combining this with the first step, we see that $[a,b]_\ell = 1$, as desired.

Step 3. *If $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$, then $[a,b]_\ell = 1$.*

This is very similar to the previous step (but with a slight twist). Since $\gcd(a,b) = 1$, Dirichlet's theorem on primes in arithmetic progressions implies that there exists some prime p such that $p \equiv -a \pmod b$. We then have $[a,b]_\ell = [-p,b]_\ell$ and

$$p \equiv -a \equiv -1 \equiv 3 \pmod 4.$$

The number $\frac{p-1}{2}$ is thus odd. We have

$$b^{\frac{p-1}{2}} \equiv \pm 1 \pmod{-p},$$

so using Lemma 5.1 we have

$$[a,b]_\ell^{\frac{p-1}{2}} = [-p,b]_\ell^{\frac{p-1}{2}} = [-p, b^{\frac{p-1}{2}}]_\ell = 1.$$

This implies that the order of $[a,b]_\ell$ divides the odd number $\frac{p-1}{2}$, and thus that the order of $[a,b]_\ell$ is odd. Combining this with the first step, we see that $[a,b]_\ell = 1$, as desired. □

References

[BLS] H. Bass, M. Lazard and J.-P. Serre, Sous-groupes d'indice fini dans **SL**$(n, \mathbf{Z})$, Bull. Amer. Math. Soc. **70** (1964), 385–392.

[BMiS] 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. No. 33 (1967), 59–137.

[Me] J. L. Mennicke, Finite factor groups of the unimodular group, Ann. of Math. (2) **81** (1965), 31–37.

Andrew Putman
Department of Mathematics
Rice University, MS 136
6100 Main St.
Houston, TX 77005
andyp@math.rice.edu