CONGRUENCE TESTING FOR ODD SUBGROUPS OF THE MODULAR GROUP

THOMAS HAMILTON AND DAVID LOEFFLER

Abstract. We give a computationally effective criterion for determining whether a finite-index subgroup of $\mathrm{SL}_2(\mathbf{Z})$ is a congruence subgroup, extending earlier work of Hsu for subgroups of $\mathrm{PSL}_2(\mathbf{Z})$.

Recall that a finite-index subgroup of $\mathrm{SL}_2(\mathbf{Z})$ is said to be a *congruence subgroup* if it is defined by congruence conditions on the entries of its elements; formally, a subgroup is congruence if it contains the subgroup $\Gamma(N)$ of matrices congruent to the identity modulo N, and the least such N is its *level*.

We are interested in the following question:

Question. *Is there an efficient procedure that will determine whether a finite-index subgroup of* $\mathrm{SL}_2(\mathbf{Z})$ *is congruence?*

One such algorithm follows from the following theorem, proved in [KSV11], which is an extension of a classical theorem of Wolfahrt:

Theorem 1 (Kiming–Schütt–Verrill)**.** *Let* $\Gamma \le \mathrm{SL}_2(\mathbf{Z})$ *be a finite-index subgroup, and let* d *be the lowest common multiple of the widths of the cusps of* Γ*. If* Γ *is congruence, then its level is either* d *or* $2d$*.*

(The case of level $2d$ can only occur if Γ is *odd*, i.e. does not contain -1.)

In principle, one can now determine whether Γ is congruence by calculating explicitly a list of generators for $\Gamma(N)$, where $N = d$ or $2d$ as appropriate, and testing whether each of these is contained in Γ. This approach is used in *op.cit.* in order to give explicit examples of non-congruence lifts to $\mathrm{SL}_2(\mathbf{Z})$ of congruence subgroups of $\mathrm{PSL}_2(\mathbf{Z})$. However, the number of generators of $\Gamma(N)$ grows rather quickly with N, so this algorithm rapidly becomes impractical for large values of N.

We present the following alternative approach to the above problem. As has been noted by Hsu [Hsu96] and others, a convenient data structure for representing a subgroup of $\mathrm{SL}_2(\mathbf{Z})$ of index m is by the homomorphism $\mathrm{SL}_2(\mathbf{Z}) \to S_m$ given by left multiplication on the cosets $\mathrm{SL}_2(\mathbf{Z})/\Gamma$. This, in turn, can be represented by two permutations giving the action of the generators $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ of $\mathrm{SL}_2(\mathbf{Z})$ on the cosets $\mathrm{SL}_2(\mathbf{Z})/\Gamma$.

The computer algebra package Sage contains a library of routines for working with subgroups defined in this way, implemented by Vincent Delecroix and the second author based on an earlier implementation by Chris Kurth.

Theorem 2. *Let* $N = d$ *if* $-1 \in \Gamma$ *and* $N = 2d$ *otherwise. Then there exists an explicit list of relations* $\mathcal{L}_N$ *in* L *and* R *(of length* ≤ 7*), such that* Γ *is congruence if and only if the permutation representation of* $\mathrm{SL}_2(\mathbf{Z})$ *corresponding to* Γ *satisfies the relations in* $\mathcal{L}_N$*.*

This theorem has been proved for subgroups containing -1 by Hsu [Hsu96]; our proof follows Hsu's closely, except that we use the Kiming–Schütt–Verrill theorem (Theorem 1) in place of the classical theorem of Wolfahrt.

Proposition 3. *Let $N \geq 1$. There is an explicit finite set $\mathcal{L}_N$ of words in L and R whose image in* $\mathrm{SL}_2(\mathbf{Z})$ normally generates $\Gamma(N)$ *(that is, $\Gamma(N)$ is the smallest normal subgroup of $\mathrm{SL}_2(\mathbf{Z})$ containing the elements in $\mathcal{L}_N$).*

Proof. See [Hsu96, Theorem 2.4]. The starting-point of the proof is the well-known fact that $\mathrm{SL}_2(\mathbf{Z})$ has the presentation

$$\left\langle L, R \mid (LR^{-1}L)^2(R^{-1}L)^{-3}, (LR^{-1}L)^4 \right\rangle$$

where L and R correspond to the matrices given above. Thus if $\mathcal{L}$ is any set of words in L and R, the group

$$\left\langle L, R \mid (LR^{-1}L)^2(R^{-1}L)^{-3}, (LR^{-1}L)^4, \mathcal{L} \right\rangle \tag{1}$$

is the largest quotient of $\mathrm{SL}_2(\mathbf{Z})$ in which the elements in the image of $\mathcal{L}$ map to the identity, which is the quotient of $\mathrm{SL}_2(\mathbf{Z})$ by the subgroup normally generated by the image of $\mathcal{L}$. In particular, the images of the elements of $\mathcal{L}$ normally generate $\Gamma(N)$ if and only if (1) is a presentation of the finite group $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$.

Explicit presentations of the groups $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ for all N in terms of the generators L and R are given in [Hsu96, Lemmas 3.3–3.5] (based on earlier work of Behr and Mennicke [BM68]), so it suffices to take $\mathcal{L}_N$ to be the set of relations appearing in these presentations. □

Proof of Theorem 2. Let N be as defined in the statement of the theorem. We know that Γ is congruence if and only if it contains $\Gamma(N)$. Let Γ' be the *normal core* of Γ, i.e. the intersection of the conjugates of Γ in $\mathrm{SL}_2(\mathbf{Z})$; then, since the elements of $\mathcal{L}_N$ normally generate $\Gamma(N)$, it follows that Γ is congruence if and only if $\mathcal{L}_N \subset \Gamma'$.

However, Γ' is precisely the kernel of the map $\phi : \mathrm{SL}_2(\mathbf{Z}) \to S_m$ giving the permutation representation of Γ. So Γ is congruence if and only if ϕ is trivial on the elements of $\mathcal{L}_N$. □

(One could clearly adapt this argument to work with other explicit descriptions of Γ as long as one has an algorithm for computing whether a given element of $\mathrm{SL}_2(\mathbf{Z})$ lies in the normal core of Γ.)

We now reproduce, for the reader's convenience, an explicit list of relations $\mathcal{L}_N$ as in Theorem 2, based on those given by Hsu.

- If N is odd, one may take $\mathcal{L}_N$ to contain the single relation

  $$\left(R^2L^{-\frac{1}{2}}\right)^3 = 1,$$

  where $\frac{1}{2}$ is the multiplicative inverse of 2 mod N. This follows from the fact that for N odd,

  $$\left\langle L, R \;\middle|\; L^N = 1, (LR^{-1}L)^2 = (R^{-1}L)^3, (LR^{-1}L)^4 = 1, \left(R^2L^{-\frac{1}{2}}\right)^3 = 1 \right\rangle$$

  is a presentation of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, by [Hsu96, Lemma 3.3]. The relations $(LR^{-1}L)^2 = (R^{-1}L)^3$ and $(LR^{-1}L)^4 = 1$ are redundant; they are automatically satisfied by the permutation representation of $\mathrm{SL}_2(\mathbf{Z})$ corresponding to Γ, since they are satisfied in $\mathrm{SL}_2(\mathbf{Z})$ itself. The relation $L^N = 1$ is also automatically satisfied, since by definition N is divisible by the widths of all of the cusps of Γ. (This case can, of course, only occur if $-1 \in \Gamma$ and is thus identical to the first case of Hsu's Theorem 3.1.)

- If N is a power of 2, let $S = L^{20}R^{\frac{1}{5}}L^{-4}R^{-1}$, where $\frac{1}{5}$ is the multiplicative inverse of 5 mod N. Then one may take $\mathcal{L}_N$ to consist of the three relations
$$\begin{aligned}(LR^{-1}L)^{-1}S(LR^{-1}L) &= S^{-1},\\ S^{-1}RS &= R^{25},\\ (SR^5LR^{-1}L)^3 &= (LR^{-1}L)^2.\end{aligned}$$
As in the previous case, this follows from the fact that
$$\left\langle L, R \;\middle|\; L^N = 1, (LR^{-1}L)^2 = (R^{-1}L)^3, (LR^{-1}L)^4 = 1, \mathcal{L}_N \right\rangle$$
is a presentation of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, by Lemma 3.4 of [Hsu96], and the first three relations are automatically satisfied in the permutation relation corresponding to Γ.
(Note that if we assume that $-1 \in \Gamma$, we may replace the last relation with $(SR^5LR^{-1}L)^3 = 1$, which is the relation appearing in Hsu's Theorem 3.1; but for odd subgroups we must use the slightly more complicated relation above.)
- If $N = em$ where e is a power of 2, m is odd and $e, m > 1$, then let c, d be the unique integers mod N such that $c = 0 \bmod e$, $c = 1 \bmod m$, $d = 1 \bmod e$, $d = 0 \bmod m$. Write $a = L^c, b = R^c, l = L^d, r = R^d$ and $s = l^{20}r^{\frac{1}{5}}l^{-4}r^{-1}$, where $\frac{1}{5}$ is interpreted mod e. Then we may take $\mathcal{L}_N$ to consist of the seven elements
$$\begin{aligned}[][a, r] &= 1,\\ (ab^{-1}a)^4 &= 1,\\ (ab^{-1}a)^2 &= (b^{-1}a)^3,\\ (ab^{-1}a)^2 &= (b^2a^{-\frac{1}{2}})^3,\\ (lr^{-1}l)^{-1}s(lr^{-1}l) &= s^{-1},\\ s^{-1}rs &= r^{25},\\ (lr^{-1}l)^2 &= (sr^5lr^{-1}l)^3.\end{aligned}$$
As in the previous two cases, this follows from the presentation of the group $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \cong \mathrm{SL}_2(\mathbf{Z}/e\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z}/m\mathbf{Z})$ given in [Hsu96, Lemma 3.5].

Acknowledgements. This paper is a much-condensed version of the first author's University of Warwick MMath dissertation, written in 2011-12 under the supervision of the second author. We are grateful to Vincent Delecroix for the original observation that Hsu's test should generalize to odd subgroups.

References

[BM68] Helmut Behr and Jens Mennicke, *A presentation of the groups* $\mathrm{PSL}(2, p)$, Canad. J. Math. **20** (1968), 1432–1438. MR 0236269.

[Hsu96] Tim Hsu, *Identifying congruence subgroups of the modular group*, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1351–1359. MR 1343700.

[KSV11] Ian Kiming, Matthias Schütt, and Helena A. Verrill, *Lifts of projective congruence groups*, J. Lond. Math. Soc. (2) **83** (2011), no. 1, 96–120. arXiv:0905.4798 MR 2763946.

(Hamilton) Premier Pensions Management, Corinthian House, 17 Lansdowne Road, Croydon CR0 2BX, UK

(Loeffler) Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
E-mail address: d.a.loeffler@warwick.ac.uk