CEU LECTURE NOTES: A SET OF REPRESENTATIVES FOR $\Gamma_0(q)\backslash \mathrm{SL}_2(\mathbb{Z})$

GERGELY HARCOS

Let q be a positive integer and $q = dd'$ a decomposition. For any residue class $c' \bmod d'$ satisfying $(c',d,d') = 1$ there is some $c \in \mathbb{Z}$ such that $(c,d) = 1$ and $c \equiv c' \pmod{d'}$. Indeed, by the Chinese remainder theorem, there exists $c \in \mathbb{Z}$ such that $c \equiv 1 \pmod{p}$ for any prime $p \mid d$ with $p \nmid d'$ and also $c \equiv c' \pmod{d'}$. We only need to verify that for any prime $p \mid d$ with $p \mid d'$ we have $p \nmid c$, but this follows from $p \nmid c'$ and $c \equiv c' \pmod{p}$.

Theorem. *For any $d \mid q$ take a set of integers c coprime with d which represent all residue classes $c' \bmod d'$ satisfying $(c',d,d') = 1$. Extend each such pair (c,d) to some matrix $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. The resulting matrices will represent $\Gamma_0(q)\backslash \mathrm{SL}_2(\mathbb{Z})$.*

Proof. We need to show that for any $\begin{pmatrix} * & * \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ there is a unique $\begin{pmatrix} * & * \\ c & d \end{pmatrix}$ in our set of matrices such that $\begin{pmatrix} * & * \\ C & D \end{pmatrix}\begin{pmatrix} * & * \\ c & d \end{pmatrix}^{-1} \in \Gamma_0(q)$. The condition can be rewritten as $cD \equiv Cd \pmod{q}$. In particular, it is necessary that $(d,q) = (D,q)$, hence by $d \mid q$, we must in fact take $d := (D,q)$. Writing $d' := q/d$ and $D' := D/d$, it remains to show that there is a unique c in our construction which satisfies $cD' \equiv C \pmod{d'}$. As $(D',d') = (D,q)/d = 1$, the previous congruence is equivalent to $c \equiv c' \pmod{d'}$, where $c' \bmod d'$ denotes the congruence class $C\overline{D'} \bmod d'$ with $\overline{D'}$ the inverse of $D' \bmod d'$. We clearly have $(c',d,d') = 1$ by $(C,D) = 1$ and $(\overline{D'},d') = 1$, hence there is a unique $c \equiv c' \pmod{d'}$ in our construction with the required properties. □

Corollary. *The index of $\Gamma_0(q)$ in $\mathrm{SL}_2(\mathbb{Z})$ equals*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(q)] = q\prod_{p\mid q}(1+p^{-1}).$$

Proof. The set of representatives in the Theorem has cardinality

$$\sum_{dd'=q}\ \sum_{\substack{c' \bmod d' \\ (c',d,d')=1}} 1 = \sum_{dd'=q}\ \sum_{c' \bmod d'}\ \sum_{r\mid(c',d,d')} \mu(r) = \sum_{r^2ee'=q} \mu(r) \sum_{f' \bmod e'} 1 = \sum_{r^2\mid q} \mu(r)\sigma\left(\frac{q}{r^2}\right),$$

where $\sigma(n)$ is the sum of divisors of n, and we used the notation $d = re$, $d' = re'$, $c' = rf'$. The sum on the right-hand side is multiplicative in q, and for a prime power $q = p^\alpha$ it equals $q(1+p^{-1})$ as can be seen by inspecting the cases $\alpha = 1$ and $\alpha \geqslant 2$ separately. The result follows. □

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest H-1364, Hungary
Email address: gharcos@renyi.hu