CEU LECTURE NOTES: ON THE CUSPS OF $\Gamma(q)$ AND $\Gamma_0(q)$

GERGELY HARCOS

Theorem 1. *Two cusps of* $\mathrm{SL}_2(\mathbb{Z})$, $\frac{u_1}{v_1}, \frac{u_2}{v_2} \in \mathbb{Q} \cup \{\infty\}$ *given in lowest terms, are equivalent under* $\Gamma(q)$ *if and only if* $\binom{u_1}{v_1} \equiv \pm \binom{u_2}{v_2} \bmod q$.

Proof. If $\frac{u_1}{v_1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \frac{u_2}{v_2} = \frac{au_2+bv_2}{cu_2+dv_2}$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(q)$, then $(au_2+bv_2, cu_2+dv_2) = 1$ shows that $\binom{u_1}{v_1} = \pm \binom{au_2+bv_2}{cu_2+dv_2} \equiv \pm \binom{u_2}{v_2} \bmod q$. For the converse we can assume $\binom{u_1}{v_1} \equiv \binom{u_2}{v_2} \bmod q$. We take some $\tau = \left(\begin{smallmatrix} u_2 & * \\ v_2 & * \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $\binom{u_1}{v_1} \equiv \tau \binom{1}{0} \bmod q$, so that $\binom{u}{v} := \tau^{-1} \binom{u_1}{v_1} \equiv \binom{1}{0} \bmod q$. There exists some $\sigma = \left(\begin{smallmatrix} u & v' \\ v & u' \end{smallmatrix}\right)$ in $\Gamma(q)$. Indeed, writing $u' = 1+qr$, $v' = qs$, there exist $r, s \in \mathbb{Z}$ such that $u(1+qr) - v(qs) = 1$, i.e. $ur - vs = (1-u)/q$, because $(u,v) = 1$ and $(1-u)/q \in \mathbb{Z}$. Now $\binom{u_1}{v_1} = \tau \binom{u}{v} = \tau\sigma \binom{1}{0} = \tau\sigma\tau^{-1} \binom{u_2}{v_2}$, where $\tau\sigma\tau^{-1}$ lies in $\Gamma(q)$, therefore $\frac{u_1}{v_1}$ and $\frac{u_2}{v_2}$ are equivalent under $\Gamma(q)$. □

Corollary 1. *The number of inequivalent cusps of* $\Gamma(q)$ *equals*

$$\begin{cases} 1 & \textit{for } q = 1, \\ 3 & \textit{for } q = 2, \\ \frac{1}{2} q^2 \sum_{p \mid q} (1 - p^{-2}) & \textit{for } q > 2. \end{cases}$$

Proof. For any coprime $u, v \in \mathbb{Z}$ the residue classes $u' := u \bmod q$ and $v' := v \bmod q$ satisfy $(u', v', q) = 1$. On the other hand, for any residue classes $u', v' \bmod q$ satisfying $(u', v', q) = 1$ there exist coprime $u, v \in \mathbb{Z}$ such that $u \equiv u' \pmod{q}$ and $v \equiv v' \pmod{q}$. Indeed, taking any $u \equiv u' \bmod q$ there exists $v \in \mathbb{Z}$ by the Chinese remainder theorem such that $v \equiv 1 \pmod{p}$ for any prime $p \mid u$ with $p \nmid q$ and also $v \equiv v' \pmod{q}$. Therefore the number of cusps of $\Gamma(q)$ equals the number of pairs $\left\{ \pm \left(\begin{smallmatrix} u \bmod q \\ v \bmod q \end{smallmatrix}\right) \right\}$ formed of residue classes $u, v \bmod q$ satisfying $(u, v, q) = 1$. For $q = 1, 2$ each pair consists of a single vector, hence the number of cusps is as stated. For $q > 2$ each pair consists of two vectors, hence the number of cusps is one-half of

$$\sum_{\substack{u,v \bmod q \\ (u,v,q)=1}} 1 = \sum_{u,v \bmod q} \sum_{d \mid (u,v,q)} \mu(d) = \sum_{d \mid q} \mu(d) \sum_{\substack{u,v \bmod q \\ d \mid u,v}} 1 = \sum_{d \mid q} \mu(d) \left(\frac{q}{d}\right)^2 = q^2 \sum_{p \mid q} \left(1 - \frac{1}{p^2}\right),$$

as stated. □

Theorem 2. *Two cusps of* $\mathrm{SL}_2(\mathbb{Z})$, $\frac{u_1}{v_1}, \frac{u_2}{v_2} \in \mathbb{Q} \cup \{\infty\}$ *given in lowest terms, are equivalent under* $\Gamma_0(q)$ *if and only if there exists* $v \mid q$ *such that* $(q, v_1) = (q, v_2) = v$ *and* $u_1 v_1 \equiv u_2 v_2 \pmod{(q, v^2)}$.

Proof. Fixing arbitrary elements $\left(\begin{smallmatrix} u_1 & \bar{v}_1 \\ v_1 & \bar{u}_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u_2 & \bar{v}_2 \\ v_2 & \bar{u}_2 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we need to examine the statement

$$\exists \gamma \in \Gamma_0(q) : \begin{pmatrix} u_1 & \bar{v}_1 \\ v_1 & \bar{u}_1 \end{pmatrix} \infty = \gamma \begin{pmatrix} u_2 & \bar{v}_2 \\ v_2 & \bar{u}_2 \end{pmatrix} \infty.$$

This is clearly

$$\begin{aligned}
&\iff \exists\gamma\in\Gamma_0(q) : \exists n\in\mathbb{Z} : \begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} = \begin{pmatrix}u_1 & \overline{v}_1\\ v_1 & \overline{u}_1\end{pmatrix}^{-1}\gamma\begin{pmatrix}u_2 & \overline{v}_2\\ v_2 & \overline{u}_2\end{pmatrix}\\
&\iff \exists n\in\mathbb{Z} : \begin{pmatrix}u_1 & \overline{v}_1\\ v_1 & \overline{u}_1\end{pmatrix}\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\begin{pmatrix}u_2 & \overline{v}_2\\ v_2 & \overline{u}_2\end{pmatrix}^{-1}\in\Gamma_0(q)\\
&\iff \exists n\in\mathbb{Z} : \begin{pmatrix}u_1 & \overline{v}_1+nu_1\\ v_1 & \overline{u}_1+nv_1\end{pmatrix}\begin{pmatrix}\overline{u}_2 & -\overline{v}_2\\ -v_2 & u_2\end{pmatrix}\in\Gamma_0(q)\\
&\iff \exists n\in\mathbb{Z} : \overline{u}_2v_1-\overline{u}_1v_2-nv_1v_2\equiv 0 \pmod{q}\\
&\iff \exists m,n\in\mathbb{Z} : \overline{u}_2v_1-\overline{u}_1v_2 = qm+nv_1v_2\\
&\iff \overline{u}_2v_1\equiv\overline{u}_1v_2 \pmod{(q,v_1v_2)}.
\end{aligned}$$

Let us examine the last condition. Observe that by $(\overline{u}_1,v_1)=(\overline{u}_2,v_2)=1$ the congruence forces $(q,v_1)\mid v_2$ and $(q,v_2)\mid v_1$, i.e. $(q,v_1)=(q,v_2)$. Denoting this common value by v and writing $q=vw$, the congruence becomes $\overline{u}_2v_1/v\equiv\overline{u}_1v_2/v \pmod{(w,v_1v_2/v)}$. Note that $(v_1/v,q/v)=(v_1,q)/v=1$ and $(v_2/v,q/v)=(v_2,q)/v=1$, i.e. both v_1/v and v_2/v are coprime to w. In particular, $v_1v_2/v=v(v_1/v)(v_2/v)$ shows that $(w,v_1v_2/v)=(w,v)$ and the congruence further simplifies to $\overline{u}_2v_1/v\equiv\overline{u}_1v_2/v \pmod{(w,v)}$. Note also that $u_1\overline{u}_1$ and $u_2\overline{u}_2$ are $\equiv 1 \pmod{v}$, hence the congruence is equivalent to $u_1v_1/v\equiv u_2v_2/v$ $\pmod{(w,v)}$. Multiplying this by v we obtain the congruence in the theorem. □

Corollary 2. *The number of inequivalent cusps of* $\Gamma_0(q)$ *equals* $\sum_{q=vw}\varphi((v,w))$.

Proof. For any decomposition $q=vw$ and any reduced residue class u' mod (v,w) we pick some $u\in\mathbb{Z}$ such that $(u,v)=1$ and $u\equiv u' \pmod{(v,w)}$. This exists by the Chinese remainder theorem, e.g. we can take $u\in\mathbb{Z}$ such that $u\equiv 1 \pmod{p}$ for any prime $p\mid v$ with $p\nmid w$ and also $u\equiv u' \pmod{(v,w)}$. By Theorem 2 (or its proof), the resulting rational numbers $\frac{u}{v}$ represent the $\Gamma_0(q)$-orbits of $\mathbb{Q}\cup\{\infty\}$, and their number equals $\sum_{q=vw}\varphi((v,w))$. □

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, POB 127, BUDAPEST H-1364, HUNGARY

E-mail address: gharcos@renyi.hu