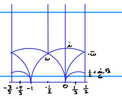
MODULAR FORMS



M. LALÍN

CONGRUENCE SUBGROUPS OF $SL_2(\mathbb{Z})$

So far we have discussed modular forms respect to all of $SL_2(\mathbb{Z})$. Sometimes it is useful to restrict to a particular subgroup.

Def: Let N be a positive integer. The **principal congruence subgroup of level** N is the group

$$\Gamma(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) \,\middle|\, \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

In other words, $\Gamma(N)$ is the kernel of the reduction $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$. It is a normal subgroup of finite index in $SL_2(\mathbb{Z}/N\mathbb{Z})$.

Prop: The reduction map is surjective.

Proof: Let $\gamma \in SL_2(\mathbb{Z}/N\mathbb{Z})$, and let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ that reduces to γ. We have that $ad - bc + mN = 1$ for some $m \in \mathbb{Z}$ and therefore $(a, b, N) = 1$. Then there is $h \in \mathbb{Z}$ such that $(a, b + hN) = 1$. Let $r, s \in \mathbb{Z}$ such that $m = ra - s(b + hN)$.

Now take $\gamma = \begin{pmatrix} a & b+hN \\ c+sN & d+rN \end{pmatrix}$. We have

$$\det(\gamma) = a(d+rN) - (b+hN)(c+sN) = ad - bc + (ra - s(b+hN))N$$
$$= 1 - mN + mN = 1.$$ and $\gamma \in SL_2(\mathbb{Z})$. #

Thus, there is an isomorphism $SL_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} SL_2(\mathbb{Z}/N\mathbb{Z})$ and $[SL_2(\mathbb{Z}) : \Gamma(N)] = \# SL_2(\mathbb{Z}/N\mathbb{Z})$.

Def: A **congruence subgroup** (of $SL_2(\mathbb{Z})$) is a subgroup $\Gamma \subset SL_2(\mathbb{Z})$ containing $\Gamma(N)$ for some $N \geq 1$. The least such N is called the **level** of Γ.

Every congruence subgroup has finite index. The converse is false.

Ex: $\Gamma_{4,3} = \left\langle \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \right\rangle$ has index 7.

Reference: Scholl, On the Hecke algebra of a noncongruent subgroup, Bull. London Math. Soc. 29 (1997) No 4. 395–399.

Ex: The most important examples

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, \begin{array}{l} a \equiv d \equiv 1 \pmod N \\ c \equiv 0 \pmod N \end{array} \right\}$$

and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod N \right\}$$

We have the inclusions $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z})$

Generally these inclusions are strict. All of them are $=$ for $N=1$ and $\Gamma_0(2)=\Gamma_1(2)$.

Ex: Show that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and that there is an isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow d \bmod N.$$

Proof: Consider the projection $\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow d \bmod N$. It is a morphism because $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ $\longrightarrow cb'+dd' \equiv dd' \pmod N$. The kernel is $d \equiv 1 \pmod N$ and since $ad-bc=1$ and $N|c$, it must have $a \equiv 1 \pmod N$. Thus $\Gamma_1(N) \triangleleft \Gamma_0(N)$. It is surjective because, given $d \pmod N$ a unit, we can find a such that $ad \equiv 1 \pmod N$ and $ad = 1+kN$. Thus take $c=N$, $b=k$. #

Both $\Gamma_0(N)$ and $\Gamma_1(N)$ have a "moduli interpretation".
For $\Gamma_0(N)$ one considers (Λ, G) with $\Lambda \subseteq \mathbb{C}$ a lattice and G a cyclic subgroup of order N of the quotient $\mathbb{C}/\Lambda$. Let Λ' be the inverse image of G in $\mathbb{C}$ with respect to the quotient $\mathbb{C} \longrightarrow \mathbb{C}/\Lambda$. Let (ω_1, ω_2) be a basis for Λ with the property that $(\omega_1, \frac{\omega_2}{N})$ is a basis for Λ'.
Then for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $(a\omega_1+b\omega_2, c\omega_1+d\omega_2)$ basis of Λ has this property iff c is divisible by N.
iff $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Restricting to $\omega_1/\omega_2 \in \mathbb{H}$ and taking the quotient by the action of $\Gamma_0(N)$, we obtain a bijection

$$\{(\Lambda, G)\}/\text{homothety} \xrightarrow{\sim} \Gamma_0(N)\backslash\mathbb{H}.$$

Similarly,

$$\{(\Lambda, P)\}/\text{homothety} \xrightarrow{\sim} \Gamma_1(N)\backslash\mathbb{H}$$

P: point of order N in the group $\mathbb{C}/\Lambda$.

Ex: Let D, N be positive integers and let β be a 2×2 matrix with integral entries and determinant D.
(i) Prove that $\beta\Gamma(DN)\beta^{-1}$ is contained in $\Gamma(N)$.
(ii) Prove that $\Gamma(N) \cap \beta^{-1}\Gamma(N)\beta$ contains $\Gamma(DN)$
(iii) Let Γ be any congruence subgroup, $\alpha \in GL_2^+(\mathbb{Q})$ Prove

that $\Gamma' = \Gamma \cap \alpha^{-1}\Gamma\alpha$ is again a congruence subgroup.

Proof: (i) Let $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $\beta^{-1} = \frac{1}{D}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. If $\gamma = \begin{pmatrix} a_1 & DNb_1 \\ DNc_1 & d_1 \end{pmatrix} \in \Gamma(DN)$, we have

$$D\beta\gamma\beta^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a_1 & DNb_1 \\ DNc_1 & d_1 \end{pmatrix}\cdot\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \quad \text{modulo } DN:$$

$$\equiv \begin{pmatrix} ada_1 - bcd_1 & -aba_1 + abd_1 \\ cda_1 - cdd_1 & -bca_1 + add_1 \end{pmatrix} \quad D = ad - bc:$$

$$\equiv \begin{pmatrix} ad(a_1 - d_1) + Dd_1 & -ab\,(a_1 - d_1) \\ cd\,(a_1 - d_1) & -bc\,(a_1 - d_1) + Dd_1 \end{pmatrix}$$

Since $a_1 \equiv d_1 \equiv 1 \pmod{DN}$ everything is divisible by D.

Also, modulo N, we get $\frac{1}{D}\begin{pmatrix} Dd_1 & 0 \\ 0 & Dd_1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ modulo N

(ii) $\beta\Gamma(DN)\beta^{-1} \subseteq \Gamma(N) \Rightarrow \Gamma(DN) \subseteq \beta^{-1}\Gamma(N)\beta$. Since $\Gamma(DN) \subseteq \Gamma(N) \Rightarrow \Gamma(DN) \subseteq \Gamma(N) \cap \beta^{-1}\Gamma(N)\beta$.

(iii) $\Gamma(N) \subseteq \Gamma$ $\alpha \in GL_2^+(\mathbb{Q})$. Thus $\alpha = \frac{1}{A}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}$

Take $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. $\det\beta = D$.

Then $\Gamma(DN) \subseteq \Gamma \cap \beta^{-1}\Gamma\beta = \Gamma \cap \alpha^{-1}\Gamma\alpha$ is a congruence subgroup. #

Def: Let f be a meromorphic function on $\mathbb{H}$, let $k \in \mathbb{Z}$ and Γ a congruence subgroup. We say that f is **weakly modular of weight k for the group Γ** (or of level Γ) if it satisfies the transformation formula $f|_k\gamma = f \quad \forall \gamma \in \Gamma$

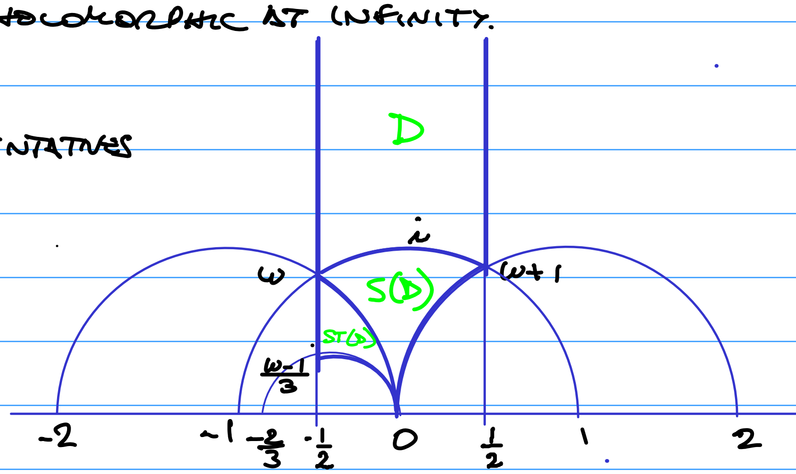
To generalize the definition of modular form, we need to generalize the notion of holomorphic at infinity.

Ex: Take $\Gamma = \Gamma_0(2) = \Gamma_1(2)$

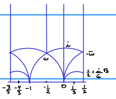
$\#SL_2(\mathbb{Z}/2\mathbb{Z}) = 6$

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

A system of coset representatives for $\Gamma \backslash SL_2(\mathbb{Z})$ is $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right\} = \{1, S, ST\}$. Using this, we can draw the fundamental domain for Γ.



There are two points "at infinity", the closure of D in the Riemann sphere, but not in $\mathbb{H}$: $\{0, \infty\}$



Fundamental domains and cusps

Prop: Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let R be a set of coset representatives for the quotient $\Gamma\backslash SL_2(\mathbb{Z})$. Then the set $D_\Gamma = \bigcup_{\gamma\in R}\gamma D$ has the property that for any $z\in\mathbb{H}$ there is a $\gamma\in\Gamma$ such that $\gamma z\in D_\Gamma$. Moreover, γ is unique up to multiplication by an element of $\Gamma\cap\{\pm 1\}$, except possibly if γz lies on ∂D.

Proof: Let $z\in\mathbb{H}$. There is $z_0\in D$, $\gamma_0\in SL_2(\mathbb{Z})$ such that $z=\gamma_0 z_0$. Since R is a set of coset representatives we can write $\gamma_0=\gamma^{-1}\gamma'$ with $\gamma\in\Gamma$ and $\gamma'\in R$ uniques. Thus,

$$\gamma z=\gamma\gamma_0 z_0=\gamma\gamma^{-1}\gamma' z_0=\gamma' z_0\in D_\Gamma$$

Suppose that $\gamma_1,\gamma_2\in\Gamma$ such that $\gamma_1 z,\gamma_2 z\in D_\Gamma$. Then there are $\gamma_1',\gamma_2'\in R$ such that $\gamma_i z\in\gamma_i' D$ or $\gamma_i'^{-1}\gamma_i z\in D$. If $\gamma_1 z\notin\partial D_\Gamma$, $\gamma_1'^{-1}\gamma_1 z\notin\partial D$ and its stabilizer in $SL_2(\mathbb{Z})$ is $\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}$. This implies that $\gamma_2'^{-1}\gamma_2\gamma_1^{-1}\gamma_1'=\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}$ or $\gamma_2\gamma_1^{-1}=\pm\gamma_2'\gamma_1'^{-1}\in\langle R\rangle\cap\Gamma=\{\pm 1\}\cap\Gamma$ #

Def: The **projective line over $\mathbb{Q}$** is the set

$$\mathbb{P}^1(\mathbb{Q})=\mathbb{Q}\cup\{\infty\}.$$

The group $SL_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$ by the same formula as the action on $\mathbb{H}$

$$\gamma t=\frac{at+b}{ct+d}\quad\text{for } \gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z}),\ t\in\mathbb{P}^1(\mathbb{Q}),$$

where $\gamma\infty=a/c$ and $\gamma t=\infty$ if $ct+d=0$.

Lemma: The action of $SL_2(\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Q})$ is transitive.

Proof: It suffices to show that $\forall t\in\mathbb{Q}$ there exists $\gamma\in SL_2(\mathbb{Z})$ such that $\gamma\infty=t$. Write $t=a/c$ with a,c coprime integers. Then there exist integers r,s such that $ar+cs=1$. Take $\gamma=\begin{pmatrix}a&-s\\c&r\end{pmatrix}$ #

Ex: It is easy to check that the stabilizer of ∞ in $SL_2(\mathbb{Z})$ is $SL_2(\mathbb{Z})_\infty=\left\{\pm\begin{pmatrix}1&b\\0&1\end{pmatrix}\,\middle|\,b\in\mathbb{Z}\right\}$

There is a bijection

$$SL_2(\mathbb{Z})/SL_2(\mathbb{Z})_\infty\xrightarrow{\sim}\mathbb{P}^1(\mathbb{Q})$$
$$\gamma SL_2(\mathbb{Z})_\infty\longmapsto\gamma\infty$$

Def: Let Γ be a congruence subgroup. The **set of cusps**

of Γ is the set of Γ-orbits in $\mathbb{P}^1(\mathbb{Q})$, i.e., the quotient

$$\mathrm{Cusps}(\Gamma) = \Gamma \backslash \mathbb{P}^1(\mathbb{Q})$$

or equivalently, $\mathrm{Cusps}(\Gamma) = \Gamma \backslash SL_2(\mathbb{Z}) / SL_2(\mathbb{Z})_\infty$

In particular, there is a surjective map

$$\Gamma \backslash SL_2(\mathbb{Z}) \twoheadrightarrow \mathrm{Cusps}(\Gamma)$$

Let c be a cusp of Γ and let t be an element of the corresponding Γ-orbit in $\mathbb{P}^1(\mathbb{Q})$. Let Γ_t be its stabilizer.

$$\Gamma_t = \{\gamma \in \Gamma \mid \gamma t = t\}.$$

We can choose $\gamma_t \in SL_2(\mathbb{Z})$ such that $\gamma_t \infty = t$.

Now for $\gamma \in \Gamma$ we have:

$$\gamma \in \Gamma_t \iff \gamma t = t \iff \gamma \gamma_t \infty = \gamma_t \infty \iff \gamma_t^{-1} \gamma \gamma_t \infty = \infty$$

$$\iff \gamma_t^{-1} \gamma \gamma_t \in SL_2(\mathbb{Z})_\infty.$$

This shows $\Gamma_t = \Gamma \cap \gamma_t SL_2(\mathbb{Z})_\infty \gamma_t^{-1}$

There is an injective map

$$\Gamma_t \backslash (\gamma_t SL_2(\mathbb{Z})_\infty \gamma_t^{-1}) \hookrightarrow \Gamma \backslash SL_2(\mathbb{Z})$$

Therefore Γ_t is of finite index in $\gamma_t SL_2(\mathbb{Z})_\infty \gamma_t^{-1}$

Define $H_c = \gamma_t^{-1} \Gamma \gamma_t \cap SL_2(\mathbb{Z})_\infty$

Hence H_c is a subgroup of finite index in $SL_2(\mathbb{Z})_\infty$.

Ex: The definition of H_c is independent of the choice of t and γ_t

Proof: Let s be an element in the same cusp as t. Thus, there is $\gamma \in \Gamma$ such that $\gamma s = t$. We can take $\gamma_s = \gamma \gamma_t$. Now $\gamma_s^{-1} \Gamma \gamma_s = \gamma_t^{-1} \gamma^{-1} \Gamma \gamma \gamma_t = \gamma_t^{-1} \Gamma \gamma_t$. (This proof applies even when $s = t$ but $\gamma_s \neq \gamma_t$.) #

Ex: Let H be a subgroup of finite index in $SL_2(\mathbb{Z})_\infty$. Show that H is one of the following.

(i) Infinite cyclic generated by $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ with $h \geq 1$.

(ii) Infinite cyclic generated by $\begin{pmatrix} -1 & h \\ 0 & -1 \end{pmatrix}$ with $h \geq 1$

(iii) Isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, generated by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$

Show that h is the index of $\{\pm 1\}H$ in $SL_2(\mathbb{Z})_\infty$.

Proof: Since $SL_2(\mathbb{Z})_\infty = \{\pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}\}$, and $H \leq SL_2(\mathbb{Z})_\infty$

Let $h = \min \{|b| \neq 0 \mid \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H\}$. Since $H \neq \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$, h is

We use the key identities: $\begin{pmatrix}1&a\\0&1\end{pmatrix}\begin{pmatrix}1&b\\0&1\end{pmatrix}=\begin{pmatrix}1&a+b\\0&1\end{pmatrix}$

well-defined. $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&h\\0&1\end{pmatrix}=\begin{pmatrix}-1&-h\\0&-1\end{pmatrix}$

Case (i) $\begin{pmatrix}1&h\\0&1\end{pmatrix}\in H$, $\begin{pmatrix}-1&h\\0&-1\end{pmatrix}\notin H$. If $\begin{pmatrix}1&b\\0&1\end{pmatrix}\in H$, divide b by h, conclude $h\mid b$. If $\begin{pmatrix}-1&b\\0&-1\end{pmatrix}$, we get that $\begin{pmatrix}-1&h\\0&-1\end{pmatrix}\in H$ a contradiction

$H=\left\langle\begin{pmatrix}1&h\\0&1\end{pmatrix}\right\rangle$.

Case (ii) $\begin{pmatrix}-1&h\\0&-1\end{pmatrix}\in H$, $\begin{pmatrix}1&h\\0&1\end{pmatrix}\notin H$. Similar.

Case (iii) $\begin{pmatrix}1&h\\0&1\end{pmatrix}, \begin{pmatrix}-1&h\\0&-1\end{pmatrix}\in H$. Thus $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\in H$.

h is index $=\#\left\{\begin{pmatrix}1&a\\0&1\end{pmatrix} \;0\leq a<h\right\}$.

__Def:__ Let $c\in \text{Cusps}(\Gamma)$, and let t be an element of the corresponding Γ-orbit in $\mathbb{P}^1(\mathbb{Q})$. The **width** of c, denoted $h_\Gamma(c)$ is the integer h defined given above. For $H=H_c$, i.e. the index of $\{\pm1\}H$ in $SL_2(\mathbb{Z})_\infty$. The cusp c is called **irregular** if $\gamma_t^{-1}\Gamma_t\gamma_t$ is of the form (ii). and **regular** otherwise.

__Rem__ If Γ is a normal congruence subgroup of $SL_2(\mathbb{Z})$, since $\gamma^{-1}\Gamma\gamma=\Gamma$, then all the cusps have the same width, and they are all regular or all irregular.

__Lemma:__ Let G be a group acting transitively on a set X and let H be a subgroup of finite index in G.

(i) For any $x\in X$, the stabilizer $\text{Stab}_H x$ has finite index in $\text{Stab}_G x$ and we have an injection

$$(\text{Stab}_H x)\backslash(\text{Stab}_G x)\hookrightarrow H\backslash G$$

with image $H\backslash H\,\text{Stab}_G x$.

(ii) Let $x_0\in X$. There is a surjective map

$$H\backslash G\twoheadrightarrow H\backslash X,\quad Hg\longrightarrow Hgx_0.$$

And for every $x\in X$ the cardinality of the fibre of this map over Hx equals $[\text{Stab}_G x:\text{Stab}_H x]$

(iii) If R is a set of orbit representatives for the quotient $H\backslash X$, we have $\sum_{x\in R}[\text{Stab}_G x:\text{Stab}_H x]=[G:H]$

__Proof:__ (i) Standard.

(ii) Since the action is transitive, $\forall x\in X$, we can choose $g_x\in G$ such that $g_x x_0=x$. Thus the map is surjective.
Let Y_{Hx} denote the fibre over Hx.

$T_{Hx} = \{ Hg \in H\backslash G \mid Hg\, x_0 = Hx \}$

Replacing Hg by $Hg'g_x$ we get

$T_{Hx} \simeq \{ Hg' \in H\backslash G \mid Hg'g_x x_0 = Hx \}$

$\simeq \{ Hg' \in H\backslash G \mid Hg'x = Hx \} = H \backslash (H\, \mathrm{Stab}_G x)$ by (ii),

$\simeq (\mathrm{Stab}_H x) \backslash (\mathrm{Stab}_G x)$.

(iii) Summing over a system of representatives R for the quotient $H\backslash X$, we obtain,

$$[G:H] = \#(H\backslash G) = \sum_{x\in R} \# T_{Hx} = \sum_{x \in R} [\mathrm{Stab}_G x : \mathrm{Stab}_H x] \quad \#.$$

Coro: Let Γ be a congruence subgroup and let $\overline{\Gamma}$ be the image of Γ in $PSL_2(\mathbb{Z})$. Then

$$\sum_{c \in Cusps(\Gamma)} h_\Gamma(c) = [PSL_2(\mathbb{Z}) : \overline{\Gamma}] = [SL_2(\mathbb{Z}) : \{\pm 1\}\Gamma]$$

Proof: Apply Lemma (iii) to $G = PSL_2(\mathbb{Z})$, $H = \overline{\Gamma}$, $X = \mathbb{P}^1(\mathbb{Q})$

Ex: Let p be a prime number. Consider $\Gamma = \Gamma_0(p)$. We remark that $\Gamma(p) \subseteq \Gamma_0(p)$ and that there is an isomorphism

$$\Gamma_0(p) \backslash SL_2(\mathbb{Z}) \xrightarrow{\sim} k_p \backslash SL_2(\mathbb{F}_p),$$

where $k_p = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p) \mid c = 0 \} = \{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \}$

Indeed, let $\gamma \in SL_2(\mathbb{Z})$ $\Gamma_0(p)\gamma \longrightarrow k_p$, in other words, $\gamma \pmod p \in k_p$. But this means $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $p | c \Rightarrow \gamma \in \Gamma_0(p)$.

It is known that $\# SL_2(\mathbb{F}_p) = p(p-1)(p+1)$

and $\# k_p = p(p-1)$. Indeed, $\# k_p$ is obvious and

$GL_2(\mathbb{F}_p) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a \\ c \end{pmatrix}$ and $\begin{pmatrix} b \\ d \end{pmatrix}$ are LI $\} \Rightarrow$

$\# GL_2(\mathbb{F}_p) = (p^2-1)(p^2-1-(p-1)) = (p^2-1)(p^2-p)$

$[GL_2(\mathbb{F}_p) : SL_2(\mathbb{F}_p)] = p-1 \Rightarrow \# SL_2(\mathbb{F}_p) = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1)$

Therefore, we have, $[SL_2(\mathbb{Z}) : \Gamma] = [SL_2(\mathbb{F}_p) : k_p] = \frac{\# SL_2(\mathbb{F}_p)}{\# k_p}$

$= \frac{p(p-1)(p+1)}{p(p-1)} = p+1$

To compute the set of cusps of Γ, we find the orbits.

$\Gamma \infty = \{ \begin{pmatrix} a & b \\ cp & d \end{pmatrix} \infty \mid a,b,c,d \in \mathbb{Z},\ ad - bcp = 1 \}$

$= \{ \frac{a}{cp} \mid a, c \in \mathbb{Z},\ (a, cp) = 1 \} = \{ \frac{r}{s} \mid r, s \in \mathbb{Z},\ (r,s) = 1,\ p | s \}$.

M. Lalín

(A fraction with denominator 0 is interpreted as ∞.)

$$\Gamma\cdot 0 = \left\{ \begin{pmatrix} a & b \\ cp & d\end{pmatrix} 0 \;\middle|\; a,b,c,d\in\mathbb{Z},\ ad-bcp=1\right\}$$

$$= \left\{ \frac{b}{d} \;\middle|\; b,d \in \mathbb{Z},\ (b,d)=1\ \ p\nmid d\right\}$$

It is clear that every element of $\mathbb{P}^1(\mathbb{Q})$ is in either $\Gamma\cdot\infty$ or $\Gamma\cdot 0$. Thus $\Gamma_0(p)$ has two cusps, namely, $[\infty],[0]\in \Gamma_0(p)\backslash\mathbb{P}^1(\mathbb{Q})$.

We find the widths. For $\mathfrak{c}=[\infty]$, we take $t=\infty$ and $\gamma_t = \begin{pmatrix}1&0\\0&1\end{pmatrix}$.

Therefore $H_\mathfrak{c} = SL_2(\mathbb{Z})_\infty$ and $h_\Gamma(\mathfrak{c})=1$. For $\mathfrak{c}=[0]$, we take $t=0$ and $\gamma_t=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$. We have

$$\Gamma_t = \left\{\pm\begin{pmatrix}1&0\\cp&1\end{pmatrix} \;\middle|\; c\in\mathbb{Z}\right\} \text{ and } H_\mathfrak{c}=\left\{\pm\begin{pmatrix}1&cp\\0&1\end{pmatrix}\;\middle|\; c\in\mathbb{Z}\right\}.$$

Thus $h_\Gamma(\mathfrak{c})=p$.