TALK 1

MODULAR CURVES

– Vinay Deolalikar

In this talk, we will discuss the action of the modular group Γ & it's congruence subgroups on the upper half plane $\mathbb{H}$ (also known as the 'hyperbolic plane'). We will study the quotients by this action $\Gamma(N)\backslash \mathbb{H} \triangleq Y(N)$ and it's natural compactification $X(N)$.

<u>FUCHSIAN GROUPS</u>: A Discrete subgroup of $SL_2(\mathbb{R})$ is called a 'Fuchsian Group'. While discrete subgroups of $SL_2(\mathbb{R})$ abound, the ones that correspond to $SL_2(\mathbb{Z})$ & it's congruence subgroups are of interest to number theorists.

<u>Definition</u>: Let $\Gamma \triangleq SL_2(\mathbb{Z})$. The 'principal congruence subgroup' of Γ of level N is

$$\Gamma(N) \triangleq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{array}{l} a \equiv d \equiv 1 \\ b \equiv c \equiv 0 \end{array} (\text{mod } N) \right\}$$

In other words, $\Gamma(N)$ consists of those matrices in Γ that are congruent to the identity matrix, mod N. Another way to look at it is that $\Gamma(N)$ is the kernel of the natural map

$$SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z}).$$

This immediately tells us that $\Gamma(N)$ is a normal subgroup of Γ.

Remark: Clearly, $\Gamma = \Gamma(1)$

Definition: A subgroup of Γ is called a 'congruence subgroup of level N' if it contains $\Gamma(N)$

Remark: A subgroup of level N also has level N', where $N \mid N'$. (Thus $\Gamma(N) \supset \Gamma(N')$)

The most important congruence subgroups for our point of view are

$$\Gamma_0(N) \triangleq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \pmod N \right\}$$

$$\Gamma_1(N) \triangleq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv 1 \pmod N \right\}$$

Remark: $\Gamma(N) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}$; $\Gamma_0(N) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

There are other discrete subgroups that come from Quaternion algebras, but we won't get into them here.

CLASSIFICATIONS OF LINEAR FRACTIONAL TRANSFORMS:

We let $\overset{\alpha}{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \in SL_2(\mathbb{R})$ act on $z \in \mathbb{C}$

by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \dfrac{az+b}{cz+d}$.

These mappings are called linear fractional transformations of $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. They map lines $\to$ lines & circles $\to$ circles.

By the Theory of Jordan Canonical Forms; each α is conjugate to a matrix of the form:

(i) $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ or (ii) $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ $\lambda \neq \mu$

(2 identical eigenvalues) (2 distinct eigenvalues)

In case (i) α is of form $z \mapsto z + \lambda^{-1}$ & in case (ii) it is of form $z \mapsto cz$, $c \neq 1$.
Case (i) is called 'parabolic'. Case (ii) is called 'elliptic' if $|c| = 1$; 'hyperbolic' if c is real & +ve; & 'loxodromic' otherwise.

Now if $\alpha \in SL_2(\mathbb{R})$

(i) <u>α Parabolic</u>: $\therefore$ α has only one real eigenvector, call it $\begin{pmatrix} e \\ f \end{pmatrix}$. If $f \neq 0$; α has a fixed pt in $\mathbb{R}$, else ∞ is the fixed pt.

(ii) <u>α elliptic</u>: α has 2 cmplx conjugate eigenvectors. Thus α has a fixed pt in $\mathbb{H}$ & one in $\overline{\mathbb{H}}$.

α hyperbolic: α has 2 distinct Real eigenvalues & $\therefore$ 2 distinct fixed points in $\mathbb{R} \cup \{\infty\}$.

Definition: Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$. Then a point $z \in \mathbb{H}$ is called an elliptic point if it is the fixed pt of an elliptic element of Γ; & a point $s \in \mathbb{R} \cup \{\infty\}$ is called a cusp if it is the fixed point of an parabolic element in Γ.

Q: What are the cusps & elliptic points for $\Gamma(1) = SL_2(\mathbb{Z})$?

Ans: The cusps for $\Gamma(1)$ are all the points $\mathbb{Q} \cup \{\infty\}$ and they form one equivalence class under $\Gamma(1)$ action. For let $\frac{m}{n} \in \mathbb{Q}$ gcd $(m,n)=1$, $\exists$ a, b s.t $am + bn = 1$. Thus $\gamma = \begin{pmatrix} m & a \\ n & b \end{pmatrix}$ acts on ∞ to give

$$\frac{m\infty + a}{n\infty + b} = \frac{m}{n}.$$ Also $\frac{m}{n}$ is the fixed point of $\gamma \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \gamma^{-1}$, which is a parabolic element in $\Gamma(1)$. Conversely, every parabolic element of $\Gamma(1)$ has $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ as its JCF.

The elliptic points γ of $\Gamma(1)$ have charact. polynomial of degree 2, & its roots are roots of unity (since γ has finite order). But since the only roots of unity lying in a quadratic extension are those of order dividing 4 or 6, every elliptic point of $\mathbb{H}$

is $\Gamma(1)$ equivalent to i or $\rho \left(= \sqrt[3]{1}\right)$.
$\left(= \frac{1+i\sqrt{3}}{2}\right)$.

Q. What are cusps & elliptic points for $\Gamma \triangleleft \Gamma(1)$ of finite index?

Ans: cusps of Γ are those of $\Gamma(1)$, but now may fall in more than one Γ-equivalence class. Elliptic points of Γ are elliptic for $\Gamma(1)$. An elliptic pt of $\Gamma(1)$ is an elliptic point of $\Gamma \iff$ it is fixed by an element of Γ other than $\pm I$.

FUNDAMENTAL DOMAINS

Definition: A ~~[illegible]~~ open region $D \subset \mathbb{H}$ is a 'fundamental domain' for the action of Γ on $\mathbb{H}$ if every $z \in \mathbb{H}$ is Γ-equivalent to some point in D, but no two distinct points $z_1; z_2$ in ~~[illegible] interior of~~ D are Γ-equivalent (points on the boundary of $\bar{D}$ can be).

Before we derive the fundamental domain for $\Gamma(1)$, let us first look at the structure of $\Gamma(1)$.

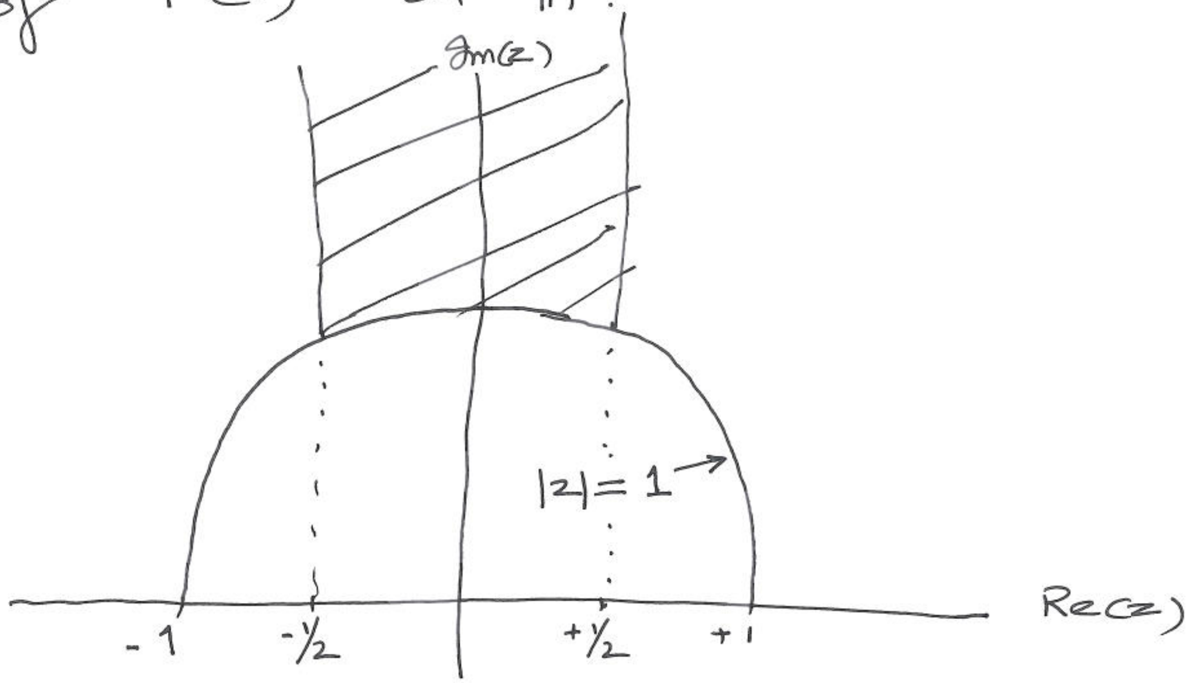
Proposition: $\Gamma(1)$ is generated by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ with}$$

relations $S^2 = (ST)^3 = 1$.

Theorem: Let $D = \left\{ z \in \mathbb{H} : \begin{array}{l} |z| \geq 1 \\ |Re(z)| \leq 1/2 \end{array} \right\}$

i) Then D is the fundamental domain for the action of $\Gamma(1)$ on $\mathbb{H}$.



(ii) $\mathrm{Stab}(i) = \langle S \rangle$, which has order 2

(iii) $\mathrm{Stab}(\rho) = \langle TS \rangle$, which has order 3

(iv) $\mathrm{Stab}(\rho^2) = \langle ST \rangle$, " " " "

(v) 2 elements in $\bar{D}$ are equivalent iff

$z' = Tz$ or $Tz' = z$

OR

$z' = Sz$ or $Sz' = z$

Sketch of proofs: To bring an element $z \in \mathbb{H}$ into the strip $|Re(z)| < 1/2$; act upon it T or T^{-1} sufficiently many times. If the resulting image has magnitude > 1, we are done, else act S upon it sufficiently many times

This works as follows:

$$\mathrm{Im}(Sz) = \frac{\mathrm{Im}(z)}{|z|^2} > \mathrm{Im}(z) \text{ if } |z|<1.$$

However, to know that this does eventually land us in the region $|z|>1$, we need the following result:

<u>Lemma</u>: For fixed $z \in \mathbb{H}$ & N a +ve integer, there are only finitely many pairs of integers (c,d) s.t

$$|cz+d| \leq N.$$

Proof: let (c,d) be such a pair & $z=x+iy$

$$|cz+d|^2 = (cx+d)^2 + c^2y^2$$

$$\Rightarrow \quad c^2y^2 < (cx+d)^2 + c^2y^2 \leq N$$

but since $z \in \mathbb{H}$, $y>0$ & so $|c| \leq \frac{N}{y}$ meaning there are only finitely many such c. For each such c,

$$(cx+d)^2 + c^2y^2 \leq N \Rightarrow \text{only finitely many } d!$$

. QED

The verification of the other statements in the Theorem is fairly easy.

FUNDAMENTAL DOMAINS FOR CONGRUENCE SUBGROUPS:

Theorem: Let Γ be any discrete subgroup of $SL_2(\mathbb{R})$ and D be it's fundamental domain. Let Γ' be a subgroup of Γ of finite index. Let

$$\Gamma = \Gamma'\gamma_1 \cup \Gamma'\gamma_2 \cup \ldots \cup \Gamma'\gamma_m$$

be a disjoint union of right cosets of Γ'. Then $D' \triangleq \cup \gamma_i D$ is the fundamental domain for Γ'.

Proof: Let $z \in \mathbb{H}$. Then $z = \gamma z'$ for some $z' \in \overline{D}$, $\gamma \in \Gamma$. But $\gamma = \gamma'\gamma_i$ for some γ_i. Thus $z = \gamma'\gamma_i z \in \Gamma'(\gamma_i \overline{D})$ & $\gamma' \in \Gamma'$

Now if $\gamma D' \cap D \neq \phi$, then it contains a transform of D. But then $\gamma\gamma_i D = \gamma_j D$ for some $i \neq j \Rightarrow \gamma\gamma_i = \gamma_j$. This is a contradiction.

. QED

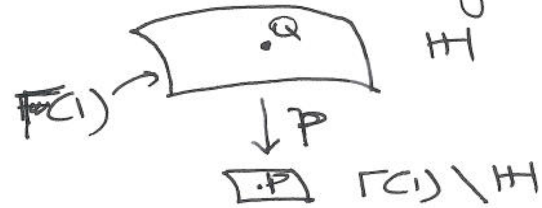
DEFINING COMPLEX STRUCTURES ON QUOTIENTS.

I : $\Gamma(1)\backslash\mathbb{H}$:

There is a complex structure on $\mathbb{H}$, trivially.

let $p : \mathbb{H} \longrightarrow \Gamma(1)\backslash\mathbb{H}$

$Q \longmapsto P$



If Q is not an elliptic point, we can choose a neighbourhood U of Q s.t $p : U \to p(U)$ is a homeomorphism. Then $(p(U), p^{-1})$ is a coordinate neighbourhood of P.

If Q is $\Gamma(1)$ equivalent to i, we might as well take it to be i. Then the map $z \longmapsto \dfrac{z-i}{z+i}$ take open Disk D with center i to open disk D with center 0. $\dfrac{z-i}{z+i}$ is a holomorphic function defined in a nbd of i & S maps it to

$$\frac{-z^{-1}-i}{-z^{-1}+i} = -\left(\frac{z-i}{z+i}\right).$$

Thus $z \mapsto \left(\dfrac{z-i}{z+i}\right)^2$ is a S-invariant holomorphic function defined in a nbd of i $\Rightarrow$ it is a holomorphic function in a nbd of $P(i)$. Thus we take it to be the coordinate function near $P(i)$

We treat $Q = \rho^2$ the same way.

$z \mapsto \frac{z-\rho^2}{z-\bar{\rho}^2}$ takes a disk centered at ρ^2 to a disk centered at 0. &

$$z \longmapsto \left(\frac{z-\rho^2}{z-\bar{\rho}^2}\right)^3 \text{ is invariant under } ST.$$

It is $\therefore$ a ST- invariant function near $P(\rho^2)$.

Problem: The Riemann Surface we obtain $\Gamma(1) \setminus \mathbb{H}$ is <u>not</u> compact.

Solution: We add to it, a point ∞. Map a nbd $U = \{ z \in \mathbb{H} \; ; \; \operatorname{Im}(z) > N \}$ of ∞ to a open disk V centered at 0 by $z \mapsto e^{2\pi i z}$. This is a holomorphic function invariant under the stabilizer T of ∞ & so defines a holomorphic function near $p(\infty)$.

Alternatively, we can start with $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$

<u>Theorem:</u> The Riemann surface $\Gamma(1) \setminus \mathbb{H}^*$ is compact and of genus zero.

Proof: triangulate it & use the fact that

$$2 - 2g = h_0 - h_1 + h_2$$
$$= 4 - 6 + 4 = 2$$
$$\Rightarrow g = 0$$

COMPLEX STRUCTURE ON $\Gamma \backslash \mathbb{H}^*$

($\Gamma \subset \Gamma(1)$ of finite index)

Notation:

$$Y(\Gamma) = \Gamma \backslash \mathbb{H}$$

$$X(\Gamma) = \Gamma \backslash \mathbb{H}^* = \text{compactification of } Y(\Gamma)$$

modular curves

$$Y(N) = Y(\Gamma(N))$$

$$X(N) = X(\Gamma(N))$$

$$X_0(N) = X(\Gamma_0(N))$$

$$X_1(N) = X(\Gamma_1(N))$$

We define a complex structure on $X(N)$ & $Y(N)$ the same way as on $X(1)$ & $Y(1)$. Note that ∞ always remains a cusp since $\Gamma(N)$ contains T^h for some h & then T^h is a parabolic element fixing ∞. Now if h is the smallest such, $q = e^{\frac{2\pi i z}{h}}$ is a coordinate function near ∞.

With the above complex structures, the $X(N)$, $Y(N)$, $X_0(N)$, $Y_0(N)$ are all Riemann Surfaces of algebraic curves, called <u>ELLIPTIC MODULAR CURVES</u>.

GENERA OF MODULAR CURVES $X(\Gamma)$.

Consider the covering

$$\begin{array}{c} X(\Gamma) \\ \Big\downarrow \text{degree } m. \\ X(\Gamma(1)) = X(1) \end{array}$$

Then Riemann Hurwitz Formula (sometimes also called "Hurwitz-Zeuthen")

$$2g_{X(\Gamma)}-2 = m\,(2g_{X(1)}-2) + \sum (e_p - 1)$$

$$2g_{X(\Gamma)}-2 = -2m + \sum (e_p - 1)$$

<u>Theorem:</u> Let Γ be a subgroup of $\Gamma(1)$ of finite index m. Let

ν_2 = # of inequivalent elliptic pts of order 2

ν_3 = " " " " " of order 3

ν_∞ = # of inequivalent cusps.

Then the genus of $X(\Gamma)$ is

$$g_{X(\Gamma)} = 1 + \frac{m}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

Proof:

$$\begin{tikzcd} \mathbb{H}^* \arrow[r] \arrow[d, "p"'] & \Gamma\backslash\mathbb{H}^* \arrow[dl, "\varphi"] \\ \Gamma(1)\backslash\mathbb{H}^* & \end{tikzcd}$$

$$Q \longmapsto p', \qquad p' \longmapsto p$$

Then $e(Q/P) = e(Q/P') \cdot e(P'/P)$
(ramification indices multiply).

Suppose Q is $\Gamma(1)$-equivalent to i ($\therefore e(Q/P) = 2$)
$\therefore$ either $e(Q/P') = 2$ & $e(P'/P) = 1$ $\Longrightarrow$ Q is elliptic for Γ, P' unramified over P

OR

$e(Q/P') = 1$ & $e(P'/P) = 2$

$\Longrightarrow$ Q is not elliptic.

There are ν_2 points P' of first type
$\left(\frac{m-\nu_2}{2}\right)$ points of second type

$$\therefore \sum (e_{P'} - 1) = \left(\frac{m-\nu_2}{2}\right)$$

Similarly, if Q is $\Gamma(1)$-equivalent to ρ.
either $e(Q/P') = 3$ & $e(P'/P) = 1$

OR

$e(Q/P') = 1$ & $e(P'/P) = 3$

There are ν_3 points P' of first type &
$\left(\frac{m-\nu_3}{3}\right)$ points of 2^{nd} type

$$\therefore \sum (e_{P'} - 1) = 2\left(\frac{m-\nu_3}{3}\right)$$

If Q is a cusp for Γ, there are ν_∞ pts P' and $\sum e_i = m \Rightarrow \sum e_i - 1 = m - \nu_\infty$

Adding all of these $\sum(e_{p_i} - 1)$ terms in the 3 cases & substituting in the Riemann Hurwitz genus formula, we get our result. QED

INDEX OF $\Gamma(N)$ in $\Gamma(1)$

Now all we need is the index of $\Gamma(N)$ in $\Gamma(1)$. Recall that $\Gamma(N)$ is the kernel of the natural map

$$\Gamma = SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/_N\mathbb{Z})$$

$\therefore$ the index of $\Gamma(N)$ in $\Gamma(1)$ is just the order of $SL_2(\mathbb{Z}/N\mathbb{Z})$.

Consider the following facts: Let $N = \prod p_i^{r_i}$

(a) $GL_2(\mathbb{Z}/N\mathbb{Z}) \approx \prod GL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$

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

(c) Kernel of $GL_2(\mathbb{Z}/p^r\mathbb{Z}) \to GL_2(\mathbb{F}_p)$ is all matrices of form $I + p\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{Z}/p^{r-1}\mathbb{Z}$. $\therefore$ order of $GL_2(\mathbb{Z}/p^r\mathbb{Z})$ is $(p^{r-1})^4 (p^2-1)(p^2-p)$

(d) $|GL_2(\mathbb{Z}/p^r\mathbb{Z})| = \varphi(p^r)\, SL_2(\mathbb{Z}/p^r\mathbb{Z})$

From (a) to (d), we get

$$(\Gamma(1) : \Gamma(N)) = |SL_2(\mathbb{Z}/N\mathbb{Z})|$$

$$= N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

Q: What are values of ν_2, ν_3 & ν_∞?

Ans: If $N > 1$, $\Gamma(N)$ has no elliptic points at all (thus $\nu_2 = \nu_3 = 0$)! Indeed $\Gamma(N)$ has no torsion. Because the only torsion in $\Gamma(1)$ is $S, ST, (ST)^2$ & conjugates thereof. But $S, ST, (ST)^2 \notin \Gamma(N)$ & since $\Gamma(N)$ is a normal subgroup, neither are the conjugates of S, ST & $(ST)^2$ in $\Gamma(N)$.

Number of inequivalent cusps is μ_N / N

Where $\mu_N = (\bar{\Gamma}(1) : \bar{\Gamma}(N))$

$$= (\Gamma(1) : \Gamma(N)) / 2$$

[here $\bar{\Gamma}$ is image of Γ in $\Gamma(1)/\pm I$.]

$\therefore$ genus of $\Gamma(N) / \mathbb{H}^* = X(N)$

is $g_{X(N)} = 1 + \mu_N \cdot \dfrac{(N-6)}{12N}$ $N > 1$