Last time: $SL_2(\mathbb{Z}) \circlearrowright \mathbb{H}$ via Lean. (K. Heather Macbeth)

Want fund dom for action. $SL_2(\mathbb{R}) \circlearrowright \mathbb{H}$ ($\mathbb{P}^1$).

$\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$. fractional-linear action. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ z = \dfrac{az+b}{cz+d}$. linear action.

- $I \circ z = z$. ✓
- $(g_1 \cdot g_2) \circ z = g_1 \circ (g_2 \circ z)$ ✓ nasty as fract linear but follows immediately from assoc of matrix mult.
- $g \circ z \in \mathbb{H}$.

Need $\operatorname{Im} g \circ z$

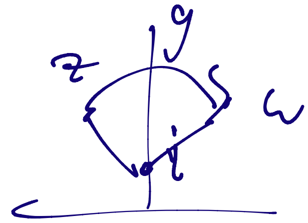
$$\frac{(az+b)(c\bar{z}+d)}{(cz+d)(c\bar{z}+d)} = \frac{ac|z|^2 + adz + bc\bar{z} + bd}{|cz+d|^2 > 0} \quad \left(z \neq -\frac{d}{c} \in \mathbb{R}\right)$$

$\Rightarrow \operatorname{Im} g \circ z = \dfrac{\det g \cdot \operatorname{Im} z}{|cz+d|^2} > 0$. In fact, $GL_2^+(\mathbb{R}) \circlearrowright \mathbb{H}$ ; $G$

(conn component det $> 0$.)

Is action transitive?

$\forall z, w \in \mathbb{H}$ $\exists g \in G$ with $gz = w$.




Enough to move $i$ to any point.

$(y > 0)$ $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \circ i = \dfrac{iy + x}{0 \cdot i + 1} = x + iy$. ✓

$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}y & 0\\ 0 & 1\end{pmatrix}$

→ unipotent, diagonal

action: $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} \circ z \mapsto z+x$. translations

action $\begin{pmatrix}y & 0\\ 0 & 1\end{pmatrix} \circ z = y \cdot z$ dilation.

$G = GL_2^+(\mathbb{R})$

$Z = \{ z \in G \mid \forall g \in G,\ zg = gz \}$ Zentrum

$= \left\{ \begin{pmatrix}d & 0\\ 0 & d\end{pmatrix},\ d \in \mathbb{R}^\times \right\}$

$N = \left\{ \begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix} \right\}$. "$\exp \begin{pmatrix}0 & x\\ 0 & 0\end{pmatrix}$" nilpotent

$A = \left\{ \begin{pmatrix}* & 0\\ 0 & *\end{pmatrix} \right\}$ abelian.

$\frac{ai+b}{ci+d} = i$, $ai+b = -c+id$

$\mathrm{Stab}_G\, i = \{ g \in G : g \circ i = i \}$

$= Z \cdot K$

$\begin{pmatrix}a & b\\ -b & a\end{pmatrix}$, $a^2+b^2 \neq 0$, $a^2+b^2=1$

$K = SO(2) = \left\{ \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix} \right\}$ Kompakt.

"Iwasawa" decomposition $G = NAK \cdot Z$ (QR decomp)

$g \cdot R = \begin{pmatrix}x & x\\ 0 & x\end{pmatrix}$.
$g \in GL(n)$, $R$ ... $O(n)$

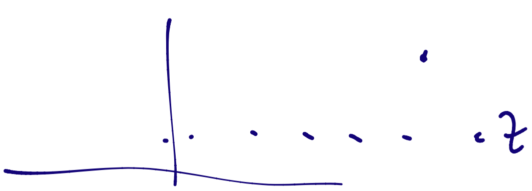
$\mathbb{H} = G/K \cdot Z$.

Haar measure $d\mu(z) = \frac{dx\,dy}{y^2}$.

$\Gamma < G$
$SL_2(\mathbb{Z})$

Want 1: Siegel Domain: $R \subseteq \mathbb{H}$ s.t.

$\forall z \in \mathbb{H}, \exists \gamma \in \Gamma$ s.t. $\gamma z \in R$. & $\mathrm{vol}(R) < \infty$.

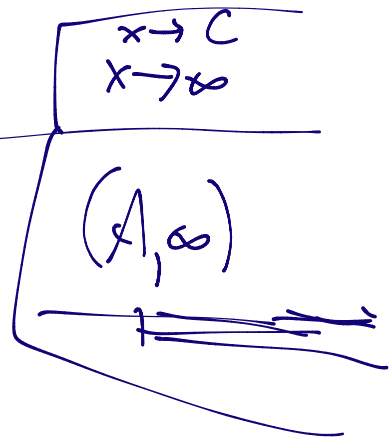



$T = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $S = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ ← want to avoid explicit use of

**Lemma 1:** Given $z \in \mathbb{H}$, map $(c,d)$ coprime integers

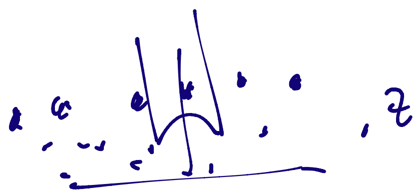
$\mapsto |cz+d|^2$ is proper, ie if $(c,d)$ escape compact sets of $\mathbb{R}^2$, then $c(c,d) \to \infty$.

**pf:** $(cx+d)^2 + c^2y^2$ is pos-def quad form in $c,d$. ∎




$\Rightarrow \dfrac{1}{|cz+d|^2} \to 0$ as $(c,d) \to \infty$.

Look at $\Gamma . z$, $\exists\, \gamma_0 \in \Gamma$ s.t. $\forall \gamma \in \Gamma$,




$\operatorname{Im} \gamma_0 z \geq \operatorname{Im} \gamma z$.

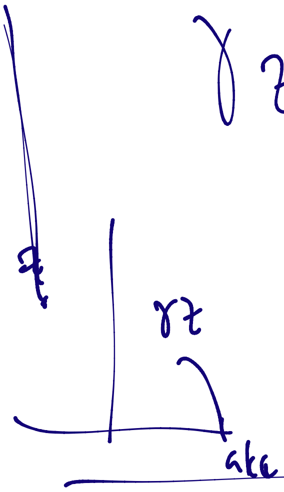
Since $\operatorname{Im} \gamma z = \dfrac{\operatorname{Im} z}{|cz+d|^2}$ ← gives best $(c_0, d_0)$.

**Exercise:** If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\begin{pmatrix} \alpha & \beta \\ c & d \end{pmatrix}$ have same bottom row,

then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -\beta \\ -c & \alpha \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Same up to translation

Want to capture $\operatorname{Re} \gamma z$.

**Standard:** $\dfrac{az+b}{cz+d} - \dfrac{a}{c} = \dfrac{\overbrace{acz + bc - acz - ad}^{-1}}{c(cz+d)}$.




$$\gamma z = \frac{a}{c_0} - \frac{1}{c_0(c_0 z + d_0)}$$ ← partial inversion

$\frac{a}{c_0}$: only part dep on a & b & is real.

$\frac{1}{c_0(c_0 z+d_0)}$: fixed.

important: Fix $z$ & $c_0, d_0$,

Need two cases, dep on $c_0 = 0$ or not!

## New Identity:

For $(c,d) = (c_0, d_0)$, $z$ fixed,

Exercise:
$$\frac{az+b}{cz+d} = \frac{ac_0+bd_0}{c_0^2+d_0^2} + \frac{dz-c}{(c^2+d^2)(cz+d)}$$

$\frac{ac_0+bd_0}{c_0^2+d_0^2} \in \mathbb{R}$. ← fixed, rotation.

Need: For $\gamma \in \Gamma$, $\gamma = \begin{pmatrix} * & * \\ c_0 & d_0 \end{pmatrix}$ want $|\ | \to \infty$.

Linear map $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} c_0 & d_0 \\ d_0 & -c_0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ac_0 + bd_0 \\ ad_0 - bc_0 \end{pmatrix}$. $\to \infty$.

$c_0^2 + d_0^2 = \det \neq 0$.

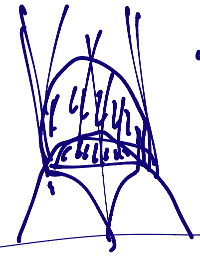
$ad_0 - bc_0 = 1$.

proper

- NAK Iwasawa
- KAK Cartan
- $NAN_{\cdots}$ Bruhat

Upshot: $\mathrm{Re}(\gamma z) \to \infty$ among $\gamma$'s with $\gamma = \begin{pmatrix} * & * \\ c_0 & d_0 \end{pmatrix}$

$\Rightarrow \exists$ least real part.

Now moved to  : $\left\{ |\mathrm{Re}(z)| \le 1/2 \ \& \ \mathrm{Im}(z) > \frac{\sqrt{3}}{2} \right.$.

Siegel domain

Why is this a fundamental region? If $\mathrm{Re}\, z > 1/2$, $T^{-1} z$ has smaller real.
If $\mathrm{Im}\, z \le \frac{\sqrt{3}}{2}$, $Sz$ has larger Im.

---

What happens on $GL_n^+(\mathbb{R})$? $\left[ GL_n^+(\mathbb{R}) / Z \cdot O(n) \right]$

any $g \in GL(n,\mathbb{R})$

$$= \begin{pmatrix} 1 & & x_{ij} \\ & 1 & \\ 0 & & 1 \end{pmatrix} \begin{pmatrix} y_1 \cdots y_{n-1} & & & \\ & \ddots & & 0 \\ & & y_1 y_2 & \\ 0 & & & y_1 \\ & & & & 1 \end{pmatrix} \underbrace{k}_{O(n)} \cdot \underbrace{z}_{\begin{pmatrix} d & & \\ & \ddots & \\ & & d \end{pmatrix}}$$

$GL_n(\mathbb{Z})$

inductive arg shows: $\forall\, g \in GL_n(\mathbb{R})$ $\exists$ fin many $\gamma \in GL_n(\mathbb{Z})$ s.t. $\gamma g = \begin{pmatrix} 1 & x_{ij} \\ & 1 \end{pmatrix} \begin{pmatrix} \ddots & & \\ & y_1 & \\ & & 1 \end{pmatrix} \underline{k}\, \underline{z}$.

with $|x_{ij}| \le 1/2$, $y_i \ge \frac{\sqrt{3}}{2}$. Siegel domain for $GL_n(\mathbb{Z})$.

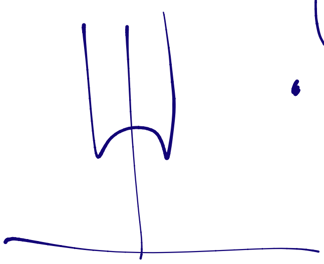
---

No Known Fundamental Domain for $GL_n(\mathbb{Z})$.

$\Rightarrow$ Lattice Crypto Rests on difficulty !.

---

## Finiteness of $h(D) = \#\{[Q],\ \mathrm{disc} = D\}$.



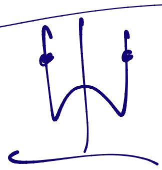
$D<0,\ A>0$ $\quad |\mathrm{Re}\,\alpha_Q| \le 1/2 \Rightarrow |B| \le A.$

$\alpha_Q = \dfrac{-B+\sqrt{|D|}\,i}{2A}$ $\quad \mathrm{Re} = \dfrac{-B}{2A}$

$1 < |\alpha_Q|^2 = \dfrac{B^2+|D|}{4A^2} \le \dfrac{A^2+|D|}{4A^2},$ $\quad 4A^2 \le A^2+|D|.$

$h(-23)=3.$ $\quad A \le \sqrt{\dfrac{|D|}{3}}.$ $\quad D = B^2-4AC$

$D=-23.$ $\quad \left\lfloor \sqrt{\dfrac{23}{3}} \right\rfloor = 2.$ $\quad C = \dfrac{B^2-D}{4A}$



$A=1,\ B$: $\pm 1$ $\quad C=6.$ ; $0$ ✗

$\alpha = \dfrac{\pm 1+\sqrt{23}\,i}{2}$ $\quad 1 \quad C=6$

$A=2,\ B$: $-1$ — $C=3$ ; $0$ ✗ ; $1$ ; $2$ ✗

$\dfrac{\pm 1+\sqrt{23}\,i}{4}$

---

$L(1,\chi_{23}) = \dfrac{-\pi}{\sqrt{23}}\,\dfrac{1}{23}\left(1+2+3+4-5 \ldots = -69.\right)$

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $n^2$ | 1 | 4 | 9 | 16 | 2 | 13 | | | | | |

$= \dfrac{\pi}{\sqrt{23}} \cdot 3.$

$$q \equiv 3\,(4): \quad L(1, \chi_q) = \frac{\pi}{\sqrt{q}} \cdot h(-q).$$