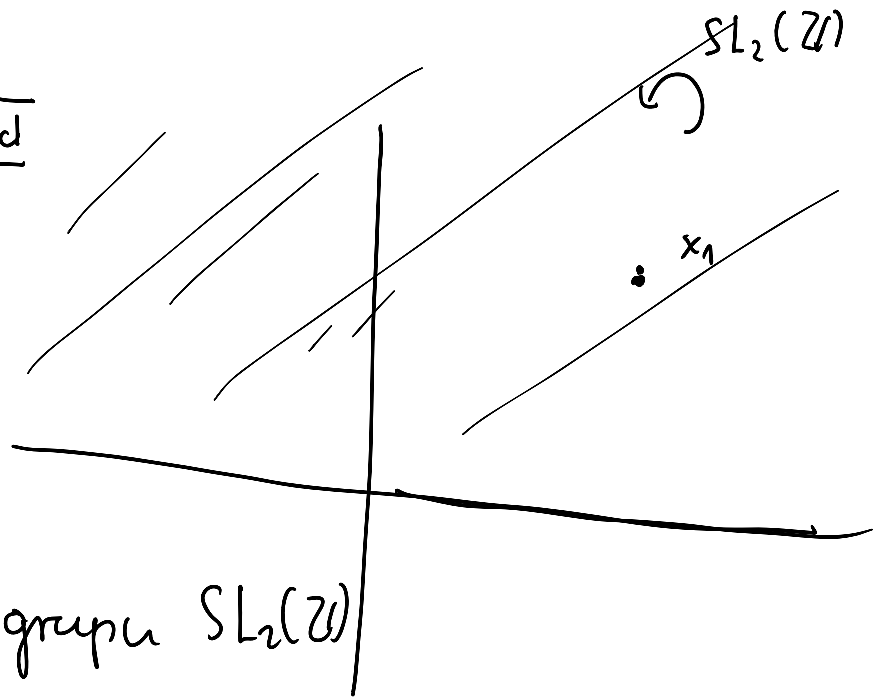
$ax^2+bxy+cy^2$; $a,b,c\in\mathbb{Z}$ $\rightsquigarrow$ ax^2+bx+c $\rightsquigarrow$ $x_1=\dfrac{-b+\sqrt{d}}{2a}$

$d=b^2-4ac$

$d<0$ i $a>0$



Def. (Fundamentalna domena)

Za zatvoreni i povezan podskup F od $\mathbb{H}$ kažemo da je fundamentalna domena za grupu $SL_2(\mathbb{Z})$ ako je svaki $z\in\mathbb{H}$ $SL_2(\mathbb{Z})$-ekvivalentan nekoj točki iz F, s time da nikoje dvije točke iz unutrašnjosti od F nisu $SL_2(\mathbb{Z})$-ekvi

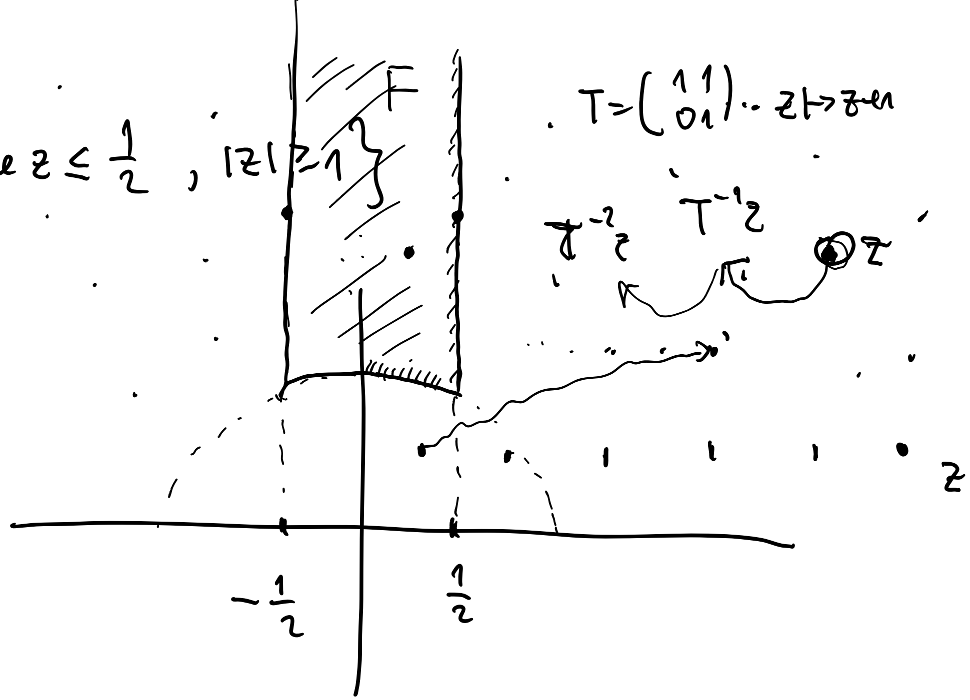
Napomena: 1) $\mathbb{H}=\bigcup_{\gamma\in SL_2(\mathbb{Z})}\gamma F$ $\rightsquigarrow$ $\{\gamma z : z\in F\} = \gamma(F)$

2) Unutrašnjost od $\gamma_1 F\cap\gamma_2 F$ je prazan skup za $\gamma_1\neq\gamma_2$

z_1, z_2 ako $\exists\, \gamma\in SL_2(\mathbb{Z})$ t.d. $\gamma z_1=z_2$

$\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ $\Leftrightarrow$ $\dfrac{az_1+b}{cz_1+d}=z_2$

Propozicija: Skup $F = \{ z \in \mathbb{H} : -\frac{1}{2} \leq \operatorname{Re} z \leq \frac{1}{2}, \ |z| \geq 1 \}$ je fundamentalna domena za $SL_2(\mathbb{Z})$



__Dokaz:__ Definirajmo prve dvije matrice

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{i} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2\mathbb{Z}.$$

Primijetimo $Tz = \frac{z+1}{1} = z+1$ $\qquad Sz = \frac{-1}{z}$ ⇝ inverzija.

$$T^{-1}z = z-1$$

> **Lema:** Za $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\mathbb{Z}$
>
> $$\operatorname{Im}(\gamma z) = \frac{\operatorname{Im} z}{|cz+d|^2}$$
>
> Dokaz: (d.z.)

Ideja je koristeći translacije T^j točku z preslikati u prugu $-\frac{1}{2} \leq \operatorname{Re} z \leq \frac{1}{2}$. Ako se tako dobivena točka ne nalazi u F, primijenimo presl. S i ponovimo cijeli postupak.

Promotrimo fju. $SL_2(\mathbb{Z}) \to \mathbb{R}$ koja $\underset{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}{\overset{}{\gamma}} \mapsto \frac{\operatorname{Im} z}{|cz+d|^2} = \operatorname{Im}(\gamma z)$.

Tvrdimo da ova fju. postiže maksimum za neki $\gamma_m \in SL_2(\mathbb{Z})$ (d.z.)

Odaberemo $j \in \mathbb{Z}$ t.d. $T^j(\gamma_m z)$ nalazi u traci $|\operatorname{Re} z| \leq \frac{1}{2}$. Ako je $|T^j(\gamma_m z)| \geq 1$, onda smo gotovi jer je $T^j(\gamma_m z)$ nalazi u F $\quad S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$

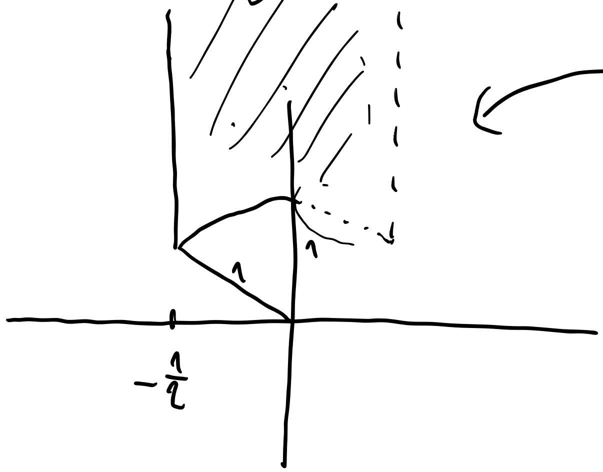
Inače primijenimo S. Kako vrijedi $\operatorname{Im}(S(T^j(\gamma_m z))) = \frac{\operatorname{Im}(T^j(\gamma_m(z)))}{|T^j(\gamma_m z)|^2}$

$\Rightarrow$ $\cancel{\Leftarrow}$ s maksimalnošću od $\gamma_m z$. $\quad > \operatorname{Im}(T^j(\gamma_m z))$

Pokažimo još da nikoje dvije točke iz unutrašnjosti od F nisu $= \operatorname{Im}(\gamma_m z)$

$SL_2(\mathbb{Z})$ ekvivalentne. Pretp. suprotno. Neka su $z_1, z_2 \in F$ t.d. $z_1 = \gamma z_2$ za neki $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Možemo pretp. $\operatorname{Im} z_1 \geq \operatorname{Im} z_2$. Iz formule za imaginarni dio od γz_2 slijedi da je $|cz_2 + d| \leq 1$.

$$\left.\begin{array}{l} |cz_2+d|\le 1 \\ |z_2|\ge 1 \\ |\mathrm{Re}\, z_2|\le \frac{1}{2} \end{array}\right\} \Rightarrow |c|\le 1 \rightsquigarrow c=-1,0,1 \rightsquigarrow \text{(d.z.)}$$



$\tilde{F} = F -$

Kažemo da je f $[a,b,c]$ reducirana $(d<0,\ a>0)$ ako i samo ako $\frac{-b+\sqrt{d}}{2a} \in \tilde{F}$!

Teorem 4.4. Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana onda je $-d = 4ac-b^2 \ge 3ac$ pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$. ∎

Definicija 4.4. Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava s $h(d)$.

Primjer 4.2. Izračunajmo $h(-4)$. $\rightsquigarrow x^2+y^2$

Rješenje: Iz $3ac \le 4 \Rightarrow a=c=1 \Rightarrow b=0 \Rightarrow h(-4)=1$.

Teorem 4.6. Neka su $d<0$ i $n>0$ cijeli brojevi. Tada je n pravo reprezentiran nekom binarnom kvad. formom diskriminante d ako i samo ako kongr. $x^2 \equiv d \pmod{4n}$ ima rješenje.

Dokaz: Pretp. da gornja kongruencija ima rješenje i da je $x=b$ rješenje. Definirajmo c s $b^2-4nc=d$, i odaberimo $a=n$. Sada kvadratna forma $f(x,y)=ax^2+bxy+cy^2$ ima diskriminantu d i $f(1,0)=n$, pa f pravo reprezentira broj n.

Obratno, pretp. da forma f ima diskriminantu d i da je $n=f(p,r)$ za neke $p,r\in\mathbb{Z}$, $(p,r)=1$. Tada postoje $q,s\in\mathbb{Z}$ takvi da je

$$ps-rq=1.$$

Def. s $\tilde{f}$ kvad. formu koju dobijemo iz f djelovanjem matrice $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$

Znamo da je diskr. od $\tilde{f}$ jednaka d. Označimo s $[a', b', c'] = \tilde{f}$.

Ključno: $a' \underset{\uparrow}{=} f(p, r) = n \rightsquigarrow \underline{d} = b'^2 - 4a'c' = \underline{\underline{b'^2 - 4nc'}}$

provjerite za d. z.

$\Rightarrow b'$ rješenje kongr. $x^2 \equiv d \pmod{4n}$ ✓.

$\blacksquare$