THIN GROUPS AND THE AFFINE SIEVE

$SL_n(\mathbb{Z})$ the group of $n \times n$ matrices of determinant equal to 1.

- It is a complicated big group
- It is central in automorphic forms, number theory, geometry....

It satisfies some basic properties when reduced mod q:

1) Strong Approximation (Chinese remainder theorem)

$$SL_n(\mathbb{Z}) \xrightarrow{\pi_q} SL_n(\mathbb{Z}/q\mathbb{Z})$$

is onto.

There is a quantification of this that is also fundamental.

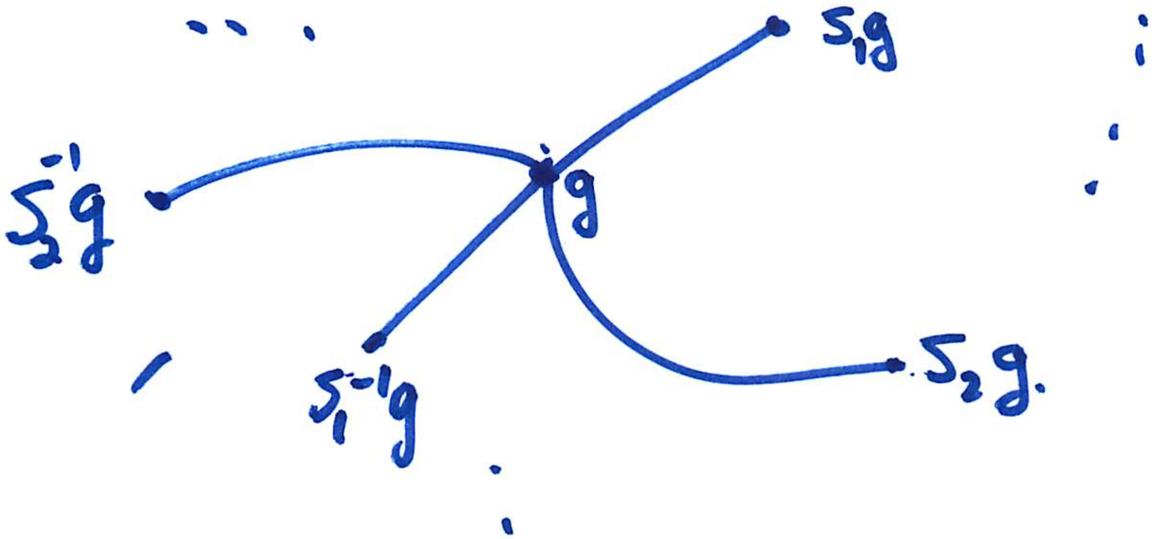
② Fix a finite generating set S of $SL_n(\mathbb{Z})$ (assume that it is symmetric, $s \in S \iff s^{-1} \in S$).

Form the finite "congruence graphs"

$$X_q = \left(SL_n(\mathbb{Z}/q\mathbb{Z}), S \right)$$

vertices are elements of $SL_n(\mathbb{Z}/q\mathbb{Z})$

edges $g \to sg$, $s \in S$.



X_q is connected (by strong approximation) X_q is $|S|$ regular.

③

(2) <u>Super-strong approximation</u>

The X_q's are an 'expander family'.

i.e. if the eigenvalues of the adjacency matrix

$$|S| = \lambda_1 > \lambda_2 \geq \lambda_3 \cdots \geq \lambda_N$$

satisfy

$$\lambda_2 \leq |S| - \varepsilon_0$$

with $\varepsilon_0 > 0$ (independent of q !)

"spectral gap".

$\Rightarrow$ the graphs X_q are very highly connected, random walk on X_q with generators S is rapidly mixing, ...

(2) follows from automorphic forms

If $\Gamma(q) = \ker(A \to A \pmod q)$

consider $L^2(\Gamma(q) \backslash SL_n(\mathbb{R}))$

and in particular the Ramanujan-Selberg Conjectures about which a lot is known. (If $n \geq 3$ one can also use "property T")

More generally if G is a semisimple simply connected group defined over $\mathbb{Q}$ Then both (1) and (2) continue to hold for $\Gamma = G(\mathbb{Z})$ (assume $G(\mathbb{R})$ has no compact factors).

(2) due to Burger-Sarnak Clozel "property tau".

For many applications one needs these fundamental properties for general $\Gamma \leq SL_n(\mathbb{Z})$.

Let $G = Zcl(\Gamma)$, the "Zariski closure" of Γ. The smallest algebraic matrix group to contain Γ. It's equations are over $\mathbb{Q}$.

So G is a familiar and a well understood object.

<u>Definition:</u> If Γ is infinite index in $G(\mathbb{Z})$ we say Γ is thin.

<u>Ubiquity of thin groups:</u>

(A) Fix $l \geq 2$ and choose $A_1, \ldots, A_l$ at random in $SL_n(\mathbb{Z})$ by taking them from a big ball $\|A_j\| \leq X$ $j = 1, \ldots, l$. Then with probability tending to 1 as $X \to \infty$,

$\Gamma = \langle A_1, \dots, A_\ell \rangle$ is Zariski dense in SL_n, it is thin and free (in fact "Schottky") R. Aoun (2010)

(B) diophantine geometric constructions typically yield thin groups

<u>eg</u>: Integral Apollonian packings:

$$F(x_1,x_2,x_3,x_4) = 2(x_1^2+x_2^2+x_3^2+x_4^2) - (x_1+x_2+x_3+x_4)^2$$

$G = O_F$ the orthogonal group of F

$$O_F(\mathbb{Z}) \leq GL_4(\mathbb{Z})$$

A = apollonian group, $A = \langle S_1, S_2, S_3, S_4 \rangle$

$$S_1 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}, \quad S_3 = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix} \quad S_4 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$A \leq O_F(\mathbb{Z})$, A is thin!

Figure 3.

Figure 4.

Figure 5.

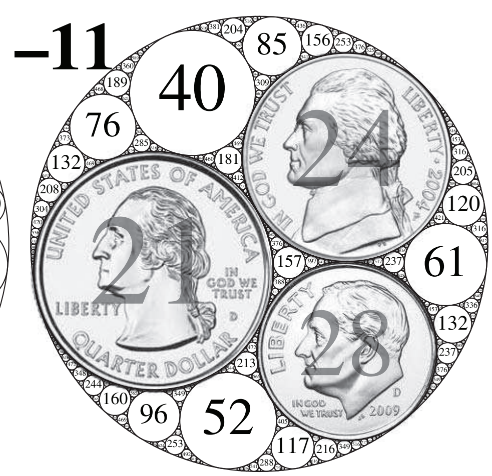


Figure 6.

If $a = (-11, 21, 24, 28)$ then the orbit $\mathcal{O}_a = a.A$ of a under A in $\mathbb{Z}^4$ produces the curvatures of all 4-tuples of mutually tangent circles in the packing determined by a.

(c) Topological monodromy often produces thin groups

Eg 1: Consider the family of hyperelliptic curves

$$C_t : \quad y^2 = (x-a_1)(x-a_2)\cdots(x-a_r)(x-t)$$

here $a_1, \dots, a_r$ are distinct in $\mathbb{C}$, t varies over $S = \mathbb{C} \setminus \{a_1, \dots, a_r\}$.

Fix a base point t_0, $H_1(C_{t_0}) \cong \mathbb{Z}^{2g}$

$g = \text{genus}(C_{t_0})$.

traverse the closed loop γ and follow a cycle β in $H_1(C_{t_0})$. gives

$M(\gamma)\beta \in H_1(C_{t_0})$, representation

$$M : \pi_1(S, t_0) \longrightarrow Sp(2g, \mathbb{Z})$$

monodromy

$$\boxed{\begin{aligned} Sp : \ & X^t J X = J \\ & J = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \end{aligned}}$$

· Image(M) is Zariski dense in $Sp(2g)$.

K. Yu (1990's)

$M(\pi_1(S))$ is finite index in $Sp(2g, \mathbb{Z})$ NOT THIN.

However the family

$$C_t : \quad y^5 = x^3(1-x)^3(1-tx)^2$$

corresponds to a nonarithmetic triangle group (Paula Cohen-Wolfart).

$$Zcl(M(\pi_1(S))) = H \quad \subsetneqq Sp(2g)$$

H is a Hilbert modular subgroup

$M(\pi_1(S))$ is thin (in $H(\mathbb{Z})$).

(D) Veech or Teichmuller curves in $\mathcal{M}_g$ yield thin monodromy.

(E) Do Calabi-Yau and Dwork families yield thin monodromy?

$$y_1^3 + y_2^3 + y_3^3 = 3t\, y_4 y_5 y_6$$

$$y_4^3 + y_5^3 + y_6^3 = 3t\, y_1 y_2 y_3$$

(F) Covers of hyperbolic 3 manifolds with large heegard genus are given by thin groups (Lackenby, Long-Lubotzky-Reid)

Matthews-Weisfeiler-Vaeserstein

Strong approximation holds for thin groups:

<u>Theorem</u> Let $\Gamma \leq SL_n(\mathbb{Z})$ be Zariski dense in SL_n. There is a finite set S of primes $p_1, \ldots, p_\nu$ depending on Γ s.t. for $(q, S) = 1$

$$\Gamma \longrightarrow SL_n(\mathbb{Z}/q\mathbb{Z}) \text{ is onto}$$

· Similarly for other simple, ~~G's~~ simply connected G's in place of SL_n.
new treatments: Nori, Larsen-Pink.

As for ~~as~~ expansion the familiar number theoretic methods don't work when $Vol(\Gamma \backslash G(\mathbb{R})) = \infty$. However a combinatorial method going back to S-Xu 1990's does when combined with many new ideas

(1) Bourgain - Gamburd - S
general set up and proof for $G = SL_2$
(2006 - 2009)

(2) Proof in (1) depends on
Helfgott's combinatorial A.A.A
theorem for
$SL_2(\mathbb{F}_p)$

nonabelian "sum product"
Theorem

(3) (2) is generalized to
Chevelly groups $G(\mathbb{F}_p)$ by
Pyber - Szabo, Breuillard - Green - Tao
(2010)

(4) P. Varju extends (1) to $G = SL_n$
(2010)

(5) A. Salehi - Varju prove the
most general expander property
(2010)

THEOREM (Superstrong approximation)
(Salehi-Varjú 2011).

Let $\Gamma \leq GL_n(\mathbb{Q})$ be finitely generated with generating set S. Then the congruence graphs $(\pi_q(\Gamma), S)$ for q square-free, q prime to a fixed set of primes (depending on Γ) is an expander family iff G° the connected component of $G = Zcl(\Gamma)$, is perfect ($G = [G,G]$).
(effective).

This and its earlier versions is at the heart of many diophantine applications. We discuss the affine sieve which is an extension of the Brun Sieve to orbits of affine linear actions.

SEARCH FOR PRIMES

1 - dimension:

$\mathbb{Z}$, $f \in \mathbb{Z}[x]$

Are there infinitely many x s.t. $f(x)$ is prime?

(I) $f(x) = x$ — yes.

(II) $f(x) = ax+b$ — yes if $(a,b)=1$ otherwise no (DIRICHLET)

(III) $f(x) = x^2+1$ — (Euler Conj yes)

(IV) $f(x) = x(x+2)$, are There infinitely many x s.t. $f(x)$ has at most two prime factors $\Longleftrightarrow$ twin prime conjecture.

<u>BRUN</u>: There are infinitely many x such that $\underset{=x(x+2)}{f(x)}$ has at most 20 prime factors

Saturation Number

Let $r_0(Z, f)$ = least r such that the set of $x \in Z$ which ~~has~~ have at most r prime factors is infinite

$\Longleftrightarrow$ (better for higher dimensions)

the least r such that

$$\mathrm{Zcl}(\{x \in \mathbb{Z} : f(x) \text{ has at most } r \text{ prime factors}\})$$

$$= \mathbb{A}^1.$$

BRUN: for any f

$r_0(\mathbb{Z}, f)$ is finite !

More generally let

$$\mathcal{O} = a.\Gamma \quad , \Gamma \leq SL_n(\mathbb{Z})$$

be the orbit of $a \in \mathbb{Z}^n$ under Γ.

Let $f \in \mathbb{Z}[x_1, \dots, x_n]$

Set $r_0(\mathcal{O}, f)$ the least r (if it exists) such that

$$\mathrm{Zcl}\left(\{x \in \mathcal{O} : f(x) \text{ has at most } r \text{ prime factors}\}\right)$$

$$= \mathrm{Zcl}(\mathcal{O}).$$

Enemy is a torus (for saturation)

Eg $\mathcal{O} = \Gamma = \{2^m : m \in \mathbb{Z}\} \subset GL_1(\mathbb{Q})$ a torus.

set $F(x) = (x-1)(x-2)$

Then the standard heuristics suggest that the number of prime factors of $(2^m - 1)(2^m - 2)$ goes to infinity with m.

I.E. $\quad \tau_0(\Gamma, F) = \infty$.

So we must avoid ~~torii~~ tori that are in the radical of G. The following was conjectured in B-G-S.

<u>Fundamental Theorem of the Affine sieve</u>
(Salehi - S 2011)

Let $\Gamma \leq GL_n(\mathbb{Z})$, $\mathcal{O} = a.\Gamma \subset \mathbb{Z}^n$

If $G = Zcl(\Gamma)$ is Levi semisimple (i.e. rad G contains no torus) then for $f \in \mathbb{Z}[x_1, \ldots, x_n]$ with $f\big|_{Zcl(\mathcal{O})} \not\equiv 0$, (on any cpt)

~~then~~ $\tau_0(\mathcal{O}, f) < \infty$. That is there is an $r < \infty$ (effective but not feasible) s.t.

$Zcl\{x \in \mathcal{O} : f(x) \text{ has at most } r \text{ prime factors}\}$
$= Zcl(\mathcal{O})$.

This applies to integral apollonian packings. For these and certain f's there some gems.

Theorem (S 07):

There are infinitely many circles with curvature a prime number in any integral Apollonian packing. In fact there are infinitely many pairs of tangent circles ("twin primes") both of whose curvatures are prime.

In fact

$$r_0(\mathcal{O}_a, x_1) = 1$$

$$r_0(\mathcal{O}_a, x_1 x_2) = 2.$$

Zaremba's Conjecture:

For A large (≥ 5) and fixed let D_A be the positive integers q s.t. there is $1 \leq b \leq q-1$, $(b,q)=1$ with

$$\frac{b}{q} = [a_1, \ldots, a_k] \qquad \text{continued fraction}$$

$$a_j \leq A .$$

Conjecture: $\quad D_A = \mathbb{N}$.

Equivalently let Γ_A be the semi subgroup of $SL_2(\mathbb{Z})$ generated by

$$\begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}, \quad 1 \leq a \leq A$$

$$\begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & a_2 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & a_k \end{bmatrix} = \begin{bmatrix} * & b \\ * & q \end{bmatrix}$$

$$\Longleftrightarrow \qquad \frac{b}{q} = [a_1, a_2, \ldots, a_k].$$

So the conjecture is equivalent to the orbit of $(0,1)$ under Γ_A having second coordinate q for any given $q \geq 1$.

Γ_A is "thin". This is a 'local to global' question for thin semigroups.

<u>Theorem</u> (Bourgain–Kontorovich 2011)

For $A \geq 3000$ fixed, D_A has density 1, i.e. almost all q in the sense of density are in D_A.

One of the many new ingredients in the proof of expansion for thin groups is SUM product theory from additive combinatorics.

<u>THEOREM</u> (Bourgain, Netz Katz, Tao)

given $\varepsilon > 0$ there is $\delta > 0$ such that for p any large prime and $A \subset \mathbb{F}_p$ with $p^{\varepsilon} \leq |A| \leq p^{1-\varepsilon}$

$$|A+A| + |A.A| \gtrsim |A|^{1+\delta}.$$

Some references:

0). A. Lubotzky "Expander graphs in pure and applied Math"

1). S. Hoory - N. Linial - A. Wigderson "Expanders" BAMS 43 (2006) 439-561

2). P. Sarnak "Integral Apollonian Packing" Amer. Math. Monthly 118, (2011) 291-307

3). J. Bourgain - A. Gamburd - P. Sarnak Invent. Math. 179 (2010) 559-644

4). H. Helfgott Ann. Math. 167 (2008) 601-623

5). L. Pyber and E. Szabo "Growth in finite simple groups of Lie type" ArX. 1001.4556

6). E. Breuillard - B. Green - T. Tao "Linear approximate groups" ArX. 1006.3365

7). P. Varju "Expansion in $SL_d(\mathcal{O}/I)$" ArX. 1001.3664

8). A. Salehi and P. Varju "Expansion in perfect groups" preprint 2011

9). J. Bourgain and A. Kontorovich, ArX. 1103.0422.