Thin Groups and the Affine Sieve

Peter Sarnak
Mahler Lectures 2011

$\mathrm{SL}_n(\mathbb{Z})$ the group of integer $n \times n$ 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 modulo q:

(1) Strong Approximation (Chinese remainder theorem)

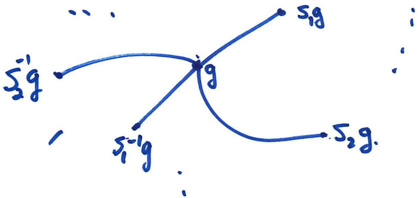
$$\mathrm{SL}_n(\mathbb{Z}) \xrightarrow{\pi_q} \mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z}) \quad \text{is onto.}$$

There is a quantification of this that is also fundamental.

Fix a finite generating set S of $\mathrm{SL}_n(\mathbb{Z})$ (assume that it is symmetric, $s \in S \Leftrightarrow s^{-1} \in S$).
Form the finite "congruence graphs"

$$X_q = (\mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z}), S)\,,$$

vertices are elements of $\mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})$, edges $g \mapsto sg$, $s \in S$.



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

(2) Super-strong Approximation

The X_q's are an "expander family", i.e. if the eigenvalues of the adjacency matrix

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

satisfy

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

with $\varepsilon_0 > 0$ (independent of q!)
"spectral gap".

$\Longrightarrow$ 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 $\Gamma(q) = \ker(A \mapsto A \pmod{q})$, consider $L^2(\Gamma(q) \setminus \mathrm{SL}_n(\mathbb{R}))$, 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 $\Gamma \leq \mathrm{SL}_n(\mathbb{Z})$.
let $G = \mathcal{Z}\mathrm{cl}(\Gamma)$, the "Zariski closure" of Γ. The smallest algebraic matrix group to contain Γ. Its equations are over $\mathbb{Q}$.
So G is a familiar and a well understood object.

Definition

If Γ is of infinite index in $G(\mathbb{Z})$, we say Γ is thin.

- In general, the question of whether Γ is thin has no decision procedure (Mikhailova 1958).

Ubiquity of Thin Groups:
(A) Fix $\ell \geq 2$ and choose $A_1, \ldots, A_\ell$ at random in $\mathrm{SL}_n(\mathbb{Z})$ by taking them from a big ball $\|A_j\| \leq X$, $j = 1, \ldots, \ell$. Then with probability tending to 1 as $X \to \infty$, $\Gamma = \langle A_1, \ldots, A_\ell \rangle$ 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.

E.g.: Integral Apollonian packings:

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

$$G = \mathrm{O}_F, \quad \text{the orthogonal group of } F$$

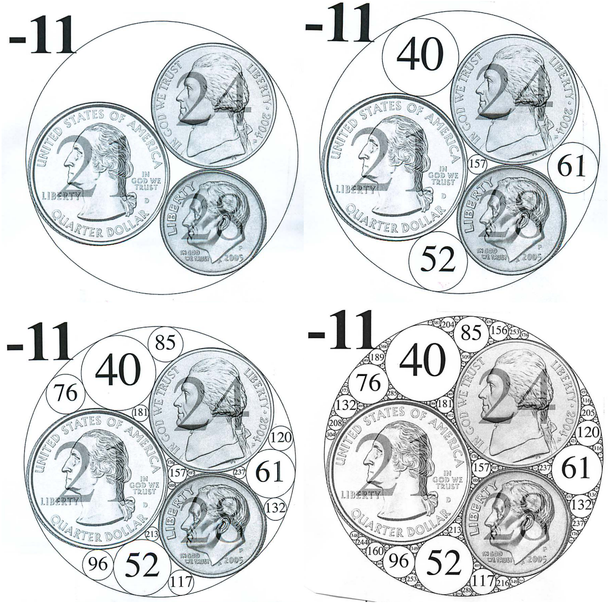
$$\mathrm{O}_F(\mathbb{Z}) \le \mathrm{GL}_4(\mathbb{Z})$$

$$A = \text{Apollonian group}, \quad A = \langle S_1, S_2, S_3, S_4 \rangle$$

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

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

$$A \le \mathrm{O}_F(\mathbb{Z}), \qquad A \text{ is thin!}$$


-11
24
21
28
-11
40
24
21
157
61
28
52
-11
85
40
76
181
24
21
120
157
237
61
28
132
213
96
52
117
-11
204
85
156
40
189
76
132
181
208
24
205
120
21
157
237
61
28
132
213
160
96
52
117
216

If $a = (-11, 21, 24, 28)$, then the orbit $\mathcal{O}_a = a \cdot A$ 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.
E.g. 1: Consider the family of hyperelliptic curves

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

Here $a_1, \ldots, a_r$ are distinct in $\mathbb{C}$, t varies over $S = \mathbb{C} \setminus \{a_1, \ldots, a_r\}$. Fix a base point t_0, $H_1(C_{t_0}) \cong \mathbb{Z}^{2g}$, where $g = \mathrm{genus}(C_{t_0})$.

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

$$M(\gamma)\beta \in H_1(C_{t_0}), \quad \text{representation}$$
$$M : \pi_1(S, t_0) \to \mathrm{Sp}(2g, \mathbb{Z})$$

monodromy

$$\mathrm{Sp} : X^t J X = J, \qquad J = \begin{bmatrix} 0 & I & -I & 0 \end{bmatrix}.$$

- $\mathrm{Image}(M)$ is Zariski dense in $\mathrm{Sp}(2g)$.

K. Yu (1990's): $M(\pi_1(S))$ is finite index in $\mathrm{Sp}(2g, \mathbb{Z})$, not thin.

However, the family

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

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

$$\mathcal{Z}\mathrm{cl}(M(\pi_1(S))) = H \lneqq \mathrm{Sp}(2g).$$

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

(D) Veech or Teichmuller curves in M_g yield thin monodromy.

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

$$\begin{aligned} y_1^3 + y_2^3 + y_3^3 &= 3ty_4y_5y_6 \\ y_4^3 + y_5^3 + y_6^3 &= 3ty_1y_2y_3. \end{aligned}$$

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

Matthews–Weisfeiler–Vaeserstein
Strong approximation holds for thin groups:

Theorem

Let $\Gamma \leq \mathrm{SL}_n(\mathbb{Z})$ be Zariski dense in SL_n. There is a finite set S of primes $p_1, \ldots, p_v$ depending on Γ such that for $(q, S) = 1$, $\Gamma \to \mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})$ is onto.

- Similarly for other simple, simply-connected G's in place of SL_n. New treatments: Nori, Larsen–Pvik.

As for expansion, the familiar number theoretic methods don't work when $\mathrm{Vol}(\Gamma \setminus G(\mathbb{R})) = \infty$. 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 $G = \mathrm{SL}_2$ (2006–2009).

(2) Proof in (1) depends on Helfgott's combinatorial A.A.A. theorem (nonabelian "sum-product" theorem) for $\mathrm{SL}_2(\mathbb{F}_p)$.

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

(4) P. Varjú extends (1) to $G = \mathrm{SL}_n$ (2010).

(5) A. Salehi–Varjú prove the most general expander property (2010).

Theorem (Super-strong Approximation (Salehi–Varjú 2011))

Let $\Gamma \leq \mathrm{GL}_n(\mathbb{Q})$ 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 $G = \mathcal{Z}\mathrm{cl}(\Gamma)$, 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 such that $f(x)$ 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 conjectured yes).

(IV) $f(x) = x(x + 2)$ — are there infinitely many x such that $f(x)$ has at most two prime factors? $\Longleftrightarrow$ twin prime conjecture.

Brun: There are infinitely many x such that $f(x) = x(x + 2)$ has at most 20 prime factors.

Saturation Number

Let $r_0(\mathbb{Z}, f)$ be the least r such that the set of $x \in \mathbb{Z}$ which have at most r prime factors is infinite $\Longleftrightarrow$ (better for higher dimensions) the least r such that

$$\mathcal{Z}\mathrm{cl}\left(\{x \in \mathbb{Z} : f(x) \text{ has at most } r \text{ prime factors}\}\right) = \mathbb{A}^1.$$

Brun: for any f, $r_0(\mathbb{Z}, f)$ is finite!

More generally, let $\mathcal{O} = a \cdot \Gamma$, $\Gamma \leq \mathrm{SL}_n(\mathbb{Z})$ be the orbit of $a \in \mathbb{Z}^n$ under Γ.

Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$.
Set $r_0(\mathcal{O}, f)$ be the least r (if it exists) such that

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

Enemy is a torus (for saturation). E.g.

$$\mathcal{O} = \Gamma = \{2^m : m \in \mathbb{Z}\} \subset \mathrm{GL}_2(\mathbb{Q}) \quad \text{a torus.}$$

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. $r_0(\Gamma, F) = \infty$.

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

Fundamental Theorem of the Affine Sieve (Salehi–S. 2011)

Let $\Gamma \leq \mathrm{GL}_n(\mathbb{Z})$, $\mathcal{O} = a \cdot \Gamma \subset \mathbb{Z}^n$. If $G = \mathcal{Z}\mathrm{cl}(\Gamma)$ is Levi semisimple (i.e. $\mathrm{rad}\, G$ contains no torus) then for $f \in \mathbb{Z}[x_1, \ldots, x_n]$ with $f|_{\mathcal{Z}\mathrm{cl}(\mathcal{O})} \not\equiv 0$ (on any compact), $r_0(\mathcal{O}, f) < \infty$. That is, there is an $r < \infty$ (effective but not feasible) such that

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

This applies to integral Apollonian packings. For these and certain f's there are 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 such that 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

$$D_A = \mathbb{N}.$$

Equivalently, let Γ_A be the semi-subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by

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

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

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

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.

Theorem (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.

Theorem (Bourgain, Nets Katz, Tao)

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

$$|A + A| + |A \cdot A| \geq |A|^{1+\delta}.$$

Some references:

- J. Bourgain, A. Gamburd, and P. Sarnak, Invent. Math. **179** (2010), 559–644.
- J. Bourgain and A. Kontorovich, arXiv:1103.0422.
- E. Breuillard, B. Green, and T. Tao, "Linear approximate groups", arXiv:1006.3365.
- Y. Chen, Y. Yang, and N. Yui, "Monodromy of Pichard–Fuchs differential equations for Calabi–Yau threefolds", arXiv 2007.
- H. Helfgott, Ann. Math. **167** (2008), 601–623.
- S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications", BAMS **43** (2006), 439–561.
- A. Lubotzky, "Expander Graphs in Pure and Applied Math".
- K. A. Mikhailova, Dokl. Akad. Nauk SSSR **119** (1958), 1103–1105.

- L. Pyber and E. Szabo, "Growth in finite simple groups of Lie type", arXiv:1001.4556.
- A. Salehi and P. Sarnak, "Affine Sieve", preprint, 2011.
- A. Salehi and P. Varjú, "Expansion in perfect groups", preprint, 2011.
- P. Sarnak, "Integral Apollonian Packing", Amer. Math. Monthly **118** (2011), 291–307.
- P. Varjú, "Expansion in $\mathrm{SL}_d(O/I)$", arXiv:1001.3664.