Thin Groups and the Affine Sieve

$SL_n(Z)$ 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)

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

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"

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

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.
(2) Super-strong approximation

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

$$1 \geq \lambda_1 \geq \lambda_2 \geq \lambda_3 \ldots \geq \lambda_n$$

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 \( \Pi(q) = \ker (A \rightarrow A(\mod q)) \), consider \( L^2(\Pi(q) \mid \text{SL}_n(\mathbb{R})) \) and in particular the Ramanujan-Selberg Conjectures about which a lot is known. (If \( n > 3 \), 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 \( \Pi' = G(\mathbb{Z}) \) (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 $\Gamma \leq \text{SL}_n(\mathbb{Z})$.

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

So $G$ is a familiar and well understood object.

**Definition:** If $\Gamma$ is infinite index in $G(\mathbb{Z})$ we say $\Gamma$ is thin.

**Ubiquity of thin groups:**

(A) Fix $l \geq 2$ and choose $A_1, \ldots, A_l$ at random in $\text{SL}_n(\mathbb{Z})$ by taking them from a big ball $\|A_j\|_2 \leq X$ for $j = 1, \ldots, l$. Then with probability
tending to 1 as $X \to \infty$,

$\Gamma = \langle A_1, \ldots, A_2 \rangle$ is Zariski dense in $\text{SL}_n$, it is thin and free (in fact "Schottky") \quad \text{R. Aoun (2010)}

(B) Diophantine geometric constructions typically yield thin groups

Eq: Integral Apollonian packings:

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

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

$\text{O}_F(\mathbb{Z}) \leq \text{GL}_4(\mathbb{Z})$

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

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

$A \leq \text{O}_F(\mathbb{Z})$, $A$ is thin!
yields the integral Apollonian packing we will fill in the new lunes as in Figure fis. Continuing in this way ad infinitum, the outer circle has a negative sign indicating that the other circles are in its interior mit.

With this rescaling, all of the curvatures turn out to be integers, with their curvatures which are the reciprocals of the radii. In fact, in this example, it is natural to scale everything further by so let us take as our unit of measurement, and then for each circle.

Since the circles become very small, so do their radii, and it is more convenient to work with their curvatures.

In Figure x, our three tangent circles are displayed together with the unique outer tangent to all three.

What is more remarkable is that if we continue to place circles in the resulting regions bounded by three circles as described next, then all the diameters are rationals.

At the next generation, we place circles in each of the lune regions, obtaining the configuration in Figure y with the curvatures.

Our proof is based on the use of motions of the plane that take circles to circles, and then to discuss the Diophantine properties of the integers.

My aim in this paper is first to explain the elementary plane geometry behind the above construction, and then to introduce the key object in the letter and preprints.

There are many papers in the literature dealing with Apollonian packings and their generalizations in number theory, the basic questions here are easy to state but difficult to resolve.

In Section s, we introduce the key object which is central to understanding the construction of its radius and by its curvature. Specifically, the operation of inversion in a circle, which we allow a straight line as a circle with “infinite” radius, and preserve tangencies and Apollonius’s Theorem.

What appears in the packing is the only circle with a negative sign.

The developments that we discuss below are contained in the developments that we discuss below are contained in the letter and preprints.

April rpqq

hwe allow a straight line as a circle with “infinite” radius, and preserve tangencies and Apollonius’s Theorem.

Given three mutually tangent circles $C_1$, $C_2$, and $C_3$, the operation of inversion in a circle is a transformation that takes circles to circles.

In Figure 5, we see the packing after the first generation, with the unique outer circle and the three tangent circles.

In Figure 6, we see the packing after the second generation, with the unique outer circle and the three new circles.

Figure 3.

Figure 4.

Figure 5.

Figure 6.
If \( a = (-11, 21, 24, 28) \) then the orbit \( O_a = a \). 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 \( a_1, \ldots, a_r \) 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 \( g = \text{genus}(C_{t_0}) \).
traverse the closed loop $\gamma$ and follow a cycle $\beta$ in $H_2(C_{t_0})$. gives $M(\gamma)\beta \in H_2(C_{t_0})$, representation

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

monodromy

\[ Sp : X^t J X = J \]
\[ J = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \]

- 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
\[ C_t : y^5 = x^3(1-x^3)(1-tx^2) \]
corresponds to a non-arithmetic triangle group (Paula Cohen-Wolpert).
\[ \mathcal{Z}_d(M(\pi, (5))) = H \cong Sp(2g) \]
\( H \) is a Hilbert modular subgroup
\( M(\pi, (5)) \) is thin in \( \mathbb{H}(\mathbb{Z}) \).

(D) Veech or Teichmüller 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 Heegaard genus are given by thin groups (Lackenby, Long-Lubotzky-Reid)
Matthews-Weisfeiler-Vaeserstein

Strong approximation holds for these groups:

**Theorem.** Let \( \Gamma \leq \text{SL}_n(\mathbb{Z}) \) be Zariski dense in \( \text{SL}_n \). There is a finite set \( S \) of primes \( p_1, \ldots, p_r \) depending on \( \Gamma \) s.t. for \( (q, S) = 1 \)

\[
\Gamma \twoheadrightarrow \text{SL}_n(\mathbb{Z}/q\mathbb{Z})
\]

is onto.

Similarly for other reductive, split simply connected \( G \)'s in place of \( \text{SL}_n \).

New treatments: Nori, Larsen-Pink.

As for any expansion the families of number theoretic methods don't work when \( \text{Vol}(\Gamma \backslash G(\mathbb{R})) = \infty \). However a combinatorial method going back to S-Xu 1990's does when combined with many new ideas.
(1) Bourgain-Gamburd - 5
general set up and proof for $G = SL_2$
(2006 - 2009)

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

(3) (2) is generalized to
Chevalley 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-Varju 2011)

Let $\pi \leq \text{GL}_n(\mathbb{Q})$ be finitely generated with generating set $S$. Then the congruence graphs $(\pi_\mathfrak{p}(\pi), S)$ for $\mathfrak{p}$ square-free, $\mathfrak{p}$ prime to a fixed set of primes (depending on $\pi$) is an expander family iff $G^0$, the connected component of $G = \mathbb{Z} \leq (\pi)$, 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) \( f(x) = x \) \quad yes.

(II) \( f(x) = ax + b \) \quad yes if \( (a,b) = 1 \) otherwise no (Dirichlet)

(III) \( f(x) = x^2 + 1 \) \quad (Euler Conj. Yes)

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

BRUN: There are infinitely many \( x \) such that \( f(x) \) has at most 20 prime factors
Saturation Number

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

$\iff$ (better for higher dimensions)

the least $r$ such that

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

$= \mathbb{A}^1.$

BRUN: for any $f$

$r_0(Z,f)$ is finite!

More generally let

$\mathcal{O} = a \cdot \Gamma, \Gamma \leq \text{SL}_n(Z)$

be the orbit of $a \in \mathbb{Z}^n$ under $\Gamma$. 
Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$

Set $\tau_0(0, f)$ the least $r$ (if it exists) such that

$$2\ell\left(\sum_{x \in \mathcal{O}} f(x) \text{ has at most } r \text{ prime factors}\right)$$

$$= 2\ell(\mathcal{O}).$$

---

Enemy is a torus (for saturation)

Eq $\mathcal{O} = \mathbb{Z} = \{2^m : m \in \mathbb{Z}\} \subset \text{GL}_1(\mathbb{Q})$

a torus.

Set $F(x) = (2^m - 1)(2^m - 2)$

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. \( \tau_0(P, F) = \infty \).

---

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)

\[
\text{Let } \ P \leq \text{GL}_n(Z), \ O = \text{a.p} \subset \mathbb{Z}^n
\]

If \( G = \text{Zcl}(P) \) is Levi semi-simple (i.e. \( \text{rad} G \) contains no torus) then for \( f \in \mathbb{Z}[x_1, \ldots, x_n] \) with \( f|_{\text{Zcl}(O)} \not\equiv 0 \), there \( \tau_0(O, f) < \infty \). That is there is an \( \mu < \infty \) (effective but not feasible) s.t.

\[
\text{Zcl} \left\{ x \in O : f(x) \text{ has at most } \mu \text{ prime factors} \right\} = \text{Zcl}(O).
\]
This applies to integral apollonian packings. For these and certain f's there are some gems.

**Theorem (5.07):**

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

\[ \tau_0 (O_a, x_1) = 1 \]

\[ \tau_0 (O_a, x_1, x_2) = 2. \]
Zaremba's Conjecture:

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

with

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

continued fraction

$$a_j \leq A.$$ 

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

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

$$[i \ a]$$

$1 \leq a \leq A$

$$[i \ a_1][i \ a_2] \ldots [i \ a_k] = [\ast \ b]$$

$\iff$

$$\frac{b}{q} = [a_1, a_2, \ldots, a_k].$$
So the conjecture is equivalent to the orbit of $(0,1)$ under $\Gamma A$ having second coordinate $q$ for any given $q \geq 1$. $\Gamma A$ is "thin". This is a 'local to global' question for thin semi groups.

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, Katz, Tao)**

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

\[
|A+A| + |A.A| \geq |A|^{1+S}.
\]
Some references:

1) A. Lubotzky "Expander graphs in pure and applied Math" 
   BAMS 43 (2006) 439-561

2) P. Sarnak "Integral Apollonian Packing" 

3) J. Bourgain - A. Gamburd - P. Sarnak 

4) H. Helfgott 

5) L. Pyber and E. Szabo "Growth in finite simple groups of Lie type" 
   ArX.1001.4558

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

7) P. Varju "Expansion in SLd(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