Jean Bourgain
Institute for Advanced Study
Princeton, NJ 08540

PRIMES IN LINEAR GROUPS

Joint work with

A. Gamburd, A. Kontorovich, P. Sarnak

Primes and pseudo-primes in orbits of groups acting on $\mathbb{Z}^n$

Translation groups: Classical

Matrix groups: BGS

Classical setting of translation groups

Hardy-Littlewood n-tuple conjecture

L: subgroup of $\mathbb{Z}^n$ of rank $1 \leq r \leq n$ acting by translation $\mathcal{O} = c + L$ orbit of $c \in \mathbb{Z}^n$

Assume that for each $q \geq 1$ there is an $x = (x_1, \ldots, x_n) \in \mathcal{O}$ such that $x_1 x_2 \ldots x_n \in (\mathbb{Z}/q\mathbb{Z})^*$ (no local obstruction)

Then there are infinitely many elements in $x \in \mathcal{O}$ with $x_1, \ldots, x_n$ prime and this set is Zariski dense in $Zcl(\mathcal{O})$

EXAMPLES:

Dirichlet's Theorem ($r = n = 1$)

primes in progressions

Vinogradov: $n = 3, r = 2$

Green–Tao: $n = 4, r = 2$

Twin Prime Conjecture: $n = 2, r = 1$

Schinzel Conjecture

$\mathcal{O}$: orbit of a nontrivial subgroup L of $\mathbb{Z}$ acting on $\mathbb{Z}$ by translation

$f_1(x), \ldots, f_k(x) \in \mathbb{Q}[X]$ integral and irreducible.

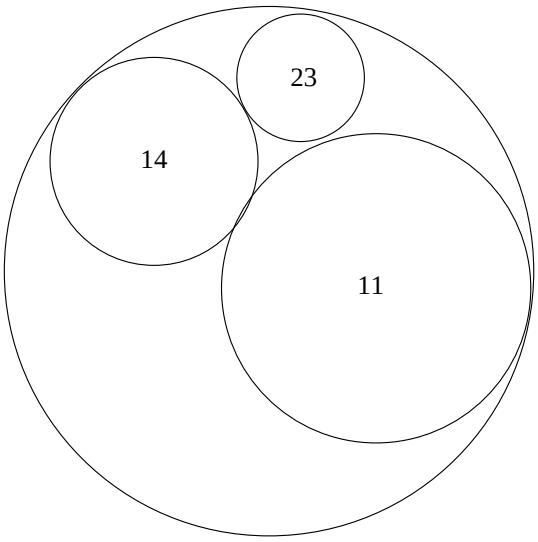
If no local obstructions, then there are infinitely many x at which $f_j(x)$ are simultaneously prime

Only pseudo-prime results

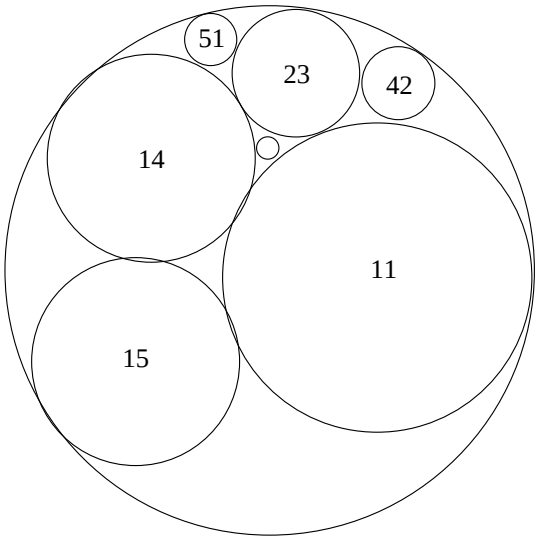
Orbits of Linear Groups

Example: Integral Appolonian packings

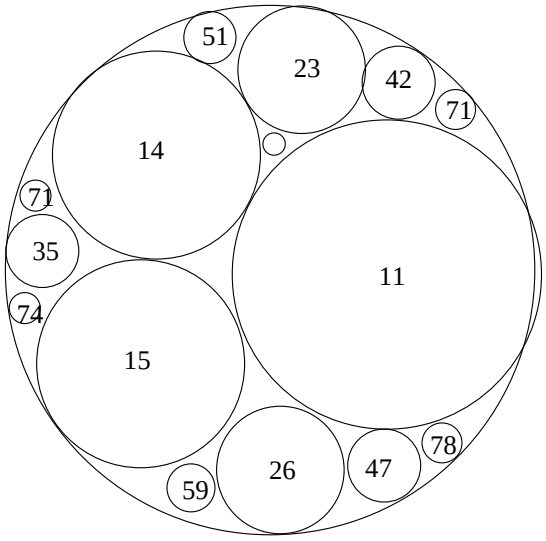
Curvatures of $\mathbb{b} = (-6, 11, 14, 23)$ packing



Generation 1



Generation 2



DESCARTE FORM

$F(x_1, x_2, x_3, x_4) =$

$2(x_1^2 + x_2^2 + x_3^2 + x_4^2) - (x_1 + x_2 + x_3 + x_4)^2$

$O_F =$ Orthogonal group

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

$=$ Appolonian packing group

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

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

Appolonian packings $\leftrightarrow$ orbits $O = A\mathfrak{b}$

CONJECTURE (BGS)

($SL_2(\mathbb{Z})$ analogue of Dirichlet's Theorem)

Λ non-elementary subgroup of $SL_2(\mathbb{Z})$

$b \in \mathbb{Z}^2$ primitive vector

$\mathcal{O} = \{gb | g \in \Lambda\}$

$\pi(\mathcal{O}) = \{x \in \mathcal{O} | x_1, x_2 \text{ are prime}\}$

Then

$$\pi(\mathcal{O}) \text{ is Zariski dense in } \mathbb{A}^2$$

if no local obstruction:

For every $q \geq 2$, there is $x \in \mathcal{O}$ such that

$$x_1 x_2 \in (\mathbb{Z}/q\mathbb{Z})^*$$

$\Lambda \subset SL_2(\mathbb{Z}) \qquad \delta(\Lambda) > 0$

$r(z)$= number of prime factors of $z \in \mathbb{Z}\backslash\{0\}$

Theorem. *There is a constant* $C(\Lambda)$ *such that for* $N \to \infty$

$$\left|\left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Lambda \middle| \|\gamma\| < N, r(abcd) < C(\Lambda)\right\}\right|$$

$$> \frac{N^{2\delta}}{(\log N)^4}$$

and Zariski dense in SL_2

Theorem.

Let $f \in \mathbb{Q}[x_1, x_2, x_3, x_4]$ *taking integer values on* Λ *and not a multiple of*

$$g(x_1, x_2, x_3, x_4) = x_1x_4 - x_2x_3 - 1$$

There is $r = r(\Lambda) \in \mathbb{Z}_+$ *s.t.*

$\{x \in \Lambda | f(x)$ *has at most* r *prime factors*$\}$

is Zariski dense in SL_2

Theorem

There is $\delta_0 < 1$ *such that if* $\delta(\Lambda) > \delta_0$ *and* $1 \leq i, j \leq 2$, *then* Λ *has infinitely many elements* x *with* x_{ij} *prime, provided no local obstruction.*

Moreover

$$\left|\{x \in \Lambda; \|x\| \leq N \text{ and } x_{ij} \text{ prime}\}\right| \sim \frac{N^{2\delta}}{\log N}$$

Ingredients

• Expansion of $SL_2(q)$ Cayley graphs (arithmetic combinatorics)

• Lax-Phillips/Lalley theory of counting in orbits of linear groups

• Extension of Selberg's eigenvalue theorem

• Estimates on bilinear forms

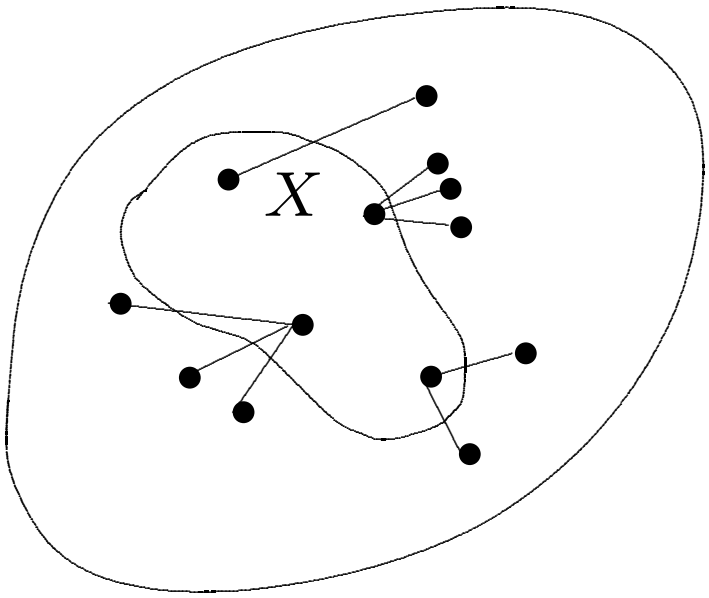
• Sieving Theory

EXPANDER GRAPHS

$\mathcal{G}$ = graph on vertex set V

Expansion coefficient of $\mathcal{G}$

$$c(\mathcal{G}) = \min_{|X|<\frac{1}{2}|V|} \frac{|\partial X|}{|X|}$$



CAYLEY GRAPHS

$V =$ finite group

$S =$ symmetric generating set

$\mathcal{G} = \{(x, y) \in V \times V | xy^{-1} \in S\}$

$= \mathcal{G}(V, S)$

Theorem

Let S be a finite subset of $SL_2(\mathbb{Z})$ generating a non elementary subgroup Λ

Then there is $q_0 \in \mathbb{Z}$ such that the family of Cayley graphs

$$\mathcal{G}(SL_2(\mathbb{Z}/q\mathbb{Z}), \pi_q(S))$$

$(q, q_0) = 1$ and q square free forms a family of expanders

Selberg: $[SL_2(\mathbb{Z}) : \Lambda] < \infty$

SUM-PRODUCT THEOREM
IN $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Theorem. (BKT).

For all $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$ and $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| > c|A|^{1+\delta}$$

Extensions to:

Arbitrary finite fields $\mathbb{F}_{p^r}$

$\mathbb{Z}/q\mathbb{Z}$

O/I ($\mathcal{O} =$ integers in numberfield)

SCALAR SUM-PRODUCT THEOREMS

$\Downarrow$

PRODUCT THEOREMS IN MATRIX SPACE

Theorem. (**HELFGOTT**)

$$G = SL_2(p)$$

Assume $A \subset G$ *generates* G *and*

$|A| < |G|^{1-\varepsilon}$

Then

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

HYPERBOLIC LATTICE POINT COUNTING

Λ acting on $\mathbb{H} = \mathbb{H}^2 = \{x + iy \in \mathbb{C} | y > 0\}$

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \quad gz = \frac{az+b}{cz+d}$$

$$\|g\|^2 = a^2 + b^2 + c^2 + d^2 = 4u(gi, i) + 2$$

$$\cosh d_H(z, w) = 1 + 2u(z, w)$$

$$u(z, w) = \frac{|z - w|^2}{4\text{Im}\, z\, \text{Im}\, w}$$

$L = L(\Lambda) \subset \mathbb{R} =$ limit set of Λ

$\delta = \delta(L) =$ Hausdorff dimension of $L \quad (0 < \delta \leq 1)$

$$|B_N = \{\gamma \in \Lambda |\ \|\gamma\| < N\}| \sim N^{2\delta}$$

$\delta > \frac{1}{2}$ LAX-PHILLIPS (wave equation methods)

$\delta \leq \frac{1}{2}$ LALLEY (methods from symbolic dynamics)

CASE $\delta(L) > \frac{1}{2}$

Spectrum of Laplace operator on $\Lambda\backslash\mathbb{H}$

$$0 \leq \underset{\substack{\| \\ \delta(1-\delta)}}{\lambda_0(\Lambda)} < \lambda_1(\Lambda) \leq \ldots \leq \lambda_{\max}(\Lambda) < \frac{1}{4} \xrightarrow[\text{continuous}]{\qquad\qquad}$$

Theorem. (LAX-PHILLIPS)

$$\lambda_j = \delta_j(1-\delta_j) \qquad \delta_0 = \delta$$

$$|\{\gamma \in \Lambda | d_H(w, \gamma w_0) \leq s\}| =$$

$$\sum_{j \geq 0} C_j \varphi_j(w) \varphi_j(w_0) e^{\delta_j s} + 0(e^{\frac{1}{3}(1+\delta_0)s})$$

Corollary.

$$|\{\gamma \in \Lambda | \ \|\gamma\| \leq N\}| \sim N^{2\delta} + 0\big(N^{2\delta_1}\big)$$

SELBERG'S THEOREM

AND CONJECTURE

$$\Gamma(q) = \left\{\gamma \in SL_2(\mathbb{Z}) : \gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\, q)\right\}$$

Theorem. (SELBERG) $\lambda_1\Big(\Gamma(q)\Big) \geq 3/16$

Conjecture. (SELBERG) $\lambda_1\Big(\Gamma(q)\Big) \geq \frac{1}{4}$

(no exceptional eigenvalues)

Theorem. (KIM-SARNAK) $\lambda_1\Big(\Gamma(q)\Big) > \frac{1}{4} - \Big(\frac{7}{64}\Big)^2$

GENERALIZATION OF SELBERG'S THEOREM

$$\Lambda = \langle S \rangle \subset SL_2(\mathbb{Z}) \quad \delta(\Lambda) > \frac{1}{2}$$

$$\Lambda_q = \{\gamma \in \Lambda : \gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{q}\}$$

$$\lambda_0(\Lambda_q) = \lambda_0(\Lambda)$$

Theorem. $\lambda_1(\Lambda_q) > \lambda_0 + \varepsilon$

$\varepsilon = \varepsilon(\Lambda) > 0$ *and all square-free* $q \geq 1$

$L^2(\Lambda_q \backslash \mathbb{H}) \leftrightarrow H_q$ *equivariant functions on*

$$(\Lambda \backslash \mathbb{H}) \times SL_2(q)$$

Proof of spectral gap based on expansion of

$$\mathcal{G}(SL_2(q), \pi_q(S))$$

Earlier work by **A. Gamburd** for $\delta(\Lambda) > 5/6$

Corollary.

$q \in \mathbb{Z}_+, q$ *square-free*

$(q, q_0) = 1$

$g \in SL_2(q)$

$$|\{\gamma \in \Lambda |\ \|\gamma\| \leq N \text{ and } \pi_q(\gamma) = g\}|$$

$$\sim \frac{N^{2\delta}}{|SL_2(q)|} + 0(q^C N^{2\delta - \varepsilon})$$

with ε, C *depending on* Λ

GENERAL CASE

(no L^2-spectral theory for $\delta(\Lambda) \leq \frac{1}{2}$)

$\Lambda = \langle T_1, \ldots, T_k \rangle$ Schottky group with no parabolics

$\Lambda \leftrightarrow \sum_*$ = finite sequences on $\{\pm 1, \ldots, \pm k\}$ compatible with transition matrix

L = limit set of Λ

$F : L \to L$ NIELSEN map

$f = \log |F'|$ distortion function

$(L, F) \leftrightarrow (\sum, \sigma)$ finite type shift

$\mathcal{F} = \mathcal{F}_\rho =$ Hölder functions on $\sum$

Perron-Frobenius-Rulle transfer operator

$$(\mathcal{L}_z\varphi)(x) = \sum_{\sigma y = x} e^{zf(y)}\varphi(y) \quad (z \in \mathbb{C})$$

Theorem. (LALLEY-NAUD)

- $(I - \mathcal{L}_z)^{-1}$ *meromorphic on* $Rez < -\delta + \varepsilon$ *with simple pole at* $z = -\delta$

- $\|(I - \mathcal{L}_z)^{-1}\| < C(1 + |Imz|^2)$ *for* $|z| \to \infty$

- $|\{\gamma \in \Lambda | d_H(i, \gamma(i)) \leq s\}| = Ce^{\delta s} + 0(e^{(\delta - \varepsilon)s})$

Corollary.

$$|\{\gamma \in \Lambda|\ \|\gamma\| \leq N\}| \sim N^{2\delta} + 0(N^{2\delta-\varepsilon})$$

CONGRUENCE SUBGROUPS

Theorem. q square-free, $(q, q_0) = 1$

$$g \in SL_2(q)$$

$$|\{\gamma \in \Lambda|\ \|\gamma\| \leq N \text{ and } \pi_q(\gamma) = g\}| \sim$$

$$\frac{N^{2\delta}}{|SL_2(q)|}\Big(1 + 0\Big(N^{-\frac{1}{\log\log N}}\Big)\Big) + q^C N^{2\delta-\varepsilon}$$

Extended action of $\mathcal{L}_z$ on $\mathcal{F}\big(\sum \times SL_2(q)\big)$

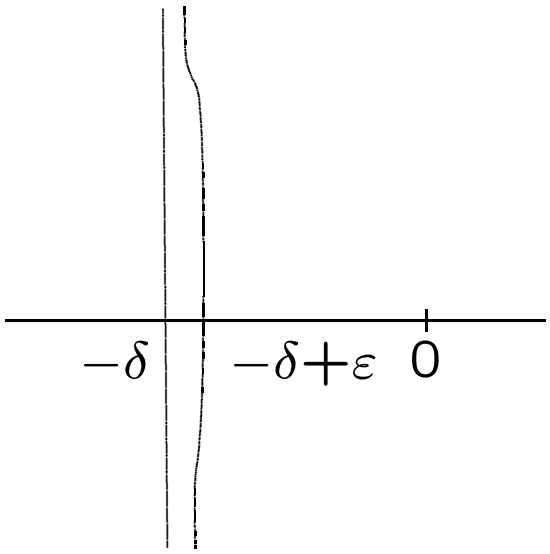
Extended action of $\mathcal{L}_z$ on $\mathcal{F}\big(\sum \times SL_2(q)\big)$

$$\ell^2\big(SL_2(q)\big) = \mathbb{R} \underset{q_1|q}{\oplus} E_{q_1}$$

Main estimate for $\mathcal{L}_z$ on $\mathcal{F}_{E_q}(\sum) = \mathcal{F}^{(q)}$

Proposition. $(I-\mathcal{L}_z)^{-1}\big|_{\mathcal{F}^{(q)}}$ holomorphic on

$$Re z < -\delta + \varepsilon \ \min\Big\{1, \frac{\log q}{\log(1+|\mathrm{Im}\, z|)}\Big\}$$



$$\|(I-\mathcal{L}_z)^{-1}\| < (q+|\mathrm{Im}\, z|)^C$$

Role of Expansion

Theorem.

μ probability measure on $SL_2(q)$
(q square free)

Assume

$$\mu(aH) < [G : H]^{-\kappa}$$

for all $H < SL_2(q)$ and $a \in SL_2(q)$

Then for $\varphi \in E_q$

$$\|\mu * \varphi\|_2 \leq q^{-\kappa'} \|\varphi\|_2$$

where $\kappa' = \kappa'(x) > 0$

(new proof by **P. Varju**)

Primes for δ near 1

$$\delta(\Lambda) > \delta_0$$

$$\Lambda_N = \{x \in \Lambda; \|x\| \leq N\}$$

$$|\Lambda_N| \sim M^{2\delta}$$

Main Issue

Exponential sums $\sum_{x \in \Lambda_N} e(x_{ij}\theta)$ on $\mathbb{T}$

Major arcs: analysis on $\Lambda\backslash\mathbb{H}$ and $\Lambda\backslash C$ use of spectral theory and gaps

Minor arcs: estimates on bilinear forms

Lemma. *$N \in \mathbb{Z}_+$ large*

$$Q < N^{\frac{1}{2}}$$

$$\beta \in \mathbb{R}, |\beta| < \frac{1}{QN^{\frac{1}{2}}}$$

$$P = P_{Q,\beta} = \left\{\tfrac{a}{q} + \beta \middle| (a,q) = 1 \text{ and } q \sim Q\right\} \subset \mathbb{T}$$

Let μ, ν be probability measures on $\mathbb{Z}^2$

$$\text{supp}\,\mu \subset B(0, N^{3/4}) \qquad \text{supp}\,\nu \subset B(0, N^{1/4})$$

Then

$$\sum_{\theta \in P} \Big| \sum_{x,y} e^{2\pi i \theta \times x.y} \mu(x)\nu(y) \Big| \lesssim$$

$$N^{\frac{5}{4}} \Big(QN^{-\frac{1}{8}} + Q^{\frac{1}{2}} \Big) \|\mu\|_\infty^{\frac{1}{2}} \|\nu\|_\infty$$