UNIVERSITY OF PENNSYLVANIA

Department of Mathematics

Fall 2006 - *Hans Rademacher Lectures in Mathematics*

Peter Sarnak
Department of Mathematics
Princeton University

will speak on

Equidistribution and Primes

Problems of existence of the (infinitely many) primes satisfying constraints, for example, twin primes or primes in progressions, have fascinated mathematicians for centuries. While many such problems remain unsolved, there have been fine achievements. After reviewing some of these we discuss some of the powerful methods that have been developed. These include analytic tools, specifically L-functions and also sieve methods. The latter are particularly effective for producing almost primes. The traditional viewpoint for these problems in general is to search for primes lying on varieties. However, this is necessarily limited by the lack of understanding of integral points. The point of view that we will develop is that these problems are naturally associated with finding primes on orbits of a group acting on Z^n and for which a theory can be developed.

Review of some old and recent achievements and basic conjectures
Tuesday....September 19, 2006....3:30pm....A8 DRL

Sieve methods and some applications
Wednesday....September 20, 2006.....4:30pm...A6 DRL

Equidistribution in integer orbits
Expander and congruence graphs
Thursday....September 21, 2006....4:30pm...A2 DRL
(lecture will end at 6:00pm)

Lectures will be held in the David Rittenhouse Laboratory,

RADEMACHER LECTURES (2006)

PRIMES:

ERATOSTHENES SIEVE (200 BC)

. If one strikes out (sieves) all multiples of primes $p \leq z$ then the integers $n \leq x$ ($x = z^\beta$) $\beta > 1$ have at most

r = integer part of β prime factors

So $\beta < 2$ then only primes are left.

Defn: We call a number n which has at most r prime factors an r-almost prime.

② Questions (ancient ones)

(i) are there infinitely many primes?

(ii) are there infinitely many twin primes?

(i) Yes (Euclid); $p_1, \ldots, p_k$, $p_1 \cdots p_k + 1$.

(ii) Not known - surely yes

Why is (ii) of interest?

Mainly curiosity — if you are not curious about (ii) you will probably not be interested in the rest of what I say.

Local Congruence Obstructions:

- One doesn't look for pairs $n, n+1$ both prime.
- One doesn't look for triples $n, n+2, n+4$ all prime because mod 3 at least one is 0.
- On the other hand triples $n, n+2, n+6$ have no local obstructions and one might (and we do) expect that there are infinitely many triples

5,7,11 ; 11,13,17 ; 17,19,23 ; 41,43,47 ; .....

(3) Euler (1737) (analytic methods)

$$\prod_p \frac{1}{1-p^{-s}} = \prod_p \left(1 + p^{-s} + p^{-2s} \cdots\right) = \sum_{n=1}^{\infty} n^{-s}$$

$$:= \zeta(s).$$

For $s > 1$.

As $s \to 1$, $\sum \frac{1}{n} = \infty \Rightarrow \sum_p \frac{1}{p} = \infty$.

Primes in progressions:

Fix $q > 1$, $a \in \mathbb{Z}$

$$n = mq + a \quad , m \geq 1$$

- Local obstruction for infinitely many primes is

$$\gcd(a, q) = (a, q) = d > 1.$$

THEOREM Dirichlet (1837) (local to global)

If $(a, q) = 1$ then there are infinitely many primes $p \equiv a \pmod{q}$.

④ His proof introduces characters χ of $(\mathbb{Z}/q\mathbb{Z})^*$ and generalizations of $\zeta(s)$ called $L(s,\chi)$.

Quantitatively (which is at the heart of all proofs)

$$\psi(x;q,a) := \sum_{\substack{p \le x \\ p \equiv a (q)}} \log p \,,$$

here it is best to "weight p" by $\log p$.

$$\psi(x) \sim x \qquad \text{(prime number theorem)}$$

$$\psi(x;q,a) \sim \frac{x}{\phi(q)} \,, \quad \phi(q) = \left|(\mathbb{Z}/q\mathbb{Z})^*\right|$$

as $x \to \infty$

Level of equidistribution:

GRH for Dirichlet's L-functions $\Rightarrow$

GRAND RIEMANN HYPOTHESIS

$$\psi(x;q,a) - \frac{x}{\phi(q)} = O\left(x^{1/2}(\log x)^3\right)$$

uniform in q!

THEOREM (BOMBIERI, A. VINOGRADOV 1965)

$$\sum_{q<Q} \max_{(a,q)=1} \left|\psi(x;q,a) - \frac{x}{\phi(q)}\right| \ll x/(\log x)^A$$

for $Q = x^{1/2}/(\log x)^B$ where $B = B(A)$.

("This gives what GRH gives "on average".)

Return to twin primes and generalizations

HARDY-LITTLEWOOD k-tuple Conjecture:

(local to global principle)

Fix $a_1, \ldots, a_k \in \mathbb{Z}$ then

$$m+a_1, m+a_2, \ldots, m+a_k \qquad m \geq 1$$

are all prime for infinitely many m iff there is no local congruence obstruction (i.e. iff $a_1, a_2, \ldots a_k$ don't exhaust all residue classes mod p, some $p \geq 2$)

What is the general context for these problems?

$(n+a_1, n+a_2, \ldots, n+a_k)$ is a line in affine k-space $\mathbb{A}^k$

- The traditional setting is then

$V \subset \mathbb{A}^k$ a variety defined over $\mathbb{Z}$

seek points $x \in V(\mathbb{Z})$ for which $f_1(x), f_2(x), \ldots, f_t(x)$ are all prime, where $f_j \in \mathbb{Z}[X_1, \ldots, X_k]$.

- The trouble is that in view of the negative solution to Hilbert's 10th problem we cannot analyze $V(\mathbb{Z})$ in general.
- For special V's which are given by additive equations in many variables The circle method has proven to be an effective tool.

We take a different route by putting these problems in group theoretic/dynamical context.

~~We take a different point of view:~~

- $\mathbb{Z}^k \subset \mathbb{A}^k$ affine k-space with Zariski topology
- P^k all $x \in \mathbb{Z}^k$ s.t. $x_j = \pm$ prime (the reason for $\pm$ will be clear later)
- Group theoretic formulation of the generalized tuple-conjecture.

CONJECTURE 1 (local to global)

Let $0 \neq L < \mathbb{Z}^k$, $b \in \mathbb{Z}^k$ and $V = L + b$, the orbit of b under L, then

$$Zcl(V \cap P^k) = Zcl(V)$$

iff local congruence obstructions are passed (i.e. for $q > 1$ there is $x \in V$ s.t. $x_1 x_2 \cdots x_k \in (\mathbb{Z}/q\mathbb{Z})^*$,

- this needs only be checked for finitely many q). $\longrightarrow$

What is known? Some special cases:

(i) $k=1$ is Dirichlet's Theorem.

(ii) I. Vinogradov's methods (1941)
(circle method + estimation of certain exponential sums over primes + sieve)

$\Rightarrow$ If $L \subset \mathbb{Z}^3$ and $\operatorname{rank}(L) \geq 2$ and nondegenerate, then Conjecture 1 is true.

(iii) Green-Tao (2006)

If $L \subset \mathbb{Z}^4$ and $\operatorname{rank}(L) \geq 2$ and is nondegenerate then Conjecture 1 is true.

(they use Vinogradov's methods + methods of Gowers and Furstenberg... in connection with Szemerédi's theorem + sieve).

• In general elementary combinatorial sieve methods (V. BRUN (1919), ...) are powerful for producing <u>almost</u> primes and to give sharp upper bounds (up to a constant factor) for $\#(V \cap \mathcal{P}^k) \cap \mathrm{Box}(X), X \to \infty$

● Conjecture 1 is true with $\mathcal{P}^k$ replaced by $\mathcal{P}^k_r = \{(x_1, \dots x_k) : x_j \text{ is an } r \text{ almost prime}\}$

with $r = r(k)$.

• Much modern effort go into reducing r.

<u>Eg</u>: $L \subset \mathbb{Z}^2$, $L = m\begin{bmatrix}1\\1\end{bmatrix}$, $b = \begin{bmatrix}0\\2\end{bmatrix}$ i.e twin primes

V. BRUN (1919): $x_1 - x_2 = 2$ with x_j, 9-almost prime and infinitely many x's.
H. RADEMACHER (1923) same with 7-almost prime
R. CHEN (1973) x_1 prime, x_2 2 almost prime.

Generalizing Conjecture 1:

Setting "ORBITS":

Let $\phi_1, \ldots, \phi_v$ be invertible polynomial maps of $\mathbb{A}^n$ with integral coeff.

$L = \langle \phi_1, \ldots, \phi_v \rangle$ is a group of motions of $\mathbb{Z}^n$ and $V = L\upsilon$ an orbit.

Let $I \lhd \mathbb{Z}[x_1, \ldots, x_n]$ given by

$$I = \{ f : f(x) = 0 \text{ for } x \in V \}$$

and

$f_1, \ldots f_t$ prime in the ring

$\mathbb{Z}[x_1, \ldots, x_m]/I$.

Are there points $w \in V$ s.t. $f_j(w)$ is prime for each j if the local obstructions are passed?

The natural measure of there being many w's is that

$$\{x \in V : f_j(x) \text{ is prime}\}$$

be Zariski dense in $Zcl(V)$.

• If the ϕ_j's are linear we can more or less develop a theory, at least to produce almost primes.

• Examples of nonlinear L's come from the action of the mapping class group on integral models of representation varieties Φ (Teichmuller spaces) of surfaces. This theory is still at its beginings and we wont discuss it here.

The very simplest nonabelian version of Conj 1 is:

CONJECTURE 2: (BOURGAIN-GAMBURD-S):
Let $L < SL_2(\mathbb{Z})$ be nonelementary (i.e. $Zcl(L) = SL_2$) and let $b \in \mathbb{Z}^2$ be primitive and $V = Lb$. Then

$$Zcl(V \cap P^2) = Zcl(V) \quad (= \mathbb{P}^2)$$

iff the local congruence obstructions are passed.

(i) the local obstructions read as follows – for $q>1$ there is $x \in V \bmod q$ such that

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

this involves only finitely many q's.

(ii) In the Conjecture we cannot L to be finite or even elementary infinite abelian

EG: $$L = \left\langle \begin{bmatrix} 7 & 6 \\ 8 & 7 \end{bmatrix} \right\rangle, \quad b = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

then

- there are no local obstructions
- $V \subset \{(x_1, x_2): 4x_1^2 - 3x_2^2 = 1\}$ and $V \cap P^2$ is empty (x_2 cannot be prime).

Moreover in this example the orbit V is too thin to carry out any kind of sieving. x_1 is a variation on the Fibonacci sequence for which like Mersenne primes $2^p - 1$, very little can be said, even about almost primality.

Recent press release: Sept 4, 06

$2^{32,582,657} - 1$ is prime, Cooper, Boone, ...

THEOREM (BOURGAIN-GAMBURD-S 2006)

Let $L < SL_2(\mathbb{Z})$ be nonelementary and b in $\mathbb{Z}^2$ primitive, and $V = Lb$. Let $f_1, \dots, f_t \in \mathbb{Z}[x_1, x_2]$ be distinct irreducible elements. There is $\tau = \tau(V, f_1, \dots, f_t)$ s.t. if $V_{f,\tau} = \{x \in V : f_j(x) \text{ is } \tau \text{ almost prime}\}$ then

$$Zcl(V_{f,\tau}) = Zcl(V) \quad (= \mathbb{P}^2).$$

Tools:

sieves, strong approximation, "expander graphs" and equidistribution in progressions, ...

- With $f_1(x) = x_1$, $f_2(x) = x_2$ the above yields Conjecture 2 with primes replaced by almost primes

As an **application** consider the familiar Pythagorean triangle $(5,4,3)$ and its orbit under $L = \langle A, B \rangle$ where

$$A = \begin{bmatrix} 19 & 18 & 6 \\ 18 & 17 & 6 \\ -6 & -6 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 9 & 8 & 4 \\ 8 & 7 & 4 \\ -4 & -4 & -1 \end{bmatrix}$$

L is Zariski dense (but of infinite index) in $SO_f(\mathbb{Z})$ where $f(x) = x_1^2 - x_2^2 - x_3^2$.

- There is $p < \infty$ s.t. the orbit of L contains a Zariski dense set of triples (x_1, x_2, x_3) for which $x_1 x_2 x_3$ is p almost prime.

- Among all pythagorean triples (x_1, x_2, x_3) those with the hypotenuse prime are Zariski dense (FERMAT).

- Conjecturally there are infinitely many triples with two sides prime (Sierpinski)

- The recent striking theorem of Friedlander and Iwaniec; $x^4 + y^2 = p$ for infinitely many p $\Rightarrow$ the set of triangles for which the average of two sides is a 4-th power and for which the hypotenuse is prime, is Zariski dense in the former.

Note:

It is critical that we allow for primes (or almost primes) to be negative. The condition $f(x)>0$ can secretly encode a diophantine equation and then we cannot have anything like a local to global principle.

According to Matijasevic, if $S \subset \mathbb{N}$ is recursively enumerable there is $f \in \mathbb{Z}[x_1, x_2, \dots, x_{10}]$ s.t.

$$\{ f(x)>0 : x \in \mathbb{Z}^{10} \} = S.$$

Eg: (i) $S = P^+$ positive primes — so clearly for x's with $f(x)>0$ there is no equidistribution of the type we need

(ii) We can choose S so that there are no local to global principles (or almost primes) on $f(x)>0$.

Another recent development using sieves + Bombieri-Vinogradov is

Goldston-Yildirim-Pintz (2006 Annals to appear.)

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0$$

p_n = n-th prime.

Even more interestingly they show if one has equidistribution of $p \equiv a(q)$ for $q \le Q$, Q larger than allowed by B-V (but a standard Conjecture)

$\Rightarrow$ $\exists$ $B < \infty$ s.t.

$p_{n+1} - p_n \le B$ for infinitely many n.

RADEMACHER LECTURE 2

• At present the technique to sieve on the orbit of a "thin" L, i.e. L is Zariski dense in a semi-simple, connected and simply connected G, has been carried out only for $G \cong SL_2$.

• In the case that $L \leq GL_n(\mathbb{Z})$ is a congruence subgroup of G as above (defined $/\mathbb{Q}$) and $L\backslash v$ is essentially the $\mathbb{Z}$-points of a variety $V/\mathbb{Q}$, we can use more standard techniques from the spectral theory of automorphic forms.

• As an explicit example, fix $n \geq 2$, $m \neq 0$ integers.

$$V_{n,m} = V = \{\text{integral } n \times n \text{ matrices of } \det = m\}$$

$L = SL_n(\mathbb{Z})$ acts on V by multiplication on left.

Let $\|\ \|$ be a norm on $MAT_n(\mathbb{R})$, $T \gg 1$

$$N_V(T) := \#\{X \in V : \|X\| \leq T\}$$

Then $N_V(T) \sim C_V T^{n^2-n}$, [DUKE-RUDNICK-S]

(2) (the exponent is consistent with heuristics;

there are $\approx T^{n^2}$ matrices with $\|X\| \leq T$,
and det is homogeneous of degree n,
so values of det lie in $[-cT^n, cT^n]$
so we hit in roughly T^{n^2-n} times)

Let $f_1, \ldots, f_t \in \mathbb{Z}[X_{ij}]$ which
as elements of the coordinate ring

$$\mathbb{C}[X_{ij}] / \langle \det X = m \rangle$$

generate distinct prime ideals.
Set;

$$P_{V,f} = \{ x \in V : f_j(x) \text{ is prime for each } j \}$$

$$P_{V,f}^{(r)} = \{ x \in V : f_1(x) f_2(x) \cdots f_j(x) \text{ is } r\text{-almost prime} \}.$$

THEOREM 1 (NEVO-S) (sharp up to a constant factor upper bounds for primes)

$$P_{V,\mathcal{F}}(T) \ll \frac{N_V(T)}{(\log T)^t}$$

THEOREM 2. (N-S): (lower bounds for almost primes)

$$P^{(\tau)}_{V,\mathcal{F}}(T) \gg \frac{N_V(T)}{(\log T)^t}$$

for any fixed $\tau \geq n^5 \left(\sum_{j=1}^{t} \deg f_j\right)$.

Corollary: For such τ,

$P^{(\tau)}_{V,\mathcal{F}}$ is Zariski dense in $\det X = m$

In the case that the f's are the coordinate functions themselves i.e. $f_{ij}(x) = x_{ij}$ we can use Vinogradov's methods:

(4) THEOREM 3 (NEVO-S)

$n \geq 3$, the set of $n \times n$ integral matrices whose determinant is m and whose coordinates are prime, is Zariski dense in $\det X = m$ iff m is even.

Note: the condition m even is exactly the local congruence obstruction.

For $n=2$, $ad-bc=m$ a,b,c,d prime

the above is not known.

Though Goldston-Graham have shown The above is true for some $2 \leq m \leq 26$.

(They show that the difference between two numbers which are a product of exactly 2 primes is at most 26 infinitely often)

V. BRUN's COMBINATORIAL SIEVE:

MODERN VERSION (SEE KOWALSKI-IWANIEC's BOOK 2005)

$n \geq 1$, $a_n \geq 0$ finite sequence.

$$\sum_{n \geq 1} a_n = X \qquad (X \to \infty).$$

sieve out all n's with prime factors $p \in \mathcal{Z}$, i.e.

$$S(A, \mathcal{P}) = \sum_{(n, \mathcal{P})=1} a_n$$

where $$\mathcal{P} = \prod_{p \notin \mathcal{Z}} p .$$

Under certain hypotheses on the sums of a_n over progressions, S can be estimated:

(A_0) $$\sum_{n \equiv 0 (d)} a_n = \frac{\rho(d)}{d} X + r(A,d)$$

where $\rho(d) < d$ is multiplicative in d

(A_1) r is small, at least on average

$$\sum_{d \le D} |r(A,d)| = O(X^{1-\varepsilon})$$

for some $\varepsilon > 0$ and $D = D(X)$ ($D = X^{\alpha}$ some $0 < \alpha < 1$)

(A_2) A has (sieve) dimension t

$$\sum_{p \le z} \frac{\rho(p)}{p} = t \log\log z + O(1) \quad \text{as } z \to \infty.$$

(A_3) $\exists K$ s.t. for $2 \le w \le z$

$$\prod_{w \le p \le z} \left(1 - \frac{\rho(p)}{p}\right)^{-1} \le K \left(\frac{\log z}{\log w}\right)^t$$

Then for $s > 9t + 10 \log K$ and $z = D^{1/s}$

$$\frac{X}{(\log X)^t} \ll S(A, \mathcal{P}) \ll \frac{X}{(\log X)^t}$$

Now

- $$\sum_{z \le p} a_p \le \sum_{(n, P_z)=1} a_n = S(A, P_z)$$

so we get upper bounds off only by a constant factor for the sum over primes.

- If $z = X^{\delta}$ and $n \le X$ and $(n, P_z) = 1$ then n has at most $1/\delta$ prime factors

$\Longrightarrow$ so $S(A, P_z)$ produces $1/\delta$ almost primes.

- Explain the upper bound by an elegant method of Selberg "λ^2-sieve".

For $\lambda_1, \lambda_2, \ldots \lambda_m, \ldots \in \mathbb{R}$ subject to $\lambda_1 = 1$

$$\sum_{(n, P_z)=1} a_n \le \sum_{n} \left(\sum_{d \mid n, d \le z} \lambda_d \right)^2 a_n$$

$$= \sum_n \sum_{\substack{d_1,d_2 \le z \\ d_j \mid n}} \lambda_{d_1} \lambda_{d_2} a_n$$

$$= \sum_{d_1,d_2 \le z} \lambda_{d_1} \lambda_{d_2} \left(\sum_{n \equiv 0 ([d_1,d_2])} a_n \right)$$

(A_0)

$$= \sum_{d_1,d_2 \le z} \lambda_{d_1} \lambda_{d_2} \frac{\rho([d_1,d_2])}{d_1 d_2} X$$

+ smaller

from A_1)

- ρ is multiplicative and Selberg explicitly minimizes the quadratic form

$$\sum_{\substack{d_1,d_2 \\ \le z}} \frac{\lambda_{d_1} \lambda_{d_2} \rho([d_1,d_2])}{d_1 d_2}$$

subject to the linear constraint $\lambda_1 = 1$

in terms of the asymptotics in (A_2).

A typical classical application is as follows

$f(x)$ irreducible over $\mathbb{Q}$ (eg x^2+1)

$$a_n = \sum_{\substack{|x| \le T \\ f(x)=n}} 1 \quad ,$$

so $$\sum_p a_p = \sum_{\substack{|x| \le T \\ f(x) \text{ is prime}}} 1$$

$$\sum_{n \equiv 0(d)} a_n = \sum_{\substack{|x| \le T \\ f(x) \equiv 0(d)}} 1 = \sum_{\substack{y \bmod d \\ f(y) \equiv 0(d)}} \left(\sum_{\substack{|x| \le T \\ x \equiv y(d)}} 1 \right)$$

↙

this is now a sum of integers in a progression

$$= \frac{2T}{d} + O(1) \; ; \quad \text{amenable of } \mathbb{Z} !$$

$$= \frac{\rho(d)}{d} T + \text{small}$$

$$\rho(d) = \#\{x \bmod d : f(x) \equiv 0 (d)\}$$

$\rho(d)$ is multiplicative and Chebotarev's Theorem gives A_2 and A_3.

In our setting $V = L\upsilon \subset \mathbb{Z}^n$.
we need to choose a suitable height function $\|\ \|_\Lambda$ on V to count its elements.

Set $$a_n = \sum_{\substack{x \in V \\ \|x\| \le T \\ |f(x)| = n}} 1$$

(note if $\|\ \|$ is defn!)

(here $f(x) = f_1(x) f_2(x) \cdots f_t(x)$, $f_j \in$ coordinate ring of $\overline{V}$)

To verify the sieve conditions for suitable parameters

$$\sum_{n \equiv 0 (d)} a_n = \sum_{\substack{x \in V \\ \|x\| \in T \\ f(x) \equiv 0 (d)}}' 1$$

$$= \sum_{\substack{y \bmod d \\ f(y) \equiv 0 (d)}}' \left(\sum_{\substack{x \in V \\ x \equiv y (d) \\ \|x\| \in T}} 1 \right)$$

This introduces a number of basic new problems coming from the nonamenability of L and understanding the reduction of V mod d.

. At least if $\| \ \|$ on V is based on choosing generators for L and word length to order points, these issues can be described in terms of graphs associated with the problem

Congruence Graphs: For our general setting:

$$L = \langle \phi_1^{\pm 1}, \dots, \phi_\nu^{\pm 1} \rangle$$

$$V = L\upsilon \subset \mathbb{Z}^n$$

For $q \geq 1$ let $V(q)$ be the reduction of V mod q

i.e. all $y \in (\mathbb{Z}/q\mathbb{Z})^n$ which are projections of points of V.

We make $V(q)$ into a graph by joining $y \in V(q)$ to $\phi_j^{\pm} y \in V(q)$ $j = 1, 2, \dots \nu$.

Then $V(q)$ is a connected 2ν-regular graph.

One needs to understand

(i) the variation of $\#V(q)$ with q, i.e. the multiplicativity of this function and the variation of $\#V(p)$ with p, prime.

• this come from algebra

(ii) a new feature in this nonabelian sieve, which is number theoretic/combinatorial.

→ To overcome the nonamenability of L we need uniform equidistribution rates for the reduction of V to $V(q)$ when ordered by $\|\ \|$, for q large in terms of X.

• This is more or less equivalent to $V(q)$ being an <u>expander</u> family.

(in special cases this is related to generalized Ramanujan Conjectures).

Definition of $V(q)$ being expanders

Let $\Delta: L^2(V(q)) \to L^2(V(q))$ be the adjacency operator

$$\Delta f(v) = \sum_{w \sim v} f(w)$$

$\lambda_1(\Delta)$ the biggest eigenvalue is $2r$.

There should be $\varepsilon_0 > 0$ such that the next biggest eigenvalue $\lambda_1(\Delta)$ satisfie $\lambda_1(\Delta) \leq \lambda_1(\Delta) - \varepsilon_0$, independent of q.

- The algebra part (i) is used to verify (A_0) and (A_2) in the sieve.

- The expander part (ii) is used to give a "level of distribution" D in (A_1) of the sieve. The bigger the spectral gap the larger we can take D and hence eventually τ is smaller.

Lecture 3

- The algebra part – the variation of $\#V(q)$ with q is more or less standard

(1) We use the (very) strong approximation theorem of Mathews–Vaaserstein and Weisfuller

- If L is Zariski dense in SL_n (or more generally G as before)

Then there is $M \leq M(L) < \infty$ s.t.

$$L \hookrightarrow \prod_{p > M} SL_n(\mathbb{Z}_p)$$

is dense (Their proof uses the classification of finite groups, Larsen and Pink have a new proof avoiding this)

- With this one can reduce the variation $\#V(p)$ to counting points mod p for p large

The expander property uses number theory and combinatorics which we discuss. | over finite fields

• If X is a compact Riemannian manifold, let $\lambda_0(X) = 0$ be the smallest eigenvalue of $-\Delta = -\text{div grad}$ "The Laplacian" on X and let $\lambda_1(X)$ be the next to smallest eigenvalue.

$$\lambda_1 = \inf_{\int_X \phi = 0} \frac{\int_X |\nabla \phi|^2 dV}{\int_X |\phi|^2 dV}$$

One might expect that if X_j is a sequence of such X with $\text{Vol}(X_j) \to \infty$ that $\lambda_1(X_j) \to 0$. The counter intuitive fact is that this need not happen and it's underlies the notion of "expanders".

For a recent survey of expanders and applications see the latest BAMS (Wigderson et al).

Counting lattice points in $\mathbb{H}^2$ (Delsarte)

$\mathbb{H} = \mathbb{H}^2$ is the hyperbolic plane

Γ a discrete group of motions

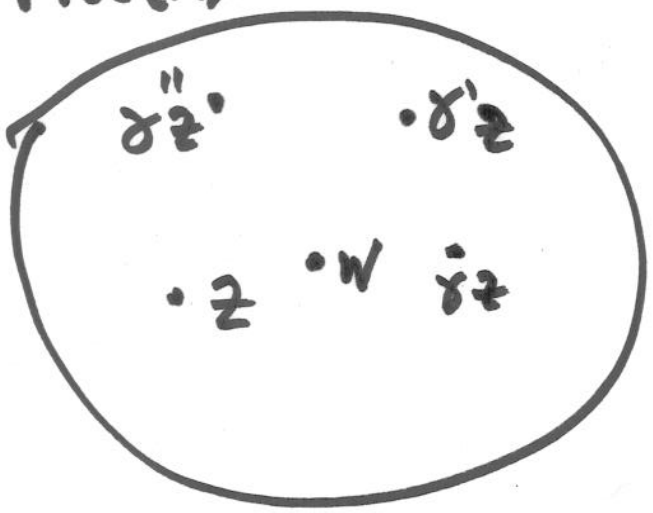
assume $X = \Gamma \backslash \mathbb{H}$ is compact.

$0 = \lambda_0 < \lambda_1 \leq \lambda_2 \leq \lambda_3 \cdots$

$\phi_0 \quad \phi_1 \quad \phi_2 \quad \phi_3 \cdots$

ϕ_j orthonormal basis of eigenfns of Δ

$$\phi_0 = \frac{1}{\sqrt{\mathrm{Vol}(X)}}.$$



$$\#\{\gamma \in \Gamma : d(\gamma z, w) \leq R\}$$

$$k(z,w) = k(\mathrm{dist}(z,w))$$

$$K(z,w) = \sum_{\gamma \in \Gamma} k(\gamma z, w) \in L^2(X \times X)$$

expand in ocnr o.n.b.

$$K(z,w) = \sum_j h_k(t_j) \phi_j(z) \overline{\phi_j(w)}$$

$\lambda_j = \frac{1}{4} + t_j^2$ and h_k is the Harish-Chandra transform

$$h_k(t_j) = \int_{\mathbb{H}} y^{1/2 + i t_j} k(z,i)\, dV(z) .$$

If $k_R(z,w) = \begin{cases} 1 & \text{if } \mathrm{dist}(z,w) < R \\ 0 & \text{otherwise} \end{cases}$

then

$$h_k(t_j) \sim \begin{cases} e^{(\frac{1}{2} + i t_j) R} & \text{if } t_j \in -i\mathbb{R} \\ O(e^{R/2}) & \text{if } t_j \in \mathbb{R} . \end{cases}$$

Hence for the simplest orbit counting

$$\sum_{\gamma\in\Gamma} k_R(z,\gamma w) = \#\text{ of images of } W \text{ by } \Gamma \text{ in ball radius } R$$

$$= \frac{e^R}{\mathrm{Vol}(X)} + \sum_{j\neq 0} h(t_j)\,\phi_j(z)\,\overline{\phi_j(w)}$$

$$= \frac{\mathrm{Vol}(\mathrm{Ball}(R))}{\mathrm{Vol}(X_\Gamma)} + O\left(e^{\alpha R}\right)$$

with $\alpha<1$ as long as $\lambda_1(X)\geq\varepsilon_0>0$.

Lax-Phillips: Carry out a similar theory for $X_L = L\backslash\mathbb{H}$ where X_L is of infinite volume (e.g. L infinite index in $SL_2(\mathbb{Z})$).

If Λ_L = limit set of L

= limit points in $\mathbb{R} \cup \{\infty\}$ of Lz_0.

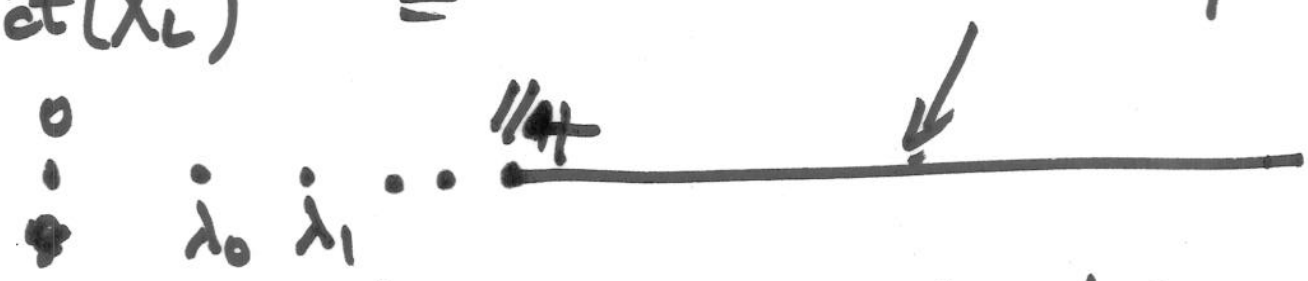
and $\delta(\Lambda_L) > \frac{1}{2}$ then

$$\lambda_0(X_L) = \delta(1-\delta) < \frac{1}{4}$$

(Patterson-Sullivan).

In this case $\phi_0(z) > 0$ and is in $L^2(X_L)$ and replaces the constant function in the asymptotics.

Spect(X_L) =



a finite no' of points in $(0, \frac{1}{4})$

The basis of the expander ~~is~~ comes from the modular case:

Selberg's Eigenvalue Conjecture:

$\Gamma(q)$ = principal congruence subgroup of $SL_2(\mathbb{Z})$, $q \geq 1$

$\Gamma(q)\backslash\mathbb{H}$ is a modular surface

Conjecture (Selberg 65):

$$\lambda_1(X(q)) \geq \frac{1}{4}.$$

Remarks:

(i) $\lambda_1 = \frac{1}{4}$ can occur!

One expects that this λ_1 happens iff the corresponding ϕ_1 is an automorphic "Maass" form corresponding to an even two-dimensional Galois representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

(ii) In general $\lambda_1(\Gamma\backslash\mathbb{H})$ can go to 0 as $\text{Area}(\Gamma\backslash\mathbb{H}) \to \infty$ with $\Gamma < SL_2(\mathbb{Z})$. Such Γ's will not be congruence subgroups of $SL_2(\mathbb{Z})$.

- Selberg using Weil's bounds for Kloosterman sums proved that

$$\lambda_1(\Gamma(q)\backslash\mathbb{H}) \geq \frac{3}{16}.$$

- Kim-S (2004)

$$\lambda_1(\Gamma(q)\backslash\mathbb{H}) \geq \frac{975}{4096} = 0.238\ldots$$

[This proof uses techniques from automorphic L-functions, and cases of "functoriality" proven by Kim-Shahidi and in particular the group E_8].

For our general problem we need similar results for $L < GL_n(\mathbb{Z})$. The case that L is a lattice is follows

G is a semisimple matrix group defined over $\mathbb{Q}$ (e.g. SL_n). $G(\mathbb{R})$ its real points, $G(\mathbb{Q})$ rational ones, $G(\mathbb{Z})$ its integral points and $\Gamma(\mathfrak{q})$ is a congruence subgroup of $\Gamma = G(\mathbb{Z})$. K a maximal compact subgroup of $G(\mathbb{R})$.

eg: $G = SL_n$, $G(\mathbb{R}) = SL_n(\mathbb{R})$, $K \cong SO_n(\mathbb{R})$ or any conjugate of it.

$S = G(\mathbb{R})/K$ is a Riemannian Symmetric space.

- In this context one should consider the full ring of invariant differential operators on S – not just the Laplacian Δ – we stick to the latter for simplicity.

The nature and location of the spectrum of $\Gamma(\mathfrak{q})\backslash G(\mathbb{R})/K$ is the content of the "Generalized Ramanujan conjectures".

Good approximations to these conjectures are now known after the works of many people:

1). Arthur in studying the discrete spectrum of these spaces has put forth general Conjectures which give strong limitations for the location of the spectrum.

2). For GL_n sharp bounds are known using techniques of families of Rankin-Selberg L-functions (Luo-Rudnick-S)

3). When functorial transfer to GL_n is available (Rogawski, Kottwitz, Arthur-Clozel, ...) one gets sharp bounds

4). The method automorphic duals via subgroups (Burger-S) gives bounds in most cases.

5). Local harmonic analysis – "unitary dual", yields nontrivial bounds when $G(\mathbb{R})$ has "property T", Vogan, Howe, J.S. Li, Hee Oh, ...

Combining the above and stabilizing the trace formula for certain unitary groups Clozel 2004 has proven:

- Let G be as above, there is an explicit $\varepsilon(G)>0$ (which is not small) such that

$$\lambda_1(\Gamma(q)\backslash G(\mathbb{R})/K) \geq \varepsilon(G) \text{ for } q \geq 1.$$

This suffices to control the equidistribution in progressions on orbits of $L \supset \Gamma(q)$ and to sieve.

L a thin (i.e. any Zariski dense) subgroup of $SL_2(\mathbb{Z})$

In these cases we have to give up automorphic forms and develop more elementary and combinatorial methods to prove the spectral bound.

Let $L < SL_2(\mathbb{Z})$ be of finite index (not necessarily congruence).

For $q \geq 1$, $L(q) = \ker$ of the reduction of L mod q; $X(q) = L(q)\backslash\mathbb{H}$.

- Xue-S (1990) give an elementary ~~methods~~ proof of a lower bound for $\lambda_1(X(q))$ in this context.

For $q \in P$ a large prime

$$\lambda_1(L(p)\backslash\mathbb{H}) \geq \min\left(\lambda_1(L\backslash\mathbb{H}), \frac{5}{36}\right) > 0$$

$\longrightarrow$

(so ~~whether~~ the only exceptional eigenvalues for $L(p)\backslash\mathbb{H}$ are in $(0, \frac{5}{36})$ are those that are already present for $L(1)\backslash\mathbb{H}$ and they could be present in this non congruence case.)

Idea of proof:

p large

$$X(p) = L(p)\backslash\mathbb{H}$$

$$\downarrow$$

$$X(1) = L\backslash\mathbb{H}$$

is a finite regular cover with deck group

$$L/L(p) \cong PSL_2(\mathbb{Z}/p\mathbb{Z})$$

(since there aren't many subgroups of the latter).

Hence if $0<\lambda$ is an eigenvalue of Δ on $X(p)$ and V_λ the corresponding eigenspace, then $PSL_2(\mathbb{Z}/p\mathbb{Z})$ acts on V_λ and we can assume this action is irreducible. If this action is trivial then the eigenfunction in V_λ lives on $X(1)$ and we are done. So we can assume the action is

nontrivial.

Frobenius classified all the representations of $PSL_2(\mathbb{Z}/p\mathbb{Z})$ and from the list (since V_λ is not trivial)

$$\dim V_\lambda \geq \frac{p-1}{2} \qquad (*)$$

So if a small eigenvalue exists it must have very high multiplicity.

Consider for R large to be chosen

$$K_R(z,w) = \sum_{\gamma \in L(q_0)} k_R(\gamma z, w)$$

$$= \sum_{t_j} h_R(t_j)\, \phi_j(z)\overline{\phi_j(w)} + \text{cts spectrum}$$

(Actually take $\widetilde{k} = k * k$ (in the algebra of such convolution operators) so that $\widetilde{h}_R(t_j) \geq 0$ for all the spectrum.)

Then $$\widetilde{K}_R(z,z) \geq h_R(t_\lambda) \sum_{\lambda_j \in V_\lambda} |\phi_j(z)|^2 \qquad (**)$$

Now integrate over z in a compact subset of $X(1)$ (together with technical considerations with cusps) yields

$$\widehat{K}_R(z,z) \geq \frac{h_R(t_\lambda)\, \dim V_\lambda}{\#\, PSL_2(\mathbb{F}_p)}$$

Now the l.h.s with say $z = i$ (or z in compact) is at most

$$\#\quad a,b,c,d \in \mathbb{Z}.$$
$$ad - bc = 1$$
$$a^2+b^2+c^2+d^2 \leq e^R \qquad -(\times\times)$$
$$a \equiv d \equiv 1 \,(p),\ b \equiv c \equiv 0 \,(p)$$

$\Rightarrow$ $a+d \equiv 2 \pmod{p^2}$!

So the no' of such points (first choose $a+d$ then d and then by is determined in at most e^{2R} ways by bound for divisor function)

$$\# \ll \left(\frac{e^{R/2}}{p^2}+1\right)\left(\frac{e^{R/2}}{p}+1\right)e^{\varepsilon R} \qquad (\text{XXXX})$$

Choosing $e^{R/3} = p$ yields

$$h_R(t_\lambda)\operatorname{dim} V_\lambda \ll e^{R(1+\varepsilon)}$$

or $$\operatorname{dim} V_\lambda \ll e^{R(1-2t_\lambda)}$$

Combined with (*) we get $\lambda \geq \frac{5}{36}$.

So the idea is a 'soft' upper bound together with (*) gives the spectral lower bound!

This was extended by Gamburd in 2000 to infinite volume!

* (Gamburd thesis 2000):

Let $L < SL_2(\mathbb{Z})$ of infinite index* and assume that $\delta(\Lambda_L) > 5/6$ (so $0 < \lambda_0(L\backslash\mathbb{H}) < 5/36$) then

$$\lambda_1(L(p)\backslash\mathbb{H}) \geq \min\left(\lambda_1(L(1)\backslash\mathbb{H}), \frac{5}{36}\right).$$

for p large, prime.

(*) we assume L is finitely generated

- The extension of the above to q square free suffice to carry out the sieve when $\delta(\Lambda_L) > 5/6$.

→

The relation between this spectral gap and that of the congruence graphs (expanders) for $(L/L(q), S)$ where S is a fixed set of generators for L, has its roots in the works of BROOKS and BUSER. In this infinite volume case it is trickier

Proposition (Gamburd, Bourgain, S)

L as above $\delta(L) > \frac{1}{2}$ so $\lambda_0 = \lambda_0(L\backslash\mathbb{H}) < 1/4$. Then $\lambda_1(L(q)\backslash\mathbb{H}) \geq \lambda_0 + \varepsilon_0$ for $\varepsilon_0 > 0$ independent of q iff $(L/L(q), S)$ is an expander family.

To handle the general L (i.e. $0<\delta(\Lambda_L)\leq 5/6$) we cannot appeal to (xxx) above and we ~~cannot~~ don't know how to count on the orbit with an archimedian ordering. Using word length ordering (with a fixed set of generators) one can use more combinatorics.

Theorem: (BOURGAIN. GAMBURD 2006):

$L<SL_2(\mathbb{Z})$, $2cl(L)=SL_2$.

S a fixed set of generators of L (symmetric) then the Cayley graphs

$(L/L(p), S)$, p prime, are an expander family.

This when extended to the case of square, which can be done, suffices

to execute the sieve when the orbits of L are ordered by word length.

The idea of the proof of the last is to do the Xue-S argument at the level of these graphs. $PSL_2(\mathbb{F}_p)$ acts on the eigenspaces as before and one needs an upper bound like (xxxx) which needs to be proven directly (after all we don't have an independent description of L in terms of any equations). The key new inputs to do this come from additive combinatorics:

Sum product:

The -ring conjecture of Erdos asserts that any Borel measurable subset of $\mathbb{R}$ which is also a ring

under + and × has dimension 0 or 1. This was proven by Edgar and Miller. A quantitative finite field analogue is as follows:

- **Theorem (Bourgain–Nets Katz–Tao):**

For $\varepsilon > 0$ there is $\delta(\varepsilon) > 0$ s.t. for any large p and $A \subset \mathbb{F}_p$ with $p^{\varepsilon} < |A| < p^{1-\varepsilon}$ we have

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

Using this and other insights Helfgott proved

- **Theorem** (Helfgott 2005)

given $\varepsilon > 0$ there is $\delta > 0$ s.t. if $A \subset SL_2(\mathbb{F}_p)$, $|A| \leq p^{3-\delta\varepsilon}$ and A is not contained in a proper subgroup then $|A.A.A| \geq |A|^{1+\delta}$.

The proof of the upper bound for the number of closed cycles of length $C\varepsilon.\log p$ in the graphs $(L/L(p), S)$ that is needed to complete the spectral gap bound, is done (by Gamburd and Bourgain) by relating that quantity to high power convolutions of the measure $\sum_{g \in S} \delta_g$. They show by combinatorial methods as above (in particular the Balog-Szemeredi / Gowers theorem) that once the mass is spread out (by Helfgott) repeated squaring flattens the measure.

To me it is quite striking that such combinatorics is used to prove the

ADDED:

"EXPANDER GRAPHS AND THEIR APPLICATIONS"
S. HOORY, N. LINIAL, A. WIGDERSON, BAMS VOL 43, 4, (2006) 439-561

G. EDGAR and C. MILLER PROC. AMS 31 (2003) 1121-1129

E. KOWALSKI "The principle of the large sieve" (2006)
www.math.u-bordeaux1.fr/~kowalski

[1] J. Bourgain, Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary, J. Analyse, in press.
[2] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$, preprint, 2005.
[3] J. Bourgain, A. Gamburd, P. Sarnak, Spectral sieving of thin sets, in preparation.
[4] J. Bourgain, A. Glibichuk, S. Konyagin, Estimate for the number of sums and products and for exponential sums in fields of prime order, Proc. London Math. Soc., in press.
[5] J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and applications, GAFA 14 (2004) 27–57.
[6] A. Gamburd, Spectral gap for infinite index "congruence" subgroups of $SL_2(\mathbb{Z})$, Israel J. Math. 127 (2002) 157–200.
[7] B. Green, T. Tao, Linear equations in primes, preprint.
[8] H. Halberstam, H. Richert, Sieve Methods, Academic Press, 1974.
[9] G.H. Hardy, J.E. Littlewood, Some problems of 'Partitio Numerorum': III. On the expression of a number as a sum of primes, Acta Math. 44 (1922) 1–70.
[10] H. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, preprint, 2005.
[11] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc., 2004.
[12] P.D. Lax, R.S. Phillips, The asymptotic distribution of lattice points in Euclidean and non-Euclidean space, J. Funct. Anal. 46 (1982) 280–350.
[13] A. Lubotzky, Cayley graphs: eigenvalues, expanders and random walks, in: P. Rowbinson (Ed.), Surveys in Combinatorics, in: London Math. Soc. Lecture Note Ser., vol. 218, Cambridge Univ. Press, 1995, pp. 155–189.
[14] C. Matthews, L. Vaserstein, B. Weisfeiler, Congruence properties of Zariski-dense subgroups, Proc. London Math. Soc. 48 (1984) 514–532.
[15] A. Nevo, P. Sarnak, in preparation.
[16] S.J. Patterson, The limit set of a Fuchsian group, Acta Math. 136 (1975) 241–273.
[17] P. Sarnak, What is an expander?, Notices Amer. Math. Soc. 51 (2004) 762–763.
[18] P. Sarnak, Notes on the generalized Ramanujan conjectures, Clay Math. Proc. 4 (2005) 659–685.
[19] P. Sarnak, X. Xue, Bounds for multiplicities of automorphic representations, Duke Math. J. 64 (1991) 207–227.
[20] A. Schinzel, W. Sierpinksi, Sur certaines hypotheses concernant les nombres premiers, Acta Arith. 4 (1958) 185–208.
[21] A. Selberg, On an elementary method in the theory of primes, Norske Vid. Selsk. Forh. 19 (1947) 64–67.
[22] A. Selberg, On the estimation of Fourier coefficients of modular forms, in: Proc. Sympos. Pure Math., vol. VII, Amer. Math. Soc., 1965, pp. 1–15.
[23] J. Tits, Free subgroups in linear groups, J. Algebra 20 (1972) 250–270.
[24] I.M. Vinogradov, Representations of an odd number as a sum of three primes, Dokl. Akad. Nauk SSSR 15 (1937) 291–294.