COUNTING PRIMES GROUPS and MANIFOLDS

A. Lubotzky

Hebrew University

Jerusalem, ISRAEL

Thm (Euclid) $\exists$ ∞ - many primes.

Pf (H. Furstenberg, Monthly AMS 56)

Put on $\mathbb{Z}$ a topology: $A \subseteq \mathbb{Z}$ is open iff $\forall x \in A, \exists\ 0 \neq d \in \mathbb{Z}$ s.t

$$x + d\mathbb{Z} \subseteq A$$

i.e., the arithmetic progressions form a basis for the topology.

Now, $\forall p$ prime $p\mathbb{Z}$ is open and closed, $\mathbb{Z} \setminus p\mathbb{Z} = \bigcup_{i=1}^{p-1} i + p\mathbb{Z}$

If there are only finitely many primes $p_1, \ldots, p_\ell$ then $\bigcup_{i=1}^{\ell} p_i\mathbb{Z}$ is closed. So $\mathbb{Z} \setminus \bigcup_{i=1}^{\ell} p_i\mathbb{Z}$ is open

but this is $\{\pm 1\}$ which is not open. Contradict

Thm (PNT – de la Vallée Poussin[96]/Hadamard[93])

$$\pi(x) \sim \frac{x}{\ln x}$$

where $\pi(x) = \#\{p \text{ primes} \mid p \leq x\}$

equiv: Let $\vartheta(x) = \sum_{p \leq x} \ln p$ then

$$\vartheta(x) \sim x$$

Write: $E(x) = |\vartheta(x) - x|$

Then

$$\text{R.H.} \iff E(x) = O_\varepsilon\left(x^{1/2+\varepsilon}\right) \quad \forall \varepsilon.$$

More generally: Let $a, q > 0 \in \mathbb{Z}$, $(a,q) = 1$.

Denote $\mathcal{P}(x; q, a) = \{p \leq x \mid p \equiv a\ (q)\}$

$\pi(x; q, a) = |\mathcal{P}(x; q, a)|$, $\vartheta(x : q, a) = \sum_{p \in \mathcal{P}(x:q,a)} \ln p$

Then: $\pi(x : q, a) \sim \frac{1}{\phi(q)} \frac{x}{\ln x}$, $\vartheta(x : q, a) \sim \frac{x}{}$

Subgroup Growth

Let Γ be a fin. gen. group.

$$a_n(\Gamma) = \#\{H \leq \Gamma \mid (\Gamma : H) = n\}$$

$$s_n(\Gamma) = \#\{H \leq \Gamma \mid (\Gamma : H) \leq n\} = \sum_{i=1}^{n} a_i$$

Ex: $\Gamma = F_r$ = free gp on r-gen's.

$$a_n(F_r) \sim n \cdot (n!)^{r-1}$$

Pf: $a_n(\Gamma) = \frac{1}{(n-1)!}$ trans. hom(Γ, S_n)

---- $\boxtimes$

Cor: $$\lim_{n\to\infty} \frac{\log s_n(F_r)}{\log n!} = r-1 = -(1-r) = -\chi(F_r).$$

Thm (Liebeck-Shalev, Muller-Puchta 04)

Γ a Fuchsian gp (e.g., free, surface gp).

$$\lim_{n\to\infty} \frac{\log s_n(\Gamma)}{\log n!} = -\chi(\Gamma).$$

So the growth for every fin. gen. gp is at most $n!^c$.

What about polynomial growth?

Thm (PSG; Lubotzky - Mann - Segal 84-92).

Let Γ be a fin. gen. ~~gp~~ residually finite group.

Γ has PSG (poly subgp growth, i.e. $s_n(\Gamma) \leq n^c$)

$\Longleftrightarrow$ Γ is virtually solvable of finite rank

Explanation:

1) Γ residually finite $\Leftrightarrow$ $\bigcap \{N \triangleleft \Gamma \mid (\Gamma : N) < \infty\} = \{e\}$.

2) virtually .... $\equiv$ $\exists$ finite index subgp with ....

3) finite rank $\equiv$ $\exists\, c$ s.t.

Counting Manifolds

Let M be a Riemannian manifold

$$b_n(M) = \# \text{ of } \le n\text{-covers of } M$$

Thm (Lubotzky – Nikolov 05
following: Goldfeld – L. – Pyber 05).

Assume $X = \tilde{M}$ = irr. sym space of rank ≥ 2 (not of type $D_4(\mathbb{C})$) and M of finite volume but not compact. Then:

$$\lim_{n\to\infty} \frac{\log b_n(M)}{(\log n)^2 / \log\log n} = \gamma(X)$$

i.e., the limit exists and is independent of M and depends only on X. $\gamma(X)$ is easily computed – see later.

The PSG thm. and the last thm. heavily depends on PNT.

In fact:

<u>Thm</u> (L.-N.) Assume G.R.H. (+ ε)

Then: $$\lim_{n\to\infty} \frac{\log b_n(M)}{(\log n)^2/(\log\log n)} = \gamma(X)$$

for every sym. space of rank ≥ 2 and every fin. volume M.

Let's start with PSG Thm.

The profinite topology

Γ fin. gen. gp.

$\mathcal{L} = \{ N \triangleleft \Gamma \mid [\Gamma : N] < \infty \}$

$\mathcal{L}_p = \{ N \triangleleft \Gamma \mid [\Gamma : N] = p^\alpha \}$

Ex: $\hat{\mathbb{Z}}$, $\mathbb{Z}_p$

If Γ an arithmetic group

i.e. $\Gamma = G(\mathcal{O})$ $\quad$ $\mathcal{O}$ = ring of integers in a number field k, G - a k-gp.

e.g. $\Gamma = SL_d(\mathbb{Z})$.

principal congruence subgroup - $I \triangleleft \mathcal{O}$

$\Gamma(I) = \mathrm{Ker}(G(\mathcal{O}) \to G(\mathcal{O}/I))$

$\mathcal{C} = \{ N \triangleleft \Gamma \mid N \supseteq \Gamma(I) \text{ for some } I \}$

The PSG Thm:

Assume Γ is res. finite & PSG

Analyze the finite quotients of Γ using CFSG (= classification of finite simple groups) ++

$\rightsquigarrow$ Γ is res.-p

i.e. $\Gamma \hookrightarrow \Gamma_{\hat{p}}$ = pro-p completion.

Thm (Lubotzky - Mann)

A pro-p gp G is PSG

$\Longleftrightarrow$ G is a p-adic Lie group.

Cor: $\rightsquigarrow$ Γ is linear over

$\Gamma \hookrightarrow GL_n(A)$ A f.g. ring

by alg. gps theory + + ...

$\rightsquigarrow$ $\Gamma \hookrightarrow GL_n(\mathbb{Q})$

infact $\Gamma \hookrightarrow GL_n(\mathbb{Z}[\frac{1}{p_1},\dots,\frac{1}{p_k}])$

say $\Gamma \hookrightarrow GL_n(\mathbb{Z})$.

Let G = Zariski closure of Γ

so $\Gamma \hookrightarrow G(\mathbb{Z}) = \Delta$

cos assume G conn., simply-conn. & simple.

<u>Strong Aproximation Thm</u>

Γ is dense in the congruence topology of Δ.

Denote:

$C_n(\Delta)$ = # congruence subgps of Δ of index $\leq n$.

Cor: $\quad s_n(\Gamma) \geq C_n(\Delta)$.

$\therefore$ So to get a contradiction it suffices to show that the number of congruence subgps of Δ grows ~~at~~ faster than polynomial.

Counting congruence subgroups (elementary).

$\Gamma = G(\mathbb{Z})$, e.g. $\Gamma = SL_d(\mathbb{Z})$

$\mathbb{R} \ni x$ large, $\mathcal{P}(x) = \{p \leq x\}$

$m = \prod_{p \leq x} p$, so $\log m = \sum \log p = \vartheta(x)$

$\ell = |\mathcal{P}|$

$$\Gamma/\Gamma(m) \simeq G(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_{p \in \mathcal{P}} G(\mathbb{F}_p)$$

Now, $2 \mid G(\mathbb{F}_p)$ so $(\mathbb{Z}/2\mathbb{Z})^\ell \leq G(\mathbb{Z}/m\mathbb{Z})$

$(\mathbb{Z}/2\mathbb{Z})^\ell$ has $\sim 2^{\ell^2/4}$ subspaces.

$\therefore$ Γ has $\geq 2^{\ell^2/4}$ subgroups of index $\leq m^{\dim(G)}$

Cor: Γ has at least

$n^{c \log n/(\log\log n)^2}$ cong.