Lecture 10:- Wednesday, Feb 8^{th}, 2012

"Affine Sieves and Expanders" by Alireza Salehi Golsefidy

Exp ① (Dirchilet theorem) $\exists\, \infty\ x$, $ax+b$ is a prime.
if $\gcd(a,b)=1$.

② (Twin prime Conjecture) $\exists\, \infty\ x$, $x(x+2)$ has at most 2 prime factors.

Chen: $\exists\, \infty\ x$, $x(x+2)$ has at most 3 prime factors.

③ (Mersenne primes ~~Conjecture~~) $\exists\, \infty\ x$, 2^x-1 is prime.

Remark:- We don't even know if $\exists\, r>0$ s.t.
$\{x \in \mathbb{N} \mid 2^x-1 \text{ has at most } r \text{ prime factors}\}$
is infinite.

- BGS

Hardy-Littlewood Conjecture

$\Lambda \subset \mathbb{Z}^n$, $\bar{b} \in \mathbb{Z}^n$.

$$\overline{\{\vec{\lambda} \mid (\lambda_1+b_1)(\lambda_2+b_2)\cdots(\lambda_n+b_n) \text{ has at most } n\text{-prime factors}\}}^{Zar} = \overline{\Lambda}^{Zar}$$

If $\underset{\text{square-free}}{\forall q}: \exists \lambda \in \Lambda$, $\gcd(f_{\vec{b}}(\vec{\lambda}), q) = 1$.

General setting. $\gamma_1, \ldots, \gamma_m \in SL_n(\mathbb{Q})$.

$$\Gamma = \langle \gamma_1, \ldots, \gamma_m \rangle \ . \ f \in \mathbb{Q}[X_{ij}]$$

$\exists\, r > 0$, S finite set of primes.

$$\Gamma_{r,S}(f) := \{ \gamma \in \Gamma : f(\gamma) \text{ has at most } r \ \mathbb{Z}_S\text{-prime factors} \}.$$

Under what condition $\overline{\Gamma_{r,S}(f)}^{zar} = \mathbb{G}$?

Example 1. $\gamma = \begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix}$

$f(X_{ij}) = X_{11} - 1 \rightsquigarrow$ Mersenne prime.

$f_1(X_{ij}) = (X_{11} - 1)(X_{11} - 2)$

$\liminf\limits_{n \to \infty} \underset{\substack{\downarrow \\ (\#\text{ of prime factors})}}{\omega}((2^n - 1)(2^{n-1} - 1)) = \infty$ (Heuristic suggestion)

- "Torus is the enemy"
- The Fundamental theorem of Affine Sieve (Salehi Golsefidy - Sarnak)

$$\left.\begin{array}{l} \text{① } \dim(V(f) \cap G) < \dim G \\ \text{② } X(G^\circ) = \{1\} \end{array}\right\} \Rightarrow \exists\, r, S : \overline{\Gamma_{r,S}(f)}^{zar} = \mathbb{G}.$$

Outline of the proof

$G = G^0$, $G = \underset{\text{semisimple}}{\mathbb{L}} \ltimes \mathbb{U} \leftarrow$ unipotent.

$$\underset{(\text{zariski-dense}) = \text{za-d}}{\Gamma} \subseteq G \Rightarrow \underset{(\text{zariski-dense})}{[\Gamma, \Gamma]} \subseteq [G, G]$$

$$\begin{tikzcd}
1 \arrow[r] & \overset{=\mathbb{H}}{D^{r_0}G} \arrow[r] & \overset{f}{G} \arrow[r, shift left, "\pi"] & \overset{=\mathbb{U}}{G/D^{r_0}G} \arrow[l, shift left, "s"] \arrow[r] & 1 \\
1 \arrow[r] & \Gamma \cap D^{r_0}G \arrow[r] \arrow[u, phantom, "\cup\ \text{za-d}"] & \Gamma \arrow[r, "\pi"] \arrow[u, phantom, "\cup\ \text{za-d}"] & \pi(\Gamma) \arrow[r] \arrow[u, phantom, "\cup\ \text{za-d}"] & 1
\end{tikzcd}$$

$D^{r_0}G$: the perfect core i.e. $[D^{r_0}G, D^{r_0}G] = D^{r_0}G$.

- $f = \sum_{i=1}^{m} p_i \otimes f_i$, $p_i \in \mathbb{Q}[\mathbb{U}]$ & $f_i \in \mathbb{Q}[\mathbb{H}]$.

$$f(g) = \sum p_i(\pi(g))\, f_i\big((s\,\pi(g))^{-1} g\big)$$

$$= p(\pi(g)) \sum_1 q_i(\pi(g))\, f_i\big((s\,\pi(g))^{-1} g\big).$$

- Theorem [Unipotent Case] $\Lambda \subseteq \mathbb{U}(\mathbb{Q})$, unipotent.

$$\left.\begin{array}{l} p, q_1, \dots, q_m \in \mathbb{Q}[\mathbb{U}] \\ \gcd(q_i) = 1 \end{array}\right\} \Rightarrow \exists\, r, s :$$

$\longrightarrow$

$$\mathcal{U} = \overline{\left\{ \lambda \in \Lambda : p(\lambda) \text{ has at most } r, \mathbb{Z}_S\text{-prime factors } \& \gcd(q_i(\lambda)) = 1 \right\}}^{\text{zar.}}$$

- Malcev theorem + careful induction + Brun's sieve.

<u>Theorem [Perfect Case]</u> : $\Gamma \subseteq \mathbb{G}$, $\mathbb{G} = \mathbb{G}^\circ = [\mathbb{G}, \mathbb{G}]$.

$$f_1, \ldots, f_n \in \mathbb{Q}[\mathbb{G}] \Rightarrow \exists\, r, S, \quad \overline{\Gamma_{r,S}\left(L_g\left(\sum v_i f_i\right)\right)}^{\text{zar}} = \mathbb{G}$$

where, $v_i \in \mathbb{Z}_S$.
$\gcd(v_i) = 1$ & $g \in \mathbb{G}(\mathbb{Z}_S)$.

<u>Theorem</u> : (Salehi Golsefidy - Varju)

$$\Omega = \Omega^{-1} \subseteq SL_n(\mathbb{Q}), \quad \Gamma = \langle \Omega \rangle$$

$\mathrm{cay}(\pi_q(\Gamma), \pi_q(\Omega))$ as 'q' runs through square free # form expanders, $\quad \overline{\Gamma}^{\text{zar}} = \mathbb{G}$

$$\Updownarrow$$

$$\mathbb{G}^\circ = [\mathbb{G}^\circ, \mathbb{G}^\circ].$$

• Helfgott, Bourgain - Gamburd, BGS, Varju, Breuillard - Green - Tao and PS.

(5)

(1) Escape from proper subgps.

$\exists\, \Omega' \subseteq \Gamma$, $\exists\, \delta > 0$, $\forall\, q$: square free no.

$H \lneq \pi_q(\Gamma) \Rightarrow \mu^{(\ell)}_{\Omega'}(Hg) \le [\pi_q(\Gamma) : H]^{-\delta}$.

$\ell \gg \log q$

(2) ℓ^2- flattening.

$\forall\, \varepsilon$, $\exists\, \delta$: $\mu \in \mathcal{P}(\pi_q(\Gamma))$,

(a) $\mu(gH) \le [\pi_q(\Gamma) : H]^{-\varepsilon}$.

(b) $\|\mu\|_2 > |\pi_q(\Gamma)|^{-\frac{1}{2}+\varepsilon}$

$\Rightarrow \|\mu * \mu\|_2 \le \|\mu\|_2^{1+\delta}$.

• $H_p \subsetneq \pi_p(\Gamma)$. $[H : H_p^+ F_p] < C$.

$H_p^+ = \mathbb{H}_p(\mathbb{F}_p)^+$, where $\mathbb{H}_p \subseteq \mathbb{G}_p$.

$\exists\, \delta$: $\mathcal{L}_\delta(\pi H_p) := \{\gamma \in \Gamma \mid \|\gamma\|_S \le [\pi_q(\Gamma) : H]^{\delta}\}$

$\Rightarrow \overline{\mathcal{L}_\delta(H)}^{zar} \subsetneq \mathbb{G}$.

—X—