Distribuzioni sugli interi profiniti

Ignazio Longhi
(collaborazione con L. Demangos e F.M.Saettone)

23 settembre 2022
6th Number Theory Meeting, Torino

Problema: dato $X \subset \mathbb{Z}^d$, come valutare quant'è grosso X?

Problema: dato $X \subset \mathbb{Z}^d$, come valutare quant'è grosso X?

Un approccio tradizionale: studiare

$$m_X(r) := |X \cap B(0,r)|$$

per $r \to \infty$. E.g.: per $X = \mathcal{P}$ (l'insieme dei primi)

$$m_{\mathcal{P}}(r) = \pi(r) \sim \frac{r}{\log r} \sim \int_2^r \frac{dt}{\log t}\ .$$

Problema: dato $X \subset \mathbb{Z}^d$, come valutare quant'è grosso X?

Un approccio tradizionale: studiare

$$m_X(r) := |X \cap B(0,r)|$$

per $r \to \infty$. E.g.: per $X = \mathcal{P}$ (l'insieme dei primi)

$$m_{\mathcal{P}}(r) = \pi(r) \sim \frac{r}{\log r} \sim \int_2^r \frac{dt}{\log t}\ .$$

Idea alla base di questo approccio: $\mathbb{Z} \hookrightarrow \mathbb{R}$.

"*die, anders lächelnd als die andern Schwestern,*" (Rilke)

Un altro approccio: usare

$$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}\,.$$

Un altro approccio: usare

$$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}\,.$$

Fatti:

- $\hat{\mathbb{Z}}$ è un anello topologico compatto;
- la topologia di $\hat{\mathbb{Z}}$ è strettamente legata alle proprietà algebriche di $\mathbb{Z}$;
- $\hat{\mathbb{Z}} = \prod_{p \in \mathcal{P}} \mathbb{Z}_p\,.$

Un altro approccio: usare

$$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z} \,.$$

Fatti:

- $\hat{\mathbb{Z}}$ è un anello topologico compatto;
- la topologia di $\hat{\mathbb{Z}}$ è strettamente legata alle proprietà algebriche di $\mathbb{Z}$;
- $\hat{\mathbb{Z}} = \prod_{p \in \mathcal{P}} \mathbb{Z}_p$.

Osservazione: lo stesso formalismo funziona, con modifiche banali, sostituendo $\mathbb{Z}$ con D anello degli S-interi in un campo globale (e.g., $D = \mathbb{Z}[i]$, $D = \mathbb{F}_q[t]$).

La nostra idea: dato $X \subset \mathbb{Z}^d$, studiare $\hat{X}$ (la sua chiusura in $\hat{\mathbb{Z}}^d$).

La nostra idea: dato $X \subset \mathbb{Z}^d$, studiare $\hat{X}$ (la sua chiusura in $\hat{\mathbb{Z}}^d$).

Si ha

$$\hat{X} = \bigcap_{n=1}^{\infty} \hat{\pi}_n^{-1}(\pi_n(X))$$

(con $\pi_n \colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ e $\hat{\pi}_n \colon \hat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ le mappe quoziente) e

$$\hat{X} \subseteq \prod_{p \in \mathcal{P}} X_p$$

dove X_p è la chiusura di X in $\mathbb{Z}_p$.

La nostra idea: dato $X \subset \mathbb{Z}^d$, studiare $\hat{X}$ (la sua chiusura in $\hat{\mathbb{Z}}^d$).

Si ha

$$\hat{X} = \bigcap_{n=1}^{\infty} \hat{\pi}_n^{-1}(\pi_n(X))$$

(con $\pi_n \colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ e $\hat{\pi}_n \colon \hat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ le mappe quoziente) e

$$\hat{X} \subseteq \prod_{p \in \mathcal{P}} X_p$$

dove X_p è la chiusura di X in $\mathbb{Z}_p$.

Caveat: se X e $\hat{X} \cap \mathbb{Z}^d$ sono "molto diversi", questo approccio non può funzionare (e.g.: $X = \bigcup_{n \in \mathbb{N}} \{n^n + 1, \ldots, n^n + n\}$).

- Se $\mathfrak{a}$ è un ideale, allora $\hat{\mathfrak{a}} = \mathfrak{a}\hat{\mathbb{Z}}$.

- Se $\mathfrak{a}$ è un ideale, allora $\hat{\mathfrak{a}} = \mathfrak{a}\hat{\mathbb{Z}}$.
- Se $X = \left\{(a, b) \in \mathbb{Z}^2 : gcd(a, b) = 1\right\}$, allora

$$\hat{X} = \prod X_p = \prod(\mathbb{Z}_p^2 - p\mathbb{Z}_p^2)$$

(dimostrazione: approssimazione forte per SL_2).

- Se $\mathfrak{a}$ è un ideale, allora $\hat{\mathfrak{a}} = \mathfrak{a}\hat{\mathbb{Z}}$.
- Se $X = \left\{(a, b) \in \mathbb{Z}^2 : gcd(a, b) = 1\right\}$, allora

$$\hat{X} = \prod X_p = \prod (\mathbb{Z}_p^2 - p\mathbb{Z}_p^2)$$

(dimostrazione: approssimazione forte per SL_2).

- L'insieme dei primi:

$$\hat{\mathcal{P}} = \mathcal{P} \sqcup \hat{\mathbb{Z}}^*$$

(equivale al teorema di Dirichlet sui primi in progressioni aritmetiche).

- Se $\mathfrak{a}$ è un ideale, allora $\hat{\mathfrak{a}} = \mathfrak{a}\hat{\mathbb{Z}}$.
- Se $X = \left\{(a, b) \in \mathbb{Z}^2 : gcd(a, b) = 1\right\}$, allora
$$\hat{X} = \prod X_p = \prod(\mathbb{Z}_p^2 - p\mathbb{Z}_p^2)$$
(dimostrazione: approssimazione forte per SL_2).
- L'insieme dei primi:
$$\hat{\mathcal{P}} = \mathcal{P} \sqcup \hat{\mathbb{Z}}^*$$
(equivale al teorema di Dirichlet sui primi in progressioni aritmetiche).
- Se $X = \mathbb{Z} - \bigcup_i \mathfrak{a}_i$, con $(\mathfrak{a}_i)_{i\in\mathbb{N}}$ una successione di ideali, allora
$$\hat{\mathbb{Z}}^*\hat{X} = \hat{\mathbb{Z}} - \bigcup_{i\in\mathbb{N}} \hat{\mathfrak{a}}_i \qquad (\text{spesso } \hat{\mathbb{Z}}^*\hat{X} = \hat{X}).$$

Si può rendere più quantitavo lo studio di $\hat{X}$?
(Analogo classico: studiare la funzione $m_X(r)$.)

Si può rendere più quantitavo lo studio di $\hat{X}$?
(Analogo classico: studiare la funzione $m_X(r)$.)

Idea: usare l'anello delle distribuzioni

$$\mathcal{D}(\hat{\mathbb{Z}}^d, \mathbb{C}) := \mathrm{Hom}(\mathcal{L}c(\hat{\mathbb{Z}}^d, \mathbb{C}), \mathbb{C})$$

dove $\mathcal{L}c(\hat{\mathbb{Z}}^d, \mathbb{C})$ è l'anello delle funzioni localmente costanti (a valori in $\mathbb{C}$).

Si ha

$$\mathcal{D}(\hat{\mathbb{Z}}, \mathbb{C}) = \prod \mathcal{D}(\mathbb{Z}_p, \mathbb{C}) = \varprojlim \mathcal{D}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C})$$

con $\mathcal{D}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}) \simeq \mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$.

A $X \subseteq \hat{\mathbb{Z}}^d$ associamo una successione di elementi $\mu_{X,n} \in \mathcal{D}(\hat{\mathbb{Z}}^d, \mathbb{C})$ tali che

$$(\hat{\pi}_n)_* \mu_{X,n} = \frac{1}{|\hat{\pi}_n(X)|} \sum_{x \in \pi_n(X)} \delta_x \in \mathcal{D}((\mathbb{Z}/n\mathbb{Z})^d, \mathbb{C})$$

e poniamo

$$\mu_X = \lim_n \mu_{X,n} \in \mathcal{D}(\hat{\mathbb{Z}}^d, \mathbb{C})$$

se il limite esiste.

A $X \subseteq \hat{\mathbb{Z}}^d$ associamo una successione di elementi $\mu_{X,n} \in \mathcal{D}(\hat{\mathbb{Z}}^d, \mathbb{C})$ tali che

$$(\hat{\pi}_n)_* \mu_{X,n} = \frac{1}{|\hat{\pi}_n(X)|} \sum_{x \in \pi_n(X)} \delta_x \in \mathcal{D}((\mathbb{Z}/n\mathbb{Z})^d, \mathbb{C})$$

e poniamo

$$\mu_X = \lim_n \mu_{X,n} \in \mathcal{D}(\hat{\mathbb{Z}}^d, \mathbb{C})$$

se il limite esiste.

Esempi:

- $\mu_{\hat{\mathbb{Z}}}$ è la misura di Haar su $\hat{\mathbb{Z}}$;
- $\mu_{\mathcal{P}} = \mu_{\hat{\mathbb{Z}}^*}$ (la misura di Haar su $\hat{\mathbb{Z}}^*$).

La densità $d(X)$ di X viene definita a partire da $\mathbb{Z} \hookrightarrow \mathbb{R}$ (spesso usando la funzione m_X).

Per ogni densità d "ragionevole" si ha $\mu_{\hat{\mathbb{Z}}}(\hat{X}) \geqslant d(X)$.

La densità $d(X)$ di X viene definita a partire da $\mathbb{Z} \hookrightarrow \mathbb{R}$ (spesso usando la funzione m_X).

Per ogni densità d "ragionevole" si ha $\mu_{\hat{\mathbb{Z}}}(\hat{X}) \geqslant d(X)$.

Teorema (Davenport-Erdős)

Sia $X = \mathbb{Z} - \bigcup \mathfrak{a}_i$, *con* $(\mathfrak{a}_i)_{i\in\mathbb{N}}$ *una successione di ideali. Allora*

$$\mu_{\hat{\mathbb{Z}}}(\hat{\mathbb{Z}}^* \hat{X}) = \mathrm{d}_{\mathrm{an}}(X)\,.$$

La densità $d(X)$ di X viene definita a partire da $\mathbb{Z} \hookrightarrow \mathbb{R}$ (spesso usando la funzione m_X).

Per ogni densità d "ragionevole" si ha $\mu_{\hat{\mathbb{Z}}}(\hat{X}) \geqslant d(X)$.

Teorema (Davenport-Erdős)

Sia $X = \mathbb{Z} - \bigcup \mathfrak{a}_i$, *con* $(\mathfrak{a}_i)_{i \in \mathbb{N}}$ *una successione di ideali. Allora*

$$\mu_{\hat{\mathbb{Z}}}(\hat{\mathbb{Z}}^* \hat{X}) = \mathrm{d}_{\mathrm{an}}(X) .$$

Teorema (Ekedahl)

Sia $Z \subset \mathbb{A}^d_{\mathbb{Z}}$ *un sottoschema chiuso e* $X = \bigcap_p \pi_p^{-1}(\mathbb{F}_p^n - Z(\mathbb{F}_p))$. *Allora*

$$\mu_{\hat{\mathbb{Z}}}(\hat{X}) = \mathrm{d}_{\mathrm{as}}(X) .$$

Supponiamo che $X \subseteq \mathbb{Z}$ soddisfi

$$\hat{X} = \prod_{p \in \mathcal{P}} X_p \tag{1}$$

dove ogni X_p è aperto in $\mathbb{Z}_p$. Allora la successione $\mu_{X,n}$ converge a $\mu_X \in \mathcal{D}(\mathbb{Z}, \mathbb{C})$.

Supponiamo che $X \subseteq \mathbb{Z}$ soddisfi

$$\hat{X} = \prod_{p \in \mathcal{P}} X_p \tag{1}$$

dove ogni X_p è aperto in $\mathbb{Z}_p$. Allora la successione $\mu_{X,n}$ converge a $\mu_X \in \mathcal{D}(\mathbb{Z}, \mathbb{C})$.

La convergenza è soddisfatta anche quando (1) è soltanto "quasi" vera. Esempi:

- $X = \mathcal{P}$;
- $X = \phi(\mathbb{Z}^k)$, dove $\phi \colon \mathbb{Z}^k \to \mathbb{Z}^d$ è una mappa polinomiale.

Siano $f_1, \ldots, f_d \in \mathbb{Z}[x]$ dei polinomi irriducibili, con coefficienti direttivi positivi, e $f = \prod_i f_i$.

Sia $\phi\colon \mathbb{Z} \to \mathbb{Z}^d$ la mappa $n \mapsto (f_1(n), \ldots, f_d(n))$.

Congettura (Ipotesi H di Schinzel)

Se $f(\hat{\mathbb{Z}}) \cap \hat{\mathbb{Z}}^* = \emptyset$ *allora* $|\phi(\mathbb{N}) \cap \mathcal{P}^d| = \infty$.

(Skorobogatov e Sofos hanno annunciato che l'ipotesi H è vera "con probabilità 1".)

Sia $\omega_f(p)$ il numero di zeri di f in $\mathbb{F}_p$ e

$$C_f = \prod_p \left(1 - \frac{1}{p}\right)^{-d} \left(1 - \frac{\omega_f(p)}{p}\right) .$$

Sia $\pi_\phi(r) := |\phi^{-1}(\mathcal{P}^d) \cap [0, r]|$.

Congettura (Bateman-Horn)

Se $f(\hat{\mathbb{Z}}) \cap \hat{\mathbb{Z}}^* = \emptyset$ allora

$$\pi_\phi(r) \sim \frac{C_f}{\prod_i \deg f_i} \int_2^r \frac{dt}{(\log t)^d} .$$

Sia $X = \phi(\mathbb{N}) \cap \mathcal{P}^d$. L'inclusione $\hat{X} \subseteq \phi(\hat{\mathbb{Z}}) \cap \hat{\mathcal{P}}^d$ è ovvia.

Sia $X = \phi(\mathbb{N}) \cap \mathcal{P}^d$. L'inclusione $\hat{X} \subseteq \phi(\hat{\mathbb{Z}}) \cap \hat{\mathcal{P}}^d$ è ovvia.

È sensato chiedersi se

$$\hat{X} \stackrel{??}{=} \phi(\hat{\mathbb{Z}}) \cap \hat{\mathcal{P}}^d = \phi(\hat{\mathbb{Z}}) \cap (\hat{\mathbb{Z}}^* \cup \mathcal{P})^d$$

possa essere vera?

Una risposta affermativa implicherebbe l'ipotesi H.

Sia $X = \phi(\mathbb{N}) \cap \mathcal{P}^d$. L'inclusione $\hat{X} \subseteq \phi(\hat{\mathbb{Z}}) \cap \hat{\mathcal{P}}^d$ è ovvia.

È sensato chiedersi se

$$\hat{X} \overset{??}{=} \phi(\hat{\mathbb{Z}}) \cap \hat{\mathcal{P}}^d = \phi(\hat{\mathbb{Z}}) \cap (\hat{\mathbb{Z}}^* \cup \mathcal{P})^d$$

possa essere vera?

Una risposta affermativa implicherebbe l'ipotesi H.

Speranza: la distribuzione associata a $\phi(\hat{\mathbb{Z}}) \cap (\hat{\mathbb{Z}}^* \cup \mathcal{P})^d$ potrebbe permettere di formulare una congettura quantitativa, confrontabile con Bateman-Horn.

Grazie per l'attenzione!