Points of algebraic varieties over finite rings.

A. Aizenbud

Weizmann Institute of Science

Joint with Nir Avni

http://www.wisdom.weizmann.ac.il/~aizenr/

Questions

Let X be a scheme of finite type over $\mathbb{Z}$.

Questions

Let X be a scheme of finite type over $\mathbb{Z}$.

Question

How many points does $X(\mathbb{Z})$ have?

Questions

Let X be a scheme of finite type over $\mathbb{Z}$.

Question

How many points does $X(\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/n\mathbb{Z})$ have?

Questions

Let X be a scheme of finite type over $\mathbb{Z}$.

Question

How many points does $X(\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/n\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/p^k\mathbb{Z})$ have?

Questions

Let X be a scheme of finite type over $\mathbb{Z}$.

Question

How many points does $X(\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/n\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/p^k\mathbb{Z})$ have?

Notation

Let R be a finite ring.

Questions

Let X be a scheme of finite type over $\mathbb{Z}$.

Question

How many points does $X(\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/n\mathbb{Z})$ have?

Question

How many points does $X(\mathbb{Z}/p^k\mathbb{Z})$ have?

Notation

Let R be a finite ring. Denote

$$h_X(R) := \frac{\#X(R)}{\#R^{\dim X_{\mathbb{Q}}}}.$$

Examples

Finite Rings

Examples

- $\mathbb{Z}/p^k\mathbb{Z}$

Finite Rings

Examples

- $\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{F}_p[t]/t^k$

Finite Rings

Examples

- $\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{F}_p[t]/t^k$
- $\mathbb{F}_q[t]/t^k$

Finite Rings

Examples

- $\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{F}_p[t]/t^k$
- $\mathbb{F}_q[t]/t^k$
- Let $\mathbb{Q}_{p^n}$ be the unique unramified extension of $\mathbb{Q}_p$ of order n. Let $\mathbb{Z}_{p^n}$ be its ring of integers and π be its uniformizer.

Finite Rings

Examples

- $\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{F}_p[t]/t^k$
- $\mathbb{F}_q[t]/t^k$
- Let $\mathbb{Q}_{p^n}$ be the unique unramified extension of $\mathbb{Q}_p$ of order n. Let $\mathbb{Z}_{p^n}$ be its ring of integers and π be its uniformizer. Consider $R := \mathbb{Z}_q/\pi^k$.

Zero vs. positive characteristic

Zero vs. positive characteristic

Notation

For a finite set of primes S denote by $\mathcal{P}_S$ the set of powers of primes outside S.

Zero vs. positive characteristic

Notation

For a finite set of primes S denote by $\mathcal{P}_S$ the set of powers of primes outside S. Denote also $\mathcal{P} := \mathcal{P}_\emptyset$.

Zero vs. positive characteristic

Notation

For a finite set of primes S denote by $\mathcal{P}_S$ the set of powers of primes outside S. Denote also $\mathcal{P} := \mathcal{P}_\emptyset$. Let $q \in \mathcal{P}$ and $k \in \mathbb{N}$. Denote:

Zero vs. positive characteristic

Notation

For a finite set of primes S denote by $\mathcal{P}_S$ the set of powers of primes outside S. Denote also $\mathcal{P} := \mathcal{P}_\emptyset$. Let $q \in \mathcal{P}$ and $k \in \mathbb{N}$. Denote:

- $h_X(q,k) = h_X(\mathbb{Z}_q/\pi^k)$

Zero vs. positive characteristic

Notation

For a finite set of primes S denote by $\mathcal{P}_S$ the set of powers of primes outside S. Denote also $\mathcal{P} := \mathcal{P}_\emptyset$. Let $q \in \mathcal{P}$ and $k \in \mathbb{N}$. Denote:

- $h_X(q,k) = h_X(\mathbb{Z}_q/\pi^k)$
- $h'_X(q,k) = h_X(\mathbb{F}_p[t]/t^k)$

Zero vs. positive characteristic

Notation

For a finite set of primes S denote by $\mathcal{P}_S$ the set of powers of primes outside S. Denote also $\mathcal{P} := \mathcal{P}_\emptyset$. Let $q \in \mathcal{P}$ and $k \in \mathbb{N}$. Denote:

- $h_X(q,k) = h_X(\mathbb{Z}_q/\pi^k)$
- $h'_X(q,k) = h_X(\mathbb{F}_p[t]/t^k)$

Theorem (Cluckers-Loeser $\sim$ 2005)

There exists a finite set S of primes s.t. for any $q \in \mathcal{P}_S$

$$h_X(q,k) = h'_X(q,k)$$

Main Results

Theorem (A.-Avni 2014)

Assume that $X_{\bar{\mathbb{Q}}}$ is irreducible local complete intersection.

Main Results

Theorem (A.-Avni 2014)

Assume that $X_{\bar{\mathbb{Q}}}$ is irreducible local complete intersection. TFAE:

Main Results

Theorem (A.-Avni 2014)

Assume that $X_{\bar{\mathbb{Q}}}$ is irreducible local complete intersection. TFAE:

1. *X has rational singularities.*

Main Results

Theorem (A.-Avni 2014)

Assume that $X_{\bar{\mathbb{Q}}}$ is irreducible local complete intersection. TFAE:

1. *X has rational singularities.*
2. *For any k: $\lim_{p\to\infty} h_X(p,k) = 1$.*

Main Results

Theorem (A.-Avni 2014)

Assume that $X_{\bar{\mathbb{Q}}}$ is irreducible local complete intersection. TFAE:

1. *X has rational singularities.*
2. *For any k: $\lim_{p\to\infty} h_X(p,k) = 1$.*
3. *There exists a finite set of primes S s.t. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$ for $q \in \mathcal{P}_S$ (uniformly on k).*

Main Results

Conjecture

Assume that $X_{\mathbb{Q}}$ is irreducible local complete intersection. TFAE:

1. *X has rational singularities.*
2. *For any k: $\lim_{p\to\infty} h_X(p,k) = 1$.*
3. *There exists a finite set of primes S s.t. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$ for $p \in \mathcal{P}_S$ (uniformly on k).*
4. *For almost any prime p: $h_X(p,k)$ is bounded.*

Main Results

Conjecture

Assume that $X_{\mathbb{Q}}$ is irreducible local complete intersection. TFAE:

1. *X has rational singularities.*
2. *For any k: $\lim_{p\to\infty} h_X(p,k) = 1$.*
3. *There exists a finite set of primes S s.t. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$ for $p \in \mathcal{P}_S$ (uniformly on k).*
4. *For almost any prime p: $h_X(p,k)$ is bounded.*
5. *For any $q \in \mathcal{P}$: $h_X(q,k)$ is bounded.*

Main Results

Conjecture

Assume that $X_{\mathbb{Q}}$ is irreducible local complete intersection. TFAE:

1. *X has rational singularities.*
2. *For any k: $\lim_{p\to\infty} h_X(p,k) = 1$.*
3. *There exists a finite set of primes S s.t. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$ for $p \in \mathcal{P}_S$ (uniformly on k).*
4. *For almost any prime p: $h_X(p,k)$ is bounded.*
5. *For any $q \in \mathcal{P}$: $h_X(q,k)$ is bounded.*
6. *There exists a finite set of primes S s.t. $h_X(q,k) - h_X(q,1) = O(\frac{1}{q})$ for $q \in \mathcal{P}_S$.*

Jet schemes and rational singularities

Jet schemes and rational singularities

Definition

For a scheme X defined over k, the jet scheme $jet_n(X)$ is the natural scheme defined over k s.t. $X(k[t]/t^n) \cong jet_n(X)(k)$.

Jet schemes and rational singularities

Definition

For a scheme X defined over k, the jet scheme $jet_n(X)$ is the natural scheme defined over k s.t. $X(k[t]/t^n) \cong jet_n(X)(k)$.

Theorem (Mustata 2001)

Assume that X is a local complete intersection irreducible variety. TFAE:

Jet schemes and rational singularities

Definition

For a scheme X defined over k, the jet scheme $jet_n(X)$ is the natural scheme defined over k s.t. $X(k[t]/t^n) \cong jet_n(X)(k)$.

Theorem (Mustata 2001)

Assume that X is a local complete intersection irreducible variety. TFAE:

- *X has rational singularities.*

Jet schemes and rational singularities

Definition

For a scheme X defined over k, the jet scheme $jet_n(X)$ is the natural scheme defined over k s.t. $X(k[t]/t^n) \cong jet_n(X)(k)$.

Theorem (Mustata 2001)

Assume that X is a local complete intersection irreducible variety. TFAE:

- *X has rational singularities.*
- *The jet schemes of X are irreducible.*

Lang Weil bounds and application of the Chebotarev theorem

Theorem (Lang-Weil)

Let X be an absolutely irreducible scheme.

$$\#X(\mathbb{F}_p) = p^{\dim X} + O(p^{\dim X - \frac{1}{2}}).$$

Lang Weil bounds and application of the Chebotarev theorem

Theorem (Lang-Weil)

Let X be an absolutely irreducible scheme.

$$\#X(\mathbb{F}_p) = p^{\dim X} + O(p^{\dim X - \frac{1}{2}}).$$

Theorem (Chebotarev)

Let X be a scheme. Then, for almost any p, the set of absolute irreducibility components of $X_{\mathbb{Q}}$ is bijective to the set of absolute irreducibility components of $X_{\mathbb{F}_p}$, and,

Lang Weil bounds and application of the Chebotarev theorem

Theorem (Lang-Weil)

Let X be an absolutely irreducible scheme.

$$\#X(\mathbb{F}_p) = p^{\dim X} + O(p^{\dim X - \frac{1}{2}}).$$

Theorem (Chebotarev)

Let X be a scheme. Then, for almost any p, the set of absolute irreducibility components of $X_{\mathbb{Q}}$ is bijective to the set of absolute irreducibility components of $X_{\mathbb{F}_p}$, and, for positive percentage of p, they are all defined over $\mathbb{F}_p$.

1. X has rational singularities.
2. $\lim_{p\to\infty} h'_X(p,k) = 1$.

1. X has rational singularities.
2. $\lim_{p\to\infty} h'_X(p,k) = 1$.

For a scheme Y, let $c_p(Y)$ be the number of absolute irreducibility components defined over $\mathbb{F}_p$.

1. X has rational singularities.
2. $\lim_{p\to\infty} h'_X(p,k) = 1$.

For a scheme Y, let $c_p(Y)$ be the number of absolute irreducibility components defined over $\mathbb{F}_p$.

$$h'_X(p,k) = h'_{Jet_k(X)}(p,1) = c_p(Jet_k(X)) + O(\frac{1}{\sqrt{p}}).$$

Rational singularities

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety.

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

1. $R\pi_*(O_{\tilde{X}}) = O_X$

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

1. $R\pi_*(O_{\tilde{X}}) = O_X$
2. $R\pi_*(\Omega_{\tilde{X}}) = \Omega_X$

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

1. $R\pi_*(O_{\tilde{X}}) = O_X$
2. $R\pi_*(\Omega_{\tilde{X}}) = \Omega_X$
3. X is Cohen-Macaulay and

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

1. $R\pi_*(O_{\tilde{X}}) = O_X$
2. $R\pi_*(\Omega_{\tilde{X}}) = \Omega_X$
3. X is Cohen-Macaulay and $\pi_*(\Omega_{\tilde{X}}) = \Omega_X$

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

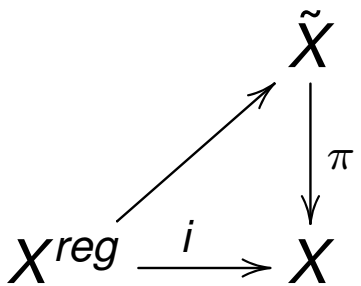
1. $R\pi_*(O_{\tilde{X}}) = O_X$
2. $R\pi_*(\Omega_{\tilde{X}}) = \Omega_X$
3. X is Cohen-Macaulay and $\pi_*(\Omega_{\tilde{X}}) = \Omega_X$
4. X is normal Cohen-Macaulay and

Rational singularities

Definition

Let $\tilde{X} \xrightarrow{\pi} X$ be a resolution of singularities of an F-algebraic variety. X is said to be of rational singularities if the following equivalent conditions hold:

1. $R\pi_*(O_{\tilde{X}}) = O_X$
2. $R\pi_*(\Omega_{\tilde{X}}) = \Omega_X$
3. X is Cohen-Macaulay and $\pi_*(\Omega_{\tilde{X}}) = \Omega_X$
4. X is normal Cohen-Macaulay and $\pi_*(\Omega_{\tilde{X}}) = i_*(\Omega_{X^{reg}})$



Pushforward of smooth measures

Pushforward of smooth measures

Theorem (A.-Avni, 2013)

Let:

$$X \overset{m}{\xrightarrow{\phi}} Y$$

s.t.

Pushforward of smooth measures

Theorem (A.-Avni, 2013)

Let:

$$X \overset{\phi}{\underset{m}{\to}} Y$$

s.t.

- ϕ *is a flat morphism of smooth algebraic varieties over a local field* F*, s.t. all its fibers are of rational singularities*

Pushforward of smooth measures

Theorem (A.-Avni, 2013)

Let:

$$X \overset{\phi}{\to} Y \quad (m)$$

s.t.

- ϕ *is a flat morphism of smooth algebraic varieties over a local field* F*, s.t. all its fibers are of rational singularities (in what follows: FRS morphism).*

Pushforward of smooth measures

Theorem (A.-Avni, 2013)

Let:

$$\overset{m}{X} \xrightarrow{\phi} Y$$

s.t.

- ϕ *is a flat morphism of smooth algebraic varieties over a local field* F*, s.t. all its fibers are of rational singularities (in what follows: FRS morphism).*
- m *is a Schwartz (i.e. compactly supported locally Haar) measure on* $X(F)$*.*

Pushforward of smooth measures

Theorem (A.-Avni, 2013)

Let:

$$\overset{m}{X} \xrightarrow{\phi} Y$$

s.t.

- ϕ *is a flat morphism of smooth algebraic varieties over a local field* F*, s.t. all its fibers are of rational singularities (in what follows: FRS morphism).*
- m *is a Schwartz (i.e. compactly supported locally Haar) measure on* $X(F)$*.*

Then $\phi_*(m)$ *has continuous density.*

1. X has rational singularities.
4. $\sup_k h_X(p,k) < \infty$.

1. X has rational singularities.
4. $\sup_k h_X(p,k) < \infty$.

WLOG we may assume that $X = \phi^{-1}(0)$ for a flat $\phi : \mathbb{A}^a \to \mathbb{A}^b$.

1. X has rational singularities.
4. $\sup_k h_X(p,k) < \infty$.

WLOG we may assume that $X = \phi^{-1}(0)$ for a flat $\phi : \mathbb{A}^a \to \mathbb{A}^b$. Let μ, ν be the Haar measures on $\mathbb{Z}_q^a$ and $\mathbb{Z}_q^b$.

$$h_X(q,k) = \frac{\mu(\phi^{-1}(\pi^k \mathbb{Z}_q^b))}{\nu(\pi^k \mathbb{Z}_q^b)}$$

1. X has rational singularities.
4. $\sup_k h_X(p,k) < \infty$.

WLOG we may assume that $X = \phi^{-1}(0)$ for a flat $\phi : \mathbb{A}^a \to \mathbb{A}^b$. Let μ, ν be the Haar measures on $\mathbb{Z}_q^a$ and $\mathbb{Z}_q^b$.

$$h_X(q,k) = \frac{\mu(\phi^{-1}(\pi^k \mathbb{Z}_q^b))}{\nu(\pi^k \mathbb{Z}_q^b)} = \frac{\phi_*(\mu)(\pi^k \mathbb{Z}_q^b)}{\nu(\pi^k \mathbb{Z}_q^b)}.$$

Theorem (Hrushovski-Kazhdan, et al.)

Let X be a definable set in an algebraic variety over a valued field, and ω be a definable top differential form on X depending on a parameter n in the valuation group. Let

$$f(q,n) := \int_{X(\mathbb{Q}_q)} |\omega|.$$

Then

$$f(q,n) = \sum f_i(q,n) \# X_i(\mathbb{F}_q),$$

where X_i are schemes and $f_i(q,n)$ are "simple-minded" non-negative functions.

2&4 $\Longrightarrow$ 3

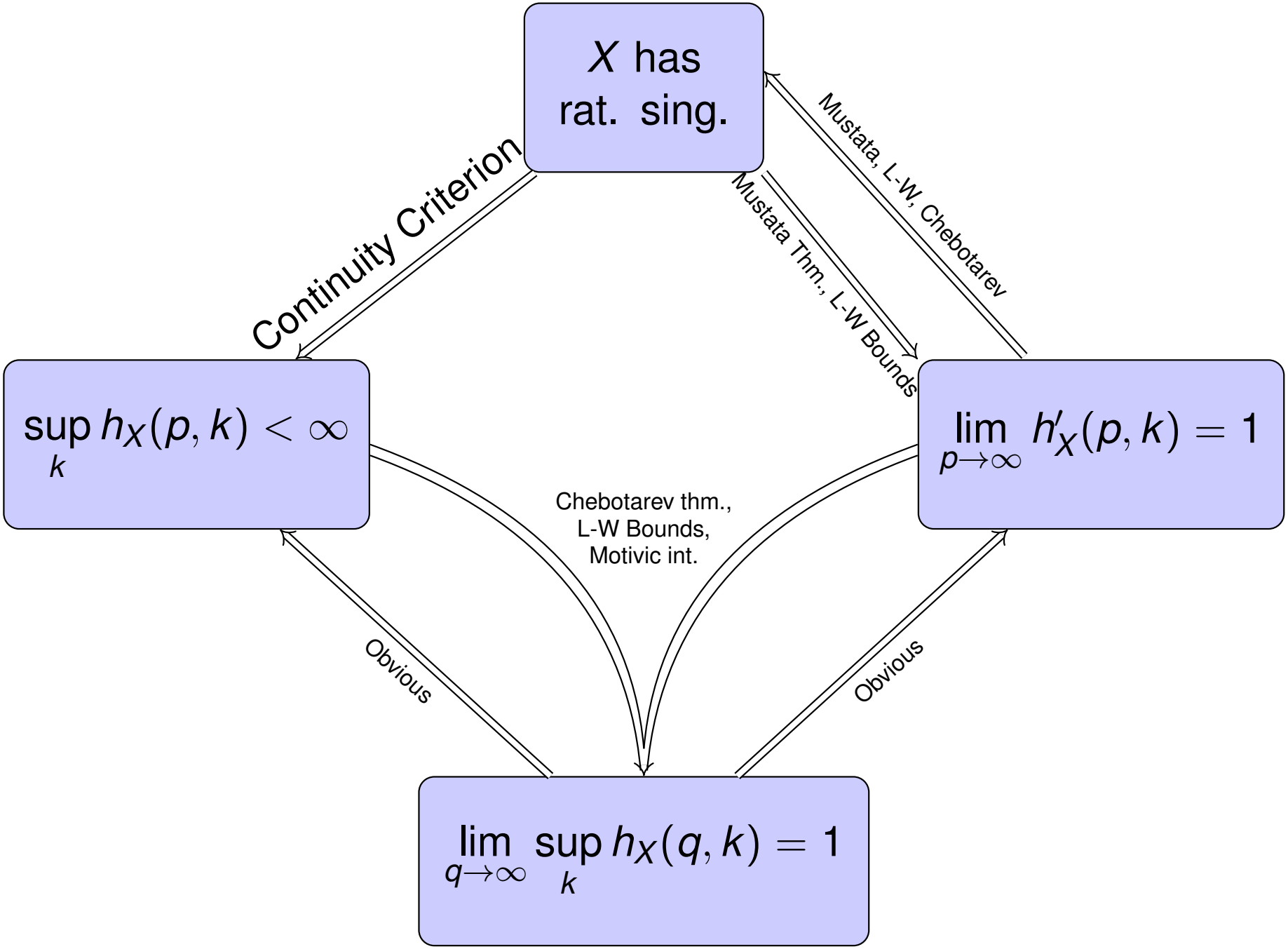
2. $\lim_{p\to\infty} h_X(p,k) = 1$.
4. $\sup_k h_X(p,k) < \infty$.
3. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$, (uniformly on k).

2. $\lim_{p\to\infty} h_X(p,k) = 1$.
4. $\sup_k h_X(p,k) < \infty$.
3. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$, (uniformly on k).

$$h_X(q,k) = \sum f_i(q,k)\#X_i(\mathbb{F}_q)$$

2. $\lim_{p\to\infty} h_X(p,k) = 1$.
4. $\sup_k h_X(p,k) < \infty$.
3. $h_X(q,k) - 1 = O(\frac{1}{\sqrt{q}})$, (uniformly on k).

$$h_X(q,k) = \sum f_i(q,k)\#X_i(\mathbb{F}_q) = 1 + O(\frac{1}{\sqrt{q}}).$$


X has rat. sing.
Continuity Criterion
Mustata, L-W, Chebotarev
Mustata Thm., L-W Bounds
$\sup_k h_X(p,k) < \infty$
$\lim_{p\to\infty} h'_X(p,k) = 1$
Chebotarev thm., L-W Bounds, Motivic int.
Obvious
Obvious
$\lim_{q\to\infty} \sup_k h_X(q,k) = 1$

Applications

Theorem (A.-Avni 2014)

Let $n > 500$ and G be a semisimple group defined over $\mathbb{Z}$. Then there exists a constant c s.t. for any integer k and $A \subset G(\mathbb{Z}/k\mathbb{Z})$:

$$\mathrm{Prob}([g_1, h_1] \cdots [g_n, h_n] \in A) < c \cdot \mathrm{Prob}(g \in A),$$

for random elements $g, g_1 \ldots g_n, h_1 \ldots h_n \in G(\mathbb{Z}/k\mathbb{Z})$

Applications

Theorem (A.-Avni 2014)

Let $n > 500$ and G be a semisimple group defined over $\mathbb{Z}$. Then there exists a constant c s.t. for any integer k and $A \subset G(\mathbb{Z}/k\mathbb{Z})$:

$$\mathrm{Prob}([g_1, h_1] \cdots [g_n, h_n] \in A) < c \cdot \mathrm{Prob}(g \in A),$$

for random elements $g, g_1 \ldots g_n, h_1 \ldots h_n \in G(\mathbb{Z}/k\mathbb{Z})$

Theorem (A.-Avni 2014)

Let G be a semisimple group defined over $\mathbb{Z}$ whose $\mathbb{Q}$-split rank is > 1.

Applications

Theorem (A.-Avni 2014)

Let $n > 500$ and G be a semisimple group defined over $\mathbb{Z}$. Then there exists a constant c s.t. for any integer k and $A \subset G(\mathbb{Z}/k\mathbb{Z})$:

$$\mathrm{Prob}([g_1, h_1] \cdots [g_n, h_n] \in A) < c \cdot \mathrm{Prob}(g \in A),$$

for random elements $g, g_1 \ldots g_n, h_1 \ldots h_n \in G(\mathbb{Z}/k\mathbb{Z})$

Theorem (A.-Avni 2014)

Let G be a semisimple group defined over $\mathbb{Z}$ whose $\mathbb{Q}$-split rank is > 1. Then

$$\#\{\pi \in \mathrm{irr}(G(\mathbb{Z})) | \dim \pi < n\} < Cn^{1000}.$$