The Green-Tao theorem for number fields

Masato MIMURA
(Tohoku U.)

j/w Wataru KAI (TU)
Akihiro MUNEMASA (TU)
Shin-ichiro SEKI (Aoyama)
Kiyoto YOSHINO (TU)

Topic:

·) number theory

·) extremal combinatorics

·) group action

1. Motivation

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$

(X, μ) : standard probability space

$T : X \circlearrowleft$ p.m.p. invertible

($\mathbb{Z}$-action)

Poincaré recurrence

$\forall E$ with $\mu(E) > 0$;
$\exists \, \ell \in \mathbb{N}$ s.t.
$\mu(T^{\ell}E \cap T^{2\ell}E) > 0$

FURSTENBERG's multi-recurrence

$\forall E$ with $\mu(E)>0$,

$\forall k \in \mathbb{N}$;

$\exists \ell \in \mathbb{N}$ s.t.

$$\mu(T^{\ell}E \cap T^{2\ell}E \cap \cdots \cap T^{k\ell}E) > 0$$

$[-N,N]$
$= [-N,N]_{\mathbb{R}} \cap \mathbb{Z}$

Outcome

||

SZEMERÉDI's theorem 1975

$A \subseteq \mathbb{Z}$

(upper) dense

$$\bar{d}(A) := \limsup_{N \to \infty} \frac{\#(A \cap [-N,N])}{\#[-N,N]} > 0$$

$\Rightarrow \forall k \in \mathbb{N};$

$\exists$ k-AP $\subseteq A$

AP = **A**rithmetic **P**rogression

a set of from

$$\ell\{1, \dots, k\} + \alpha$$

$$\left(\begin{matrix}\ell \in \mathbb{N} \\ \alpha \in \mathbb{Z}\end{matrix}\right)$$

$$\begin{matrix} \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & 2 & & k-1 & k \end{matrix}$$

$$\alpha+\ell \quad \alpha+2\ell \quad \alpha+3\ell \quad \cdots \quad \alpha+(k-1)\ell \quad \alpha+k\ell$$

$$\ell \qquad \ell \qquad \ell$$

Furstenberg –
KATZNELSON 1977

multi-recurrence for

$\mathbb{Z}^n \curvearrowright (X, \mu)$

$\Downarrow$

Multi-dim'l

Szemerédi's

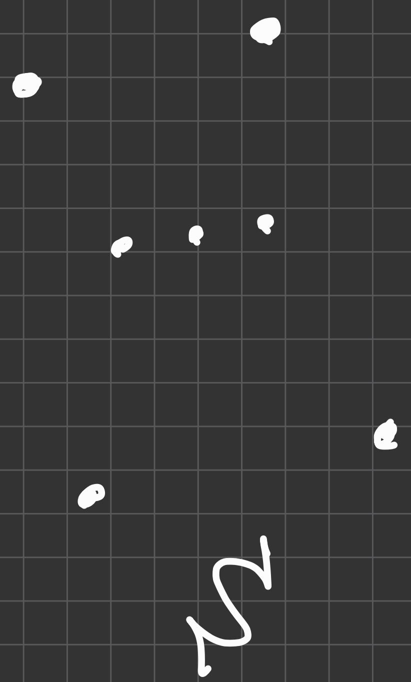
theorem

Def Z : free $\mathbb{Z}$-module of finite rank

$S \subseteq Z$ finite "shape"

$\mathcal{S}$: **S-constellation** is a set of the form

$$\ell S + \alpha \quad \begin{pmatrix} \ell \in \mathbb{N} \\ \alpha \in Z \end{pmatrix}$$



Multi dim'l Szemerédi [F-K, 1977]

$n \in \mathbb{N}$

$A \subseteq \mathbb{Z}^n$

dense

$$\bar{d}(A) := \limsup_{N \to \infty} \frac{\#(A \cap [-N, N]^n)}{\#[-N, N]^n} > 0$$

$$\Downarrow$$

$\forall S \subseteq \mathbb{Z}^n$ finite

$\exists\, \mathcal{S}$: S-constellation $\subseteq A$

2. GREEN-TAO thm

Q. **sparse** case??

$\leftarrow \bar{d}(A) = 0$

$\mathcal{P} := \{2, 3, 5, 7, 11, 13, \dots\}$

$(\subseteq \mathbb{Z})$

the set of (rational) primes

$$\left(\underline{\text{Prime Number Thm}} \qquad \#(\mathcal{P} \cap [-N, N]) \sim \frac{N}{\log N} \right)$$

Thm (Green-Tao '08)

$A \subseteq \mathcal{P} \ (\subseteq \mathbb{Z})$

rel dense

$$\bar{d}_{\mathcal{P}}(A) := \limsup_{N \to \infty} \frac{\#(A \cap [-N, N])}{\#(\mathcal{P} \cap [-N, N])} > 0$$

$$\Downarrow$$

$\forall k \in \mathbb{N},$

$\exists\, k\text{-AP} \subseteq A$

Thm (Bloom–Sisask '20)

$A \subseteq \mathbb{Z}$

with

$$\limsup_{N\to\infty} \frac{\#(A \cap [-N,N])}{\left(\frac{N}{\log N}\right)} > 0$$

$$\Downarrow$$

$\exists$ 3-AP

in A

Outlines of proof of GT thm

"subpseudorandomness"

+

"counting"

$\downarrow$ Combinatorics

(relative hypergraph removal lemma)

Constellation thm

Q. Multidim'l

case?

Main thm (Thm A)

&

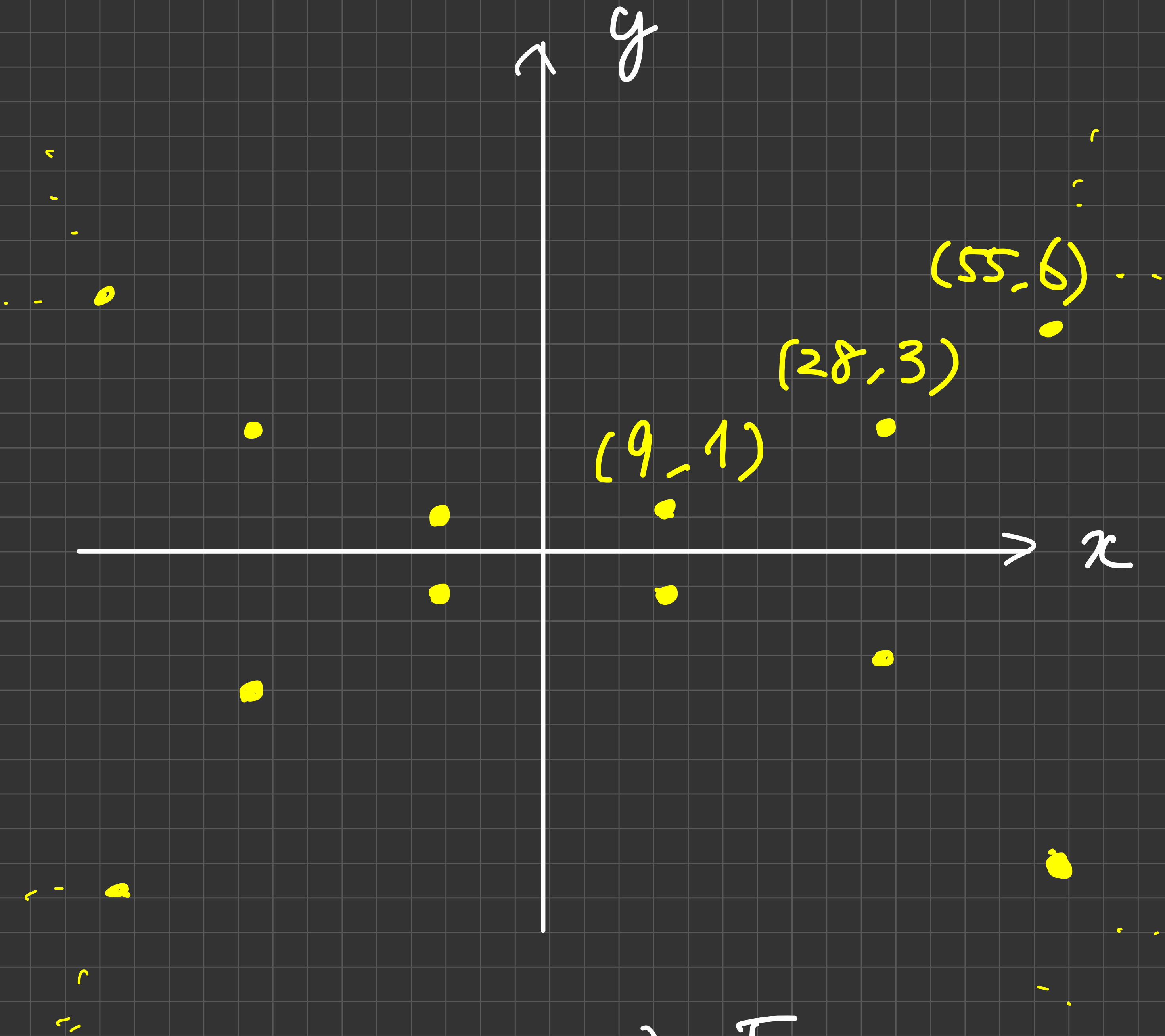
Cor (Thm C)

3. Main Cor

binary quadratic form ($\mathbb{Z}$-coeff.)

Today: Our form is

$$F : F(x, y) := x^2 - 79y^2$$



$\downarrow F$

$$9^2 - 79 \times 1^2 \qquad 28^2 - 73 \times 3^2 \qquad 55^2 - 79 \times 6^2$$

$\left(F(x,y) := x^2 - 79y^2 \right)$

Thm C ("KMMSY", '20)

$A \subseteq F^{-1}(\mathcal{P}) \subseteq \mathbb{Z}^2$ rel dense

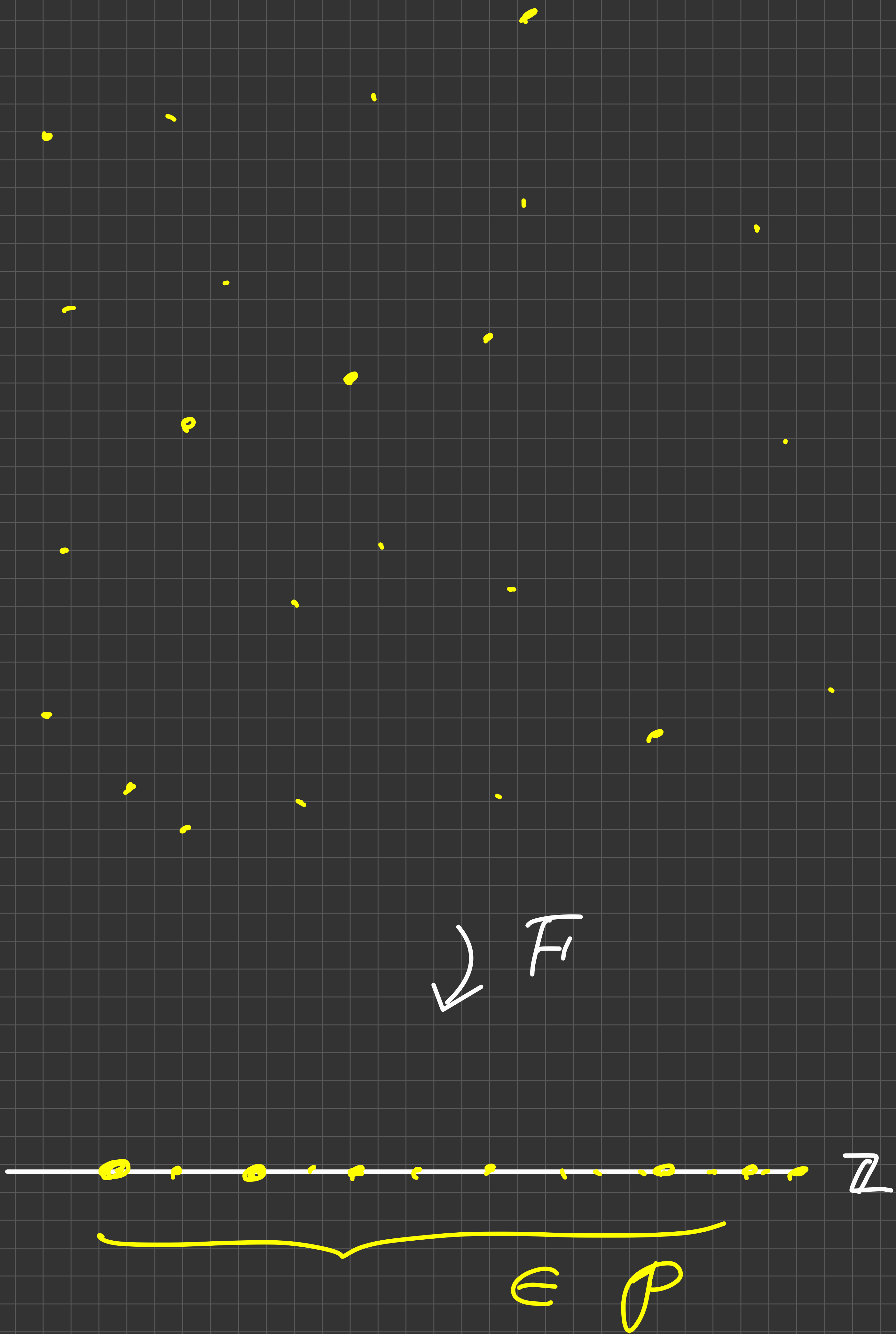
$\Downarrow$

$\forall S \subseteq \mathbb{Z}^2$ finite;

$\exists \mathcal{S}$: S-constellation

s.t. ·) $\mathcal{S} \subseteq A$

·) $F|_{\mathcal{S}}$ is inj



F_1
$\mathbb{Z}$
$\in \mathcal{P}$

TAO'06 : for $G(x,y)=x^2+y^2$

$$F\left(\begin{pmatrix}80 & 711\\ 9 & 80\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}\right) = F\left(\begin{pmatrix}x\\ y\end{pmatrix}\right)$$

$$\left((80x+711y)^2 - 79(9x+80y)^2 = x^2 - 79y^2\right)$$

$\rightsquigarrow \forall\, (x,y)\in\mathbb{Z}^2\setminus\{0\}$;

$\exists\ \infty$'ly many (x',y')

s.t. $F(x',y') = F(x,y)$

Thm C in fact

applies to

ALL

binary quadratic

forms

$$ax^2 + bxy + cy^2$$

$$(a, b, c \in \mathbb{Z})$$

with "3 obvious" caveats

① $\gcd(a, b, c) > 1$

"imprimitivity"

② $ax^2 + bxy + cy^2$

decomposes in $\mathbb{Z}[x, y]$

"degeneracy"

③ $ax^2 + bxy + cy^2$

negative definite

"negative definite"

4. Main Thm

Background of Thm C

$$F(x,y) = x^2 - 79y^2$$

$$= (x+\sqrt{79}y)(x-\sqrt{79}y)$$

$\wr$

Extend from $\mathbb{Q}$ & $\mathbb{Z}$

to $\mathbb{Q}(\sqrt{79})$ & $\mathbb{Z}[\sqrt{79}]$

Setting for $F(x,y) = x^2 - 79y^2$

$$K_F = \mathbb{Q}(\sqrt{79})$$

$$\mathcal{O}_{K_F} = \mathbb{Z}[\sqrt{79}]$$

the ring of integers

$$K_F \underset{\sigma_2}{\overset{\sigma_1}{\rightrightarrows}} \mathbb{C} \; ; \; s + \sqrt{79}t \begin{cases} \mapsto s + \sqrt{79}t \\ \mapsto s - \sqrt{79}t \end{cases}$$

$$N_{K_F/\mathbb{Q}} : \mathcal{O}_{K_F} \longrightarrow \mathbb{Z}$$

$$\begin{array}{ccc} \cup & & \cup \\ \alpha & \longmapsto & \sigma_1(\alpha)\sigma_2(\alpha) \\ \shortparallel & & \shortparallel \\ x + \sqrt{79}\,y & \longmapsto & x^2 - 79y^2 \end{array}$$

$x, y \in \mathbb{Z}$

ThmA ("KMNSY", '20)

K : ANY number field

$(n := [K : \mathbb{Q}])$

$\mathcal{O}_K$: the ring of integers $\left(\underset{\mathbb{Z}\text{-mod}}{\simeq} \mathbb{Z}^n \right)$

$\mathcal{P}_K := \{$ prime elements in $\mathcal{O}_K \}$

$$\left(= \left\{ \pi \in \mathcal{O}_K \;\middle|\; \begin{array}{l} \pi\mathcal{O}_K : \\ \text{non-zero} \\ \text{prime ideal} \end{array} \right\} \right)$$

$A \subseteq \mathcal{P}_K$ $(\subseteq \mathcal{O}_K \simeq \mathbb{Z}^n)$

rel dense

$$\Downarrow$$

$\forall\, S \subseteq \mathcal{O}_K$ finite

$\exists\, \delta : S$-constellation

s.t.

$\cdot)$ $\delta \subseteq A$

$\cdot)$ $|N_{K/\mathbb{Q}}|\,|_{\delta}$ is inj

Tao '06 $\quad Q(x,y) = x^2+y^2$

$$= (x+\sqrt{-1}\,y)(x-\sqrt{-1}\,y)$$

$$\rightsquigarrow \begin{cases} K_Q = \mathbb{Q}(\sqrt{-1}) \\ \mathcal{O}_{K_Q} = \mathbb{Z}[\sqrt{-1}] \end{cases}$$

Two Challenges

in

general cases:

(I) [class number]

$$h(K_G)\ (= h(\mathbb{Q}(\sqrt{-1})))$$
$$= 1$$

$$h(K_F)\ (= h(\mathbb{Q}(\sqrt{79})))$$
$$= 3 \neq 1$$

$$\rightsquigarrow$$

$$\{\text{ideals}\} \supsetneq \{\text{principal ideals}\}$$

(II) [action of the group of units]

(I) $\rightsquigarrow$ switch from **elements** to ideals

⚠ $$\alpha\mathcal{O}_K = \beta\mathcal{O}_K$$

$(\alpha, \beta \in \mathcal{O}_K \setminus \{0\})$

$\iff$ α, β are in the same orbit of the group action

$$\mathcal{O}_K^\times \curvearrowright \mathcal{O}_K \setminus \{0\}$$

·) $\mathcal{O}_{K_G}^\times = \{\pm 1, \pm \sqrt{-1}\}$

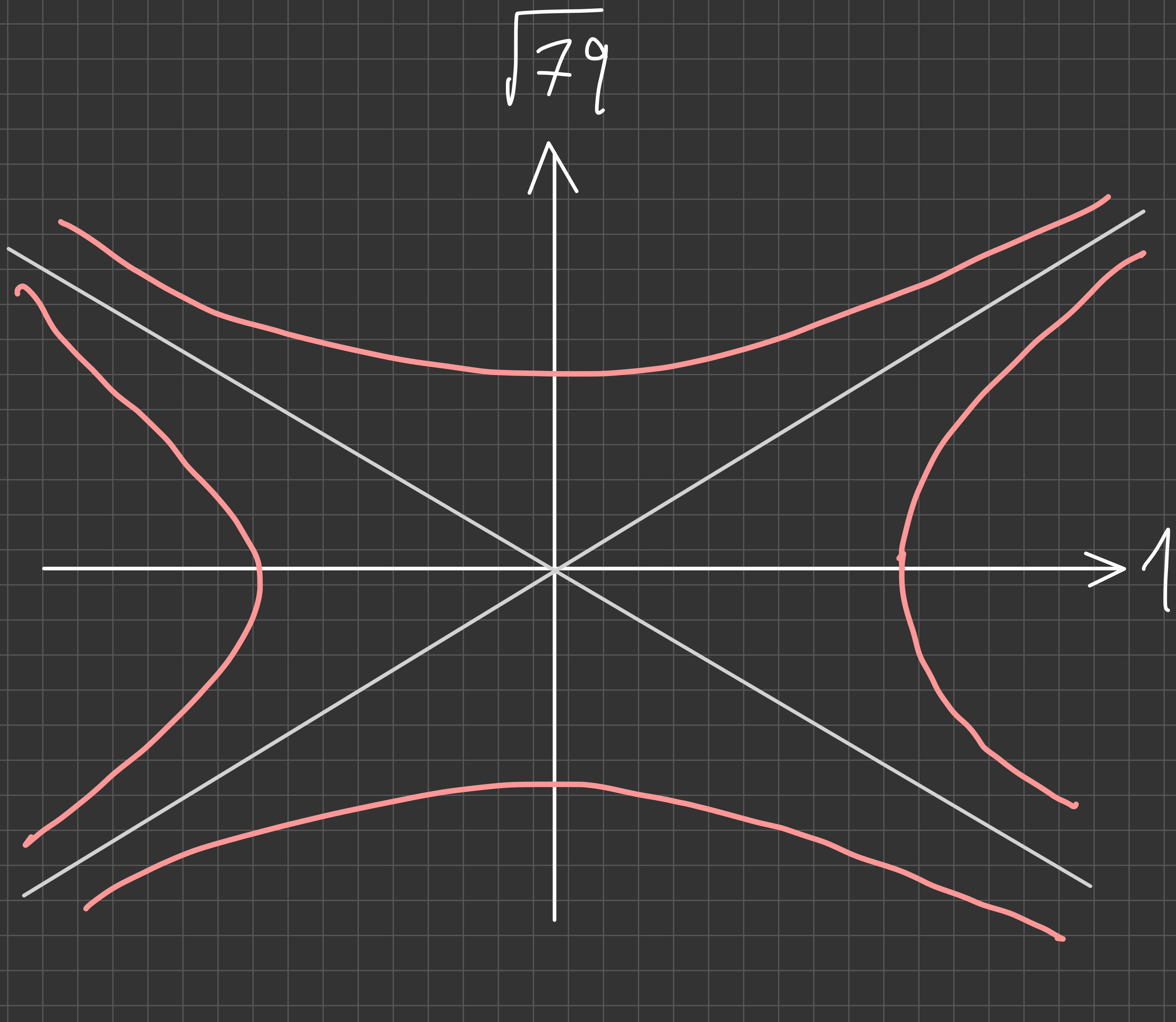
$K_G = \mathbb{Q}(\sqrt{-1})$ finite

but

·) $\mathcal{O}_{K_F}^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

$K_F = \mathbb{Q}(\sqrt{79})$ $\quad \mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$ $\quad \mathbb{Z} = \langle 80 + 9\sqrt{79} \rangle$

infinite



$$|N_{K/\mathbb{Q}}| = 1$$

<u>Note</u> $\alpha = x + \sqrt{79}\, y \in \mathcal{O}_{K_F}$

$(x, y \in \mathbb{Z})$

·) Norm $N_{K_F/\mathbb{Q}}(\alpha)$

$$:= x^2 - 79y^2$$

·) Length $\|\alpha\|_\infty$

$$:= \max\{|x|, |y|\}$$

always

$$|N_{K_F/\mathbb{Q}}(\alpha)| \leq 80\, \|\alpha\|_\infty^2$$

but no "$\geq$" in general...

BAKER-STARK-HEEGNER

There are exactly 10 K with

$$\begin{cases} h(K) = 1 \\ \# \mathcal{O}_K^\times < \infty \end{cases}$$

$\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$,

$\mathbb{Q}(\sqrt{-13})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$

5. Key in group action

Outline[7] :

modified von Mangoldt function

"Sub pseudorandom" for ideals

+

"counting"*

⇓ combinatorics

Constellation Thm

*:

CHEBOTAREV density thm:

$$\#\left\{ \pi \subset \mathcal{O}_K \;\middle|\; \begin{array}{l} \pi \in \mathcal{P}_K \\ |N_{K/\mathbb{Q}}(\pi)| \leq L \end{array} \right\} \sim \frac{1}{h(K)} \times \frac{L}{\log L}$$

Ideal counting

Want:

Switch from

ideal counting

measured by Norm $|N_{K/\mathbb{Q}}|$

to

element counting

measured by Length $\|\cdot\|_\infty$

Def for $K = K_{F_1} = \mathbb{Q}(\sqrt{79})$

$X \subseteq \mathcal{O}_{K_{F_1}} \setminus \{0\}$

is

NLC

(**N**orm **L**ength **C**ompatible)

$\overset{\text{def}}{\iff} \exists\, C > 0$ s.t.

$\forall\, \alpha \in X$;

$$\left| N_{K_{F_1}/\mathbb{Q}}(\alpha) \right| \geq C \, \|\alpha\|_\infty^2$$

Key Thm for element counting

$A \subseteq \mathcal{P}_K$ rel dense

$\Downarrow$

$\exists$ fundamental domain $\mathcal{D}$ for $\mathcal{O}_K^\times \curvearrowright \mathcal{O}_K \setminus \{0\}$

s.t.

- $\mathcal{D}$: NLC
- $A \cap \mathcal{D} \subseteq \mathcal{P}_K$ rel dense

("geometry of numbers")

arXiv:

2012.

15669

Thank You!!