# Counting rational points via additive combinatorics

Lilian Matthiesen

Institut de Mathématiques de Jussieu

joint with T. Browning

# Basic question

$K/\mathbb{Q}$ finite, $[K:\mathbb{Q}] = n$, $\qquad P \in \mathbb{Q}[X]$ polynomial

## Question:

*What can be said about* $t \in \mathbb{Q}$ *s.t.*

$$\exists k \in K: \qquad P(t) = \mathrm{N}_{K/\mathbb{Q}}(k) \neq 0 \quad ?$$

## Equivalent problem over $\mathbb{Q}$ :

If $\{\omega_1, \ldots, \omega_n\}$ a $\mathbb{Z}$-basis for $\mathfrak{o}_K$,

$$P(t) = \mathrm{N}_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_n\omega_n) = \mathbf{N}_K(\mathbf{x}) \neq 0$$

defines variety in $X \subset \mathbb{A}^{n+1}_{\mathbb{Q}}$. Interested in $X(\mathbb{Q})$.

# Rational points

1. Hasse principle: Let $X(\mathbb{A}) := X(\mathbb{R}) \times \prod_p X(\mathbb{Q}_p)$.

$$X(\mathbb{A}) \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$$

2. Weak approximation:

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{A}) \quad \text{via} \quad \mathbf{P} \mapsto \{\mathbf{P}_v\}_{v \in \Omega}$$

$X(\mathbb{Q})$ is dense in $X(\mathbb{A})$ with product topology.

Given finite $\Sigma \subset \Omega$, and $\mathbf{a}_v \in X(\mathbb{Q}_v)$ for each $v \in \Sigma$. Then
$\forall \varepsilon > 0 \quad \exists \mathbf{a} \in X(\mathbb{Q})$ s.t.

$$|\mathbf{a} - \mathbf{a}_v|_v < \varepsilon \quad \forall v \in \Sigma.$$

# Rational points

Neither needs to hold. However:

Conjecture (Colliot-Thélène)

*Brauer–Manin obstruction is the only obstruction to HP and WA for smooth and projective models $X^c$ of the variety $X$ defined by*

$$P(t) = \mathbf{N}_K(\mathbf{x}) \ .$$

Restrict to split polynomials $P \in \mathbb{Q}[X]$, that is

$$P(t) = c\prod_{j=1}^{r}(t-e_j)^{m_j} \qquad c \in \mathbb{Q}^*, e_1, \ldots, e_r \in \mathbb{Q} \text{ pairwise distinct.}$$

## Some known cases

- *under Schinzel*: $P$ arbitrary, $K/k$ cyclic
  *Colliot-Thélène, Skorobogatov, Swinnerton-Dyer 1998*
- $r = 2$ distinct roots, $K/k$ arbitrary (+extra condition)
  *Heath-Brown, Skorobogatov 2002*
- $r = 2$ distinct roots, $K/k$ arbitrary
  *Colliot-Thélène, Harari, Skorobogatov 2003*
- $r$ arbitratry, $K/\mathbb{Q}$ quadratic
  *Browning, M, Skorobogatov 2012*
- $r$ arbitratry, $K/\mathbb{Q}$ cyclic
  *Harpaz, Skorobogatov, Wittenberg 2013*

## Theorem (Browning, M., 2013)

*The conjecture holds for* $P(t) = c\prod_{j=1}^{r}(t-e_j)^{m_j}$ *and finite* $K/\mathbb{Q}$.

# Reduction via descent

Theory of descent (Colliot-Thélène, Sansuc) implies, as shown in [Schindler–Skorobogatov 2012]:

It suffices to prove HP/WA for all $V \subset \mathbb{A}^{rn+1}$ given by

$$0 \neq t - e_1 = \lambda_1 \, \mathbf{N}_K(\mathbf{x}_1)$$

$$\vdots$$

$$0 \neq t - e_r = \lambda_r \, \mathbf{N}_K(\mathbf{x}_r)$$

where $\mathbf{x}_i = (x_{i,1}, \ldots, x_{i,n})$ and $\lambda_i \in \mathbb{Q}^*$.

Equivalently (homogenisation): HP/WA holds for $V' \subset \mathbb{A}^{(r+1)n+2}$ given by

$$v = \mathbf{N}_K(\mathbf{y}) \neq 0$$
$$(u - e_i v)/\lambda_i = \mathbf{N}_K(\mathbf{x}_i) \neq 0 \quad (1 \leqslant i \leqslant r).$$

# Strategy

More generally: $V \subset \mathbb{A}^{r+ns}$ given by

$$f_i(u_1, \ldots, u_s) = \mathbf{N}_K(\mathbf{x}_i) \neq 0 \quad (1 \leqslant i \leqslant r)$$

where $f_i : \mathbb{Z}^s \to \mathbb{Z}$ linear forms, non-constant, pairwise non-proportional.

## Representation function

$$R(m) = 1_{m \neq 0} \cdot \#\{\mathbf{x} \in \mathbb{Z}^n / U_K^{(+)} : m = \mathbf{N}_K(\mathbf{x})\}$$

where $U_K^{(+)} = \{\eta \in U_K : N_{K/\mathbb{Q}}\eta = +1\}$.

If $N_{K/\mathbb{Q}}(\mathbf{x}.\omega) = N_{K/\mathbb{Q}}(\mathbf{y}.\omega) \neq 0$ and $\mathbf{x}.\omega = \eta\mathbf{y}.\omega$, then $N_{K/\mathbb{Q}}\eta = +1$. Counting problem:

$$\sum_{\mathbf{u} \in \mathbb{Z}^s \cap T\mathcal{K}} \prod_{i=1}^{r} R(f_i(\mathbf{u})) = T^s \beta_\infty \prod_p \beta_p + o(T^s)$$

where $\mathcal{K} \subset [-1, 1]^s$ convex.

# Strategy

Green–Tao methods (+Green–Tao–Ziegler inverse theorem) give such an asymptotic provided:

1. there are pseudo-random majorants $\nu^{(T)} : \{1, \dots, T\} \to \mathbb{R}_{>0}$ for sufficiently large $T$ s.t.

$$R(m) \leqslant C\nu^{(T)}(m), \qquad \text{for } 1 \leqslant m \leqslant T,$$

2. $R - (\frac{1}{T} \sum_{m \leqslant T} R(T))$ is orthogonal to nilsequences.

# Pseudo-random majorant

$(\nu^{(T)} : \{1, \ldots, T\} \to \mathbb{R}_{>0})_{T \in \mathcal{T}}$ is a family of $D$-pseudorandom majorants if:

## The total mass is roughly 1:

$$\frac{1}{T} \sum_{m \leqslant T} \nu^{(T)}(m) = 1 + o(1)$$

## The $D$-linear forms condition

For all

- integers $0 < t, d \leqslant D$,
- linear polynomials $h_1, \ldots, h_t : \mathbb{Z}^d \to \mathbb{Z}$ (coefficients bounded by $D$, pairwise non-proportional linear parts),
- convex $\mathcal{K}' \subset \mathbb{R}^d$ with $h_i(\mathcal{K}') \subseteq [1, T]$ for $1 \leqslant i \leqslant t$.

we have

$$\frac{1}{|\mathbb{Z}^d \cap \mathcal{K}'|} \sum_{\mathbf{u} \in \mathbb{Z}^d \cap \mathcal{K}'} \nu^{(T)}(h_1(\mathbf{u})) \ldots \nu^{(T)}(h_t(\mathbf{u})) = 1 + o(1).$$

# What are we looking for?

For multiplicative arith. functions one can hope for

$$\nu^{(T)}(m) = \sum_{d \leqslant T^{\gamma}} 1_{d|m} \lambda_d,$$

where $\gamma \in (0, 1/2)$ can be chosen as small as necessary.

Lemma

$$R(m) \ll r_K(|m|),$$

*where*

$$\zeta_K(s) = \sum_{(0) \neq \mathfrak{a} \subset \mathfrak{o}_K} (N\mathfrak{a})^{-s} = \sum_{m \geqslant 1} \frac{r_K(m)}{m^s}$$

*and*

$$\sum_{0 < \epsilon m \leqslant T} R(m) \sim \kappa_\epsilon T, \qquad \sum_{0 < m \leqslant T} r_K(m) \sim \kappa T.$$

# Proof of Lemma

$$\begin{aligned} R(m) &= \#\{\mathbf{x} \in \mathbb{Z}^n / U_K^{(+)} : m = \mathbf{N}_K(\mathbf{x})\} \\ &\leqslant 2\#\{\mathbf{x} \in \mathbb{Z}^n / U_K : m = \mathbf{N}_K(\mathbf{x})\} \\ &\leqslant 2\#\{\mathbf{x} \in \mathbb{Z}^n / U_K : |m| = |\mathbf{N}_K(\mathbf{x})|\} \\ &\leqslant 2\#\{(\alpha) \subset \mathfrak{o}_K : \mathrm{N}(\alpha) = |m|\} \\ &\leqslant 2\#\{\mathfrak{a} \subset \mathfrak{o}_K : \mathrm{N}\,\mathfrak{a} = |m|\} = 2r_K(|m|) \end{aligned}$$

$$U_K^{(+)} = \ker(N_{K/\mathbb{Q}} : U_K \to \{\pm 1\})$$

Aim: Construct a majorant for $r_K$ that takes the form

$$\nu^{(T)}(m) = \sum_{d \leqslant T^\gamma} 1_{d|m} \lambda_d.$$

# Multiplicative structure of $r_K$

If $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$, $\mathrm{N}\,\mathfrak{p}_i = p^{f_i}$, then

$$r_K(p^m) = \#\{\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_k^{m_k} : \sum_{i=1}^{k} f_i m_i = m\}$$
$$< (m+1)^n = \tau(p^m)^n.$$

At primes:

$$r_K(p) = \#\{\mathfrak{p} | (p) : f_{\mathfrak{p}} = 1\}.$$

Define

$$\mathcal{P}_0 = \{p \mid D_K\},$$
$$\mathcal{P}_1 = \{p \nmid D_K : \exists\, \mathfrak{p} \mid (p) \text{ such that } f_{\mathfrak{p}}(p) = 1\},$$
$$\mathcal{P}_2 = \{p \nmid D_K : f_{\mathfrak{p}}(p) \geqslant 2 \text{ for all } \mathfrak{p} \mid (p)\}.$$

Note: $\mu^2(m) = 1$ and $r_K(m) > 0$ implies

$$m \in \langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle = \{m : p | m \implies p \in \mathcal{P}_0 \cup \mathcal{P}_1\}$$

# Separate into two cases

Chebotarev: $\mathcal{P}_0 \cup \mathcal{P}_1$ has Dirichlet density $\frac{1}{n} \leqslant \delta \leqslant 1$, that is

$$|\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle \cap [1, T]| \asymp T \log^{\delta-1} T.$$

$\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle$ is a sparse set $\quad \rightsquigarrow \quad$ little control on $\mu * r_K$.

Define $$r_{\mathrm{res}}(p^m) = \begin{cases} r_K(p^m), & \text{if } p \in \mathcal{P}_0 \cup \mathcal{P}_1, \\ 1, & \text{if } p \in \mathcal{P}_2. \end{cases}$$

Then

$$r_K(m) \leqslant \sum_{\substack{q \in \langle \mathcal{P}_2 \rangle \\ v_p(q) \neq 1 \ \forall p}} \mathbf{1}_{q|m} \tau(q)^n \, \mathbf{1}_{\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle}\left(\frac{m}{q}\right) r_{\mathrm{res}}\left(\frac{m}{q}\right).$$

Suffices to find majorants for $\mathbf{1}_{\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle}$ and $r_{\mathrm{res}}$ separately.

# Characteristic function

For $\mathbf{1}_{\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle}$ can use sieve majorant (Goldston–Pintz–Yıldırım, Green–Tao)

$$\mathbf{1}_{\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle}(m) \leqslant \nu^{(T)}(m) = \left( \sum_{d \in \langle \mathcal{P}_2 \rangle} 1_{d|m} \mu(d) \chi\left( \frac{\log d}{\log T^{\gamma}} \right) \right)^2.$$

# Majorants for positive multiplicative functions

Suppose $f : \mathbb{N} \to \mathbb{R}_{>0}$ is multiplicative and satisfies

(a) $f(p^k) \leqslant H^k$ for all prime powers,

(b) $f(m) \ll_\delta m^\delta$ as $m \to \infty$ for any $\delta > 0$, and

(c) $f(p^{k-1}) \leqslant f(p^k)$ for all prime powers.

(Thus $g = \mu * f$ is non-negative.)

Define $f_\gamma^{(T)} : \{1, \dots, T\} \to \mathbb{R}_{\geqslant 0}$ via

$$f_\gamma^{(T)}(m) = \sum_{d \leqslant T^\gamma} \mathbf{1}_{d|m}\, g(d).$$

Would like $f(m) \ll f_\gamma^{(T)}(m)$ for $m \leqslant T$.

Consider *bad* sets $S(\kappa) = \{m \leqslant T : f(m) > H^\kappa f_\gamma^{(T)}(m)\}$.

Note that

$$\forall m \exists \kappa : m \in S(\kappa) \backslash S(\kappa+1) \quad \text{thus} \quad f(m) \leqslant \sum_{\kappa \geqslant 0} H^{\kappa+1} 1_{S(\kappa)}(m) f_\gamma^{(T)}(m).$$

## Lemma (Based on ideas from paper of Erdős)

*If* $f : \mathbb{N} \to \mathbb{R}_{>0}$ *as before,* $C_1 > 1$,
$H > 1$ *and* $m \leqslant T \quad s.t. \quad f(m) \geqslant H^{\kappa} f_{\gamma}^{(T)}(m) \quad$ *for some* $\kappa > 2/\gamma$.
*Then at least one of three alternatives holds:*

(i) $p^a | m$ *for some* $p^a$, $a \geqslant 2$, *with* $p^a > \log^{C_1} T$;

(ii) $m$ *is "smooth":*

$$\prod_{p \leqslant T^{1/(\log\log T)^3}} p^{v_p(m)} \geqslant T^{\gamma/\log\log T};$$

(iii) $m$ *has a "cluster" of prime factors: there is*

$$\log_2 \kappa - 2 \leqslant \lambda \ll \log\log\log T \qquad s.t.$$

$$\#\left\{p|m : T^{1/2^{\lambda+1}} \leqslant p \leqslant T^{1/2^{\lambda}}\right\} \quad \geqslant \gamma\kappa(\lambda + 3 - \log_2 \kappa)/100$$

*(The product* $u$ *of these primes satisfies* $u \leqslant T^{\gamma}$.*)*

# Truncated divisor sum majorant for $\mathbf{1}_{S(\kappa)}$

If

$$U(\kappa,\lambda) = \left\{ \prod_{j=1}^{\omega(\kappa,\lambda)} p_j : T^{1/2^{\lambda+1}} \leqslant p \leqslant T^{1/2^{\lambda}} \right\}$$

then

$$\mathbf{1}_{S(\kappa)}(m) \leqslant \sum_{\lambda} \sum_{u \in U(\kappa,\lambda)} 1_{u|m} + \text{error } (\mathbf{1}_{(i) \text{ or } (ii)}(m)).$$

Recall:

$$f(m) \leqslant \sum_{\kappa} 1_{S(\kappa)}(m) H^{\kappa+1} f_{\gamma}^{(T)}(m)$$

Replace $1_{S(\kappa)}(m)$ by above bound to obtain $\nu^{(T)}(m)$.

Then

$$\sum_{m \leqslant T} \nu^{(T)}(m) \ll \sum_{m \leqslant T} f(m)$$

# Complete majorant

$$\nu^{(T)}(m) = \Big( \sum_{d \in \langle \mathcal{P}_2 \rangle} 1_{d|m} \mu(d) \chi\Big(\frac{\log d}{\log T^{\gamma}}\Big)\Big)^2 \times \Big( \sum_{\kappa} \sum_{\lambda} \sum_{u \in U(\kappa,\lambda)} 2^{n\kappa} 1_{u|m} \sum_{d \in \langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle} g(d) \chi\Big(\frac{\log d}{\log T^{\gamma}}\Big)\Big)$$

# Summary

These ideas lead to a proof of the first of the requirements for an application of Green–Tao

1. there are pseudo-random majorants $\nu^{(T)} : \{1, \dots T\} \to \mathbb{R}_{>0}$ for sufficiently large $T$ s.t.

$$R(m) \leqslant C\nu^{(T)}(m), \qquad \text{for } 1 \leqslant m \leqslant T,$$

2. $R - (\frac{1}{T}\sum_{m \leqslant T} R(T))$ is orthogonal to nilsequences.

Both parts together lead to a proof of HP/WA for the variety

$$f_i(\mathbf{u}) = \mathbf{N}_K(\mathbf{x}_i), 1 \leqslant i \leqslant r.$$