Counting rational points via additive combinatorics

Lilian Matthiesen

Institut de Mathématiques de Jussieu

joint with T. Browning
Basic question

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

**Question:**

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

\[
\exists k \in K : \quad P(t) = N_{K/\mathbb{Q}}(k) \neq 0 \quad ?
\]

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

If \{\omega_1, \ldots, \omega_n\} a $\mathbb{Z}$-basis for $\mathfrak{o}_K$, \[P(t) = N_{K/\mathbb{Q}}(x_1 \omega_1 + \cdots + x_n \omega_n) = N_K(x) \neq 0 \]

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:**

\[
X(\mathbb{Q}) \hookrightarrow X(\mathbb{A}) \quad \text{via} \quad P \mapsto \{P_v\}_{v \in \Omega}
\]

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

Given finite \( \Sigma \subset \Omega \), and \( a_v \in X(\mathbb{Q}_v) \) for each \( v \in \Sigma \). Then

\[
\forall \varepsilon > 0 \quad \exists a \in X(\mathbb{Q}) \text{ s.t.} \quad |a - a_v|_v < \varepsilon \quad \forall v \in \Sigma.
\]
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

$$P(t) = N_K(x).$$
Restrict to split polynomials $P \in \mathbb{Q}[X]$, that is

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

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

- $r$ arbitrary, $K/\mathbb{Q}$ quadratic
  
  Browning, M, Skorobogatov 2012

- $r$ arbitrary, $K/\mathbb{Q}$ 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 $V \subset \mathbb{A}^{r+1}$ given by

$$0 \neq t - e_1 = \lambda_1 \mathbf{N}_K(x_1)$$

$$\vdots$$

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

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

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

$$v = \mathbf{N}_K(y) \neq 0$$

$$(u - e_i v)/\lambda_i = \mathbf{N}_K(x_i) \neq 0 \quad (1 \leq i \leq r).$$
More generally: \( V \subset \mathbb{A}^{r+ns} \) given by
\[
f_i(u_1, \ldots, u_s) = N_K(x_i) \neq 0 \quad (1 \leq i \leq r)
\]
where \( f_i : \mathbb{Z}^s \to \mathbb{Z} \) linear forms, non-constant, pairwise non-proportional.

Representation function

\[
R(m) = 1_{m \neq 0} \cdot \#\{x \in \mathbb{Z}^n / U_K^{(+)} : m = N_K(x)\}
\]

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

If \( N_{K/Q}(x.\omega) = N_{K/Q}(y.\omega) \neq 0 \) and \( x.\omega = \eta y.\omega \), then \( N_{K/Q}\eta = +1 \).

Counting problem:

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

where \( \mathcal{K} \subset [-1, 1]^s \) convex.
Green–Tao methods (+Green–Tao–Ziegler inverse theorem) give such an asymptotic provided:

1. there are pseudo-random majorants
   \( \nu^{(T)} : \{1, \ldots, T\} \to \mathbb{R}_{>0} \) for sufficiently large \( T \) s.t.
   \[
   R(m) \leq C\nu^{(T)}(m), \quad \text{for } 1 \leq m \leq T,
   \]

2. \( R - \left( \frac{1}{T} \sum_{m \leq T} R(T) \right) \) 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:**

\[
\frac{1}{T} \sum_{m \leq T} \nu^{(T)}(m) = 1 + o(1)
\]

**The \(D\)-linear forms condition**

For all

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

we have

\[
\frac{1}{|\mathbb{Z}^d \cap K'|} \sum_{\mathbf{u} \in \mathbb{Z}^d \cap K'} \nu^{(T)}(h_1(\mathbf{u})) \ldots \nu^{(T)}(h_t(\mathbf{u})) = 1 + o(1).
\]
For multiplicative arith. functions one can hope for

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

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

Lemma

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

where

$$\zeta_K(s) = \sum_{(0) \neq a \subset o_K} (Na)^{-s} = \sum_{m \geq 1} \frac{r_K(m)}{m^s}$$

and

$$\sum_{0 < \epsilon m \leq T} R(m) \sim \kappa_\epsilon T, \quad \sum_{0 < m \leq T} r_K(m) \sim \kappa T.$$
Proof of Lemma

\[ R(m) = \# \{ x \in \mathbb{Z}^n / U_{K}^{(+)} : m = N_K(x) \} \]
\[ \leq 2 \# \{ x \in \mathbb{Z}^n / U_K : m = N_K(x) \} \]
\[ \leq 2 \# \{ x \in \mathbb{Z}^n / U_K : |m| = |N_K(x)| \} \]
\[ \leq 2 \# \{ (\alpha) \subset \mathfrak{o}_K : N(\alpha) = |m| \} \]
\[ \leq 2 \# \{ a \subset \mathfrak{o}_K : \mathcal{N} a = |m| \} = 2r_K(|m|) \]

\[ U_{K}^{(+)} = \ker(N_{K/Q} : U_K \to \{\pm 1\}) \]

Aim: Construct a majorant for \( r_K \) that takes the form

\[ \nu^{(T)}(m) = \sum_{d \leq T^\gamma 1_{d|m} \lambda_d.} \]
Multiplicative structure of $r_K$

If $(p) = p_1^{e_1} \cdots p_k^{e_k}$, $N \, p_i = p_i^{f_i}$, then

$$r_K(p^m) = \# \{p_1^{m_1} \cdots p_k^{m_k} : \sum_{i=1}^{k} f_i m_i = m\} < (m + 1)^n = \tau(p^m)^n.$$ 

At primes:

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

Define

$$\mathcal{P}_0 = \{ p \mid D_K \},$$
$$\mathcal{P}_1 = \{ p \mid D_K : \exists \, p | (p) \text{ such that } f_p(p) = 1 \},$$
$$\mathcal{P}_2 = \{ p \mid D_K : f_p(p) \geq 2 \text{ for all } p | (p) \}.$$ 

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 $\frac{1}{n} \leq \delta \leq 1$, 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 $\implies$ little control on $\mu * r_K$.

Define

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

Then

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

Suffices to find majorants for $1_{\langle \mathcal{P}_0 \cup \mathcal{P}_1 \rangle}$ and $r_{res}$ separately.
For $1_{\langle P_0 \cup P_1 \rangle} \leq \nu^{(T)}(m) = \left( \sum_{d \in \langle P_2 \rangle \mid m} \mu(d) \chi \left( \frac{\log d}{\log T^\gamma} \right) \right)^2$. 

Characteristic function
Majorants for positive multiplicative functions

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

(a) \( f(p^k) \leq H^k \) for all prime powers,
(b) \( f(m) \ll \delta m^\delta \) as \( m \to \infty \) for any \( \delta > 0 \), and
(c) \( f(p^{k-1}) \leq f(p^k) \) for all prime powers.

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

Define \( f^{(T)}_\gamma : \{1, \ldots, T\} \to \mathbb{R}_{\geq 0} \) via

\[
 f^{(T)}_\gamma (m) = \sum_{d \mid m, d \leq T^\gamma} 1_{d\mid m} \; g(d).
\]

Would like \( f(m) \ll f^{(T)}_\gamma (m) \) for \( m \leq T \).

Consider bad sets \( S(\kappa) = \{ m \leq T : f(m) > H^\kappa f^{(T)}_\gamma (m) \} \).

Note that

\[
 \forall m \exists \kappa : m \in S(\kappa) \setminus S(\kappa + 1) \text{ thus } f(m) \leq \sum_{\kappa \geq 0} H^{\kappa+1} 1_{S(\kappa)}(m) f^{(T)}_\gamma (m).
\]
Lemma (Based on ideas from paper of Erdős)

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

(i) \( p^a \mid m \) for some \( p^a, a \geq 2 \), with \( p^a \geq \log^{C_1} T \);

(ii) \( m \) is “smooth”:
\[
\prod_{p \leq T^{1/(\log \log T)^3}} p^{v_p(m)} \geq T^{\gamma/\log \log T};
\]

(iii) \( m \) has a “cluster” of prime factors: there is \( \log_2 \kappa - 2 \leq \lambda \ll \log \log \log \log T \) s.t.
\[
\# \left\{ p \mid m : T^{1/2^\lambda + 1} \leq p \leq T^{1/2^\lambda} \right\} \geq \gamma \kappa (\lambda + 3 - \log_2 \kappa) / 100
\]
(The product \( u \) of these primes satisfies \( u \leq T^{\gamma} \).)
Truncated divisor sum majorant for \(1_{S(\kappa)}\)

If

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

then

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

Recall:

\[
f(m) \leq \sum_{\kappa} 1_{S(\kappa)}(m) H^{\kappa+1} f^{(T)}(m)
\]

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

Then

\[
\sum_{m \leq T} \nu^{(T)}(m) \ll \sum_{m \leq T} f(m)
\]
Complete majorant

\[ \nu^{(T)}(m) = \left( \sum_{d \in \langle P_2 \rangle} 1_{d|m} \mu(d) \chi\left( \frac{\log d}{\log T^\gamma} \right) \right)^2 \]

\[ \times \left( \sum_{\kappa} \sum_{\lambda} \sum_{u \in U(\kappa, \lambda)} 2^{n\kappa} 1_{u|m} \sum_{d \in \langle P_0 \cup P_1 \rangle} g(d) \chi\left( \frac{\log d}{\log T^\gamma} \right) \right) \]
These ideas lead to a proof of the first of the requirements for an application of Green–Tao

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

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

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

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

$$f_i(u) = N_K(x_i), 1 \leq i \leq r.$$