The set of non-n-th powers in a number field is diophantine

Joint work with Jan Van Geel (Gent)

Jean-Louis Colliot-Thélène (CNRS et Université Paris-Sud, Orsay, visiting BICMR)

Capital Normal University
Beijing
25th November 2015

Diophantine sets in a field

k a field
A subset $D \subset k$ is called diophantine if there exists X algebraic variety over k and $\phi : X \to \mathbf{A}^1_k$ a k-morphism such that $D = \phi(X(k))$.

- Stable under finite union, finite intersection (use fibre product), addition, multiplication, composition with k-morphism $\mathbf{A}^1_k \to \mathbf{A}^1_k$. Thus $k^{\times n}$ is diophantine.
- Stable under deleting or adding finite number of elements of k
- If K/k finite field extension, $D \subset K$ is diophantine $\Longrightarrow$ $D \cap k \subset k$ is diophantine (use Weil restriction of scalars)

There are concrete cases where one would like to understand the structure of diophantine sets.
One parameter families of conics.
One parameter families of curves of genus one.
One parameter families of elliptic curves with generic fibre of rang zero and all sections taken away.

There is a motivation from logic : Were $\mathbf{Z} \subset \mathbf{Q}$ diophantine, then Hilbert's 10th problem over the rationals would have a negative answer (using Matijasevich's theorem over $\mathbf{Z}$).

Let us here mention the astonishing
Theorem (Königsmann 2010). *The complement of* $\mathbf{Z}$ *in* $\mathbf{Q}$ *is diophantine: There exists a* $\mathbf{Q}$*-morphism* $f : X \to \mathbf{A}^1_{\mathbf{Q}}$*, with* $X/\mathbf{Q}$ *affine of finite type, with* $f(X(\mathbf{Q})) = \mathbf{Q} \setminus \mathbf{Z}$.

k a number field, v a finite place of k, k_v completion, $O_v \subset k_v$ ring of integers

Proposition (Rumely, Poonen, Eisenträger, Königsmann)

(i) $k \cap O_v \subset k$ is diophantine

(ii) For $n \geq 1$ integer, $k \cap k_v^{\times n} \subset k$ is diophantine

(iii) For $n \geq 1$ integer, the complement of $k \cap k_v^{\times n} \subset k$ in k is diophantine.

Idea for (i) : For D/k a quaternion algebra ramified only at v and $w \neq v$, one considers the image of $Nrd_D(x) = 1$ under the reduced trace map from D to k. This produces (many) elements of k which are integral at v and w. On then uses two distinct w's and add the two images. This essentially gives $k \cap O_v \subset k$.

(ii) and (iii) then follow using Hensel's lemma, density of k in k_v, finiteness of $k_v^{\times}/k_v^{\times n}$.

Theorem (CT + Van Geel, 2014)
Let k be a number field and $n \in \mathbf{N}$, $n > 1$. The complement of $k^{\times n}$ in k is diophantine.

Easy reduction to the case $n = p$ prime and $\mu_p \subset k$.
The case $n = 2$: Poonen (2009). Alternative proof for $n = 2$, $k = \mathbf{Q}$: Königsmann (2010).
The case $n = p$ prime : Várilly-Alvarado and Viray (2011), proof *conditional* on Schinzel's hypothesis (generalisation of twin primes conjecture).

Recall : k number field, exact sequence (generalized quadratic reciprocity)

$$0 \to \mathrm{Br}(k) \to \oplus_v \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

X/k smooth projective variety, pairing

$$X(\mathbf{A}_k) \times \mathrm{Br}(X) \to \mathbf{Q}/\mathbf{Z}.$$

$X(\mathbf{A}_k)^{\mathrm{Br}(X)} \subset X(\mathbf{A}_k)$, left kernel of this pairing.

Proposition (Manin 1970). $X(k) \subset X(\mathbf{A}_k)$ lies in $X(\mathbf{A}_k)^{\mathrm{Br}(X)}$.

Key tool for Poonen, VA-V, CT-VanGeel : Use of varieties X for which the Brauer-Manin obstruction to the Hasse principle for rational points is the only obstruction : $X(\mathbf{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$ implies $X(k) \neq \emptyset$.

For $n = 2$, Poonen uses surfaces $y^2 - az^2 = P(x)Q(x)$ with deg(P)=deg(Q)=2 and a result of CT, Coray, Sansuc 1980 (generalized in CT, Sansuc, Swinnerton-Dyer 1987).

For $n = p$ prime, the *conditional* result of VA-V uses k with $\zeta_p \in k$, $K = k(d^{1/p})$, variety X with affine model $Norm_{K/k}(\Xi) = P(x)Q(x)$, with deg($P$)=deg($Q$)=$p$ and results *conditional* on Schinzel's hypothesis in CT-SwD 1994, CT-Skorobogatov-SwD 1998 (extending CT-Sansuc 1982, Serre 91, Sw-D 91).

For p prime, the *unconditional* result of CT-Van Geel, to be discussed here, uses (other) results of the same papers CT-SwD 1994 and CT-Sk-SwD 1998, $+\varepsilon$.
These results are obtained by a technique initiated by Salberger (1988).
One proves an analogue of

$$X(\mathbf{A}_k)^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(k) \neq \emptyset$$

for *zero-cycles of degree one* instead of rational points.

As also remarked by Wittenberg 2012, the proof in CT-SwD 1994 and CT-Sk-SwD 1998 may be adapted to show :

Theorem A (CT, SwD, Sk + ε). *Let k be a number field, p a prime, $\mu_p \subset k$. Let $P(x)$ and $Q(x)$ be two distinct monic irreducible polynomials of degree p. Let $c \in k^\times$. Let $K = k(d^{1/p})$ be a cyclic extension of fields. Let X/k be a smooth, projective model of the affine variety with equation*

$$Norm_{K/k}(\Xi) = cP(x)Q(x).$$

If $X(\mathbf{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$, then there exists an extension L/k of degree $2p+1$ such that $X(L) \neq \emptyset$.

Under the assumption $X(\mathbf{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$, we thus have $(Sym^{2p+1}X)(k) \neq \emptyset$.

As in the work of Poonen and of VA-V, one uses a specific counterexample to the Hasse principle. In the present work, we check that we also have an obstruction to the existence of a zero-cycle of degree one.

Proposition B (an example). *Let k be a number field, p a prime, $\mu_p \subset k$. There exist a cyclic extension $K = k(d^{1/p})$ $(d \in k^\times)$, $c \in k^\times$, $P(x)$ and $Q(x)$ two distinct monic irreducible polynomials of degree p such that for any smooth projective model X of the affine variety defined by $Norm_{K/k}(\Xi) = cP(x)Q(x)$ one has $X(\mathbf{A}_k) \neq \emptyset$, and for any field extension L/k with degree prime to p, $X(\mathbf{A}_L)^{\mathrm{Br}(X_L)} = \emptyset$, hence $X(L) = \emptyset$.*

Note : There exist smooth projective varieties Y/k with $Y(\mathbf{A}_k)^{\mathrm{Br}(Y)} = \emptyset$, but with a zero-cycle of degree 1 over k.

The obstruction comes from the class $A = (K/k, P(x)) \in \mathrm{Br}(X)$.
One produces $d, c, P(x), Q(x)$ and $a \in k^\times$ such that there exists a place v_0 of k with the following properties
(a) $(K/k, a)_{v_0} \neq 0 \in \mathbf{Z}/p$
(b) For any finite field extension L/k, for any w place of L and any $M_w \in X(L_w)$
$A(M_w) = 0 \in \mathbf{Z}/p$ if w does not lie over v_0
$A(M_w) = (K/k, a)_w \in \mathbf{Z}/p$ if w lies over v_0.

For each $u \in k^\times$ we denote by X_{du} a smooth projective model of the affine variety defined by $Norm_{k((du)^{1/p})/k}(\Xi) = cP(x)Q(x)$.

As experience teaches, counterexamples to the Hasse principle are scarce. The following statement is due to Poonen for $p = 2$.

Proposition C (finiteness of exceptions). *The set of $u \in k^\times$ such that $X_{du}(\mathbf{A}_k) \neq \emptyset$ and $X_{du}(\mathbf{A}_k)^{\mathrm{Br}(X_{du})} = \emptyset$ falls into finitely many classes in $k^\times/k^{\times p}$.*

This finiteness statement is similar to a classical finiteness statement (Kneser) : for a given integral, indefinite ternary quadratic form q over $\mathbf{Z}$, the integers n which are represented by q over each $\mathbf{Z}_p$ but are not represented over $\mathbf{Z}$ fall into finitely many classes in $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$.

Proof of Proposition C.

The X_{du}'s, for varying u, all contain the common curve Γ given by $z^p = cP(x)Q(x)$.

One shows : there exists a finite set S of places depending only on $c, d, P(x), Q(x)$ such that for $v \notin S_0$, for any $u \in k^\times$ with $v(u) \neq 0 \bmod p$, $(k((du)^{1/p}), P(x))$ takes all values in $\mathbf{Z}/p$ on $\Gamma(k_v)$.

One then produces a finite set S containing S_0, all bad reduction wrt to ∞, the prime p, c, d, $P(x)$, $Q(x)$, and such that $\Gamma(k_v) \neq \emptyset$ for $v \notin S$. If $v \notin S$, $u \in k^\times$ and $v(u) \neq 0 \ mod \ p$, if $X_{du}(\mathbf{A}_k) \neq \emptyset$ then $X_{du}(\mathbf{A}_k)^{\mathrm{Br}(X_{du})} \neq \emptyset$.

Theorem (CT + Van Geel)
Let k be a number field, p a prime, $\mu_p \subset k$. The complement of $k^{\times p}$ in k is diophantine.
Proof.
Let $c, d, P(x), Q(x)$ and the X_{du} be as above. Let S be a finite set of places of k as above. We consider the following subsets of $k^\times$, all stable under multiplication by $k^{\times p}$.
For $v \in S$, let $N_v \subset k^\times$ be the complement of $k_v^{\times p} \cap k$. This is a diophantine set.
Let $D_1 \subset k^\times$ be the set of $u \in k^\times$ such that $Sym_{2p+1}(X_{du})(k) \neq \emptyset$. This is a diophantine set given by the k-morphism $Sym_{2p+1}(X_{du}) \to \mathrm{Spec} k[u, u^{-1}]$.

For u in the complement of $\bigcup_{v\in S} N_v$, we have $X_{du}(\mathbf{A}_k) \neq \emptyset$ by the definition of S (we have $\Gamma(k_v) \neq \emptyset$ for $v \notin S$ and $X_{du}(k_v) = X_d(k_v)$ for $v \in S$.)
For u in the complement of $D_1 \cup \bigcup_{v\in S} N_v$, by theorem A (CT, SwD, Sk $+ \varepsilon$), we have $X_{du}(\mathbf{A}_k)^{\mathrm{Br}(X_{du})} = \emptyset$.
Proposition C (finiteness) then shows that the complement of $D_1 \cup \bigcup_{v\in S} N_v$ consists of finitely many cosets of $k^{\times p}$ in $k^\times$. By Proposition B (example), this complement contains the coset of 1, i.e. $k^{\times p}$.
Thus the complement of $k^{\times p}$ in $k^\times$ is the union of $D_1 \cup \bigcup_{v\in S} N_v$ and finitely many cosets of $k^{\times p}$, hence is a diophantine set.