

Brauer–Manin obstruction and integral points

Jean-Louis Colliot-Thélène (CNRS et Université Paris-Sud)

Number theory seminar

Cambridge

November 9, 2010

Let X/\mathbb{Q} be a smooth variety over the rationals.

Let $X(A_{\mathbb{Q}}) \subset \prod_p X(\mathbb{Q}_p)$ denote the adèles of X equipped with the adèlic topology. If X/\mathbb{Q} is projective, $X(A_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$ and the adèle topology is just the product topology.

Let $X_{\bullet}(A_{\mathbb{Q}})$ be the modified adèles, where $X(\mathbb{R})$ is replaced by its set of connected components.

We have the diagonal embedding

$$X(\mathbb{Q}) \subset X_{\bullet}(A_{\mathbb{Q}})$$

Basic question : **Is $X(\mathbb{Q})$ dense in $X_{\bullet}(A_{\mathbb{Q}})$?**

For X/\mathbb{Q} projective, $X(A_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$, we are concerned with rational points and we are asking for a Hasse principle and for weak approximation (with a weak condition at the reals).

For X/\mathbb{Q} affine, say $X = \mathcal{X} \times_{\mathbb{Z}} \mathbb{Q}$ for a scheme \mathcal{X} affine of finite type over \mathbb{Z} , we are in particular asking for a Hasse principle for the existence of an integral point on \mathcal{X} , as well as for strong approximation (with a weak condition at the reals).

Here are classical results in this direction.

The Hasse principle and weak approximation for rational points hold for :

Quadrics, more generally projective homogeneous spaces of connected linear algebraic groups (Eichler, Landherr, Kneser, Harder).

Smooth projective hypersurfaces $F_d(x_0, \dots, x_n) = 0$ with n big with respect to d : circle method (Hardy-Littlewood, Birch, Heath-Brown, Hooley ...)

The Hasse principle and strong approximation for integral points hold for :

Representation of an integer by an indefinite integral quadratic form in at least 4 variables (Eichler, Kneser)

Representation of an integer by certain integral forms $F_d(x_0, \dots, x_n)$ with n big with respect to the degree d (Waring's problem, circle method).

But many examples show that the Hasse principle, weak approximation and strong approximation in general do not hold. Here is a general formalism which explains many counterexamples to the Hasse principle, weak approximation and strong approximation.

Let F be a contravariant functor from \mathbb{Q} -schemes to sets. For any $\alpha \in F(X)$, one has a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \rightarrow & X(A_{\mathbb{Q}}) \\ \downarrow \text{ev}_{\alpha} & & \downarrow \text{ev}_{\alpha} \\ F(\mathbb{Q}) & \xrightarrow{\phi} & \prod'_p F(\mathbb{Q}_p) \end{array}$$

where $\prod'_p F(\mathbb{Q}_p)$ is a certain restricted direct product.

If $\text{Im}(\phi) \cap \text{ev}_{\alpha}(X(A_{\mathbb{Q}})) = \emptyset$, then $X(\mathbb{Q}) = \emptyset$.

How to control the image of $\phi : F(\mathbb{Q}) \rightarrow \prod'_p F(\mathbb{Q}_p)$?

First basic example:

$F(X) = \text{Br}(X)$ (Manin 1970)

One then uses the class field theory exact sequence

$$0 \rightarrow \text{Br}(\mathbb{Q}) \rightarrow \bigoplus_p \text{Br}(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

Second basic example: $F(X) = H_{\text{ét}}^1(X, G)$, where G is an algebraic group over \mathbb{Q} (Fermat, Cassels, CT/Sansuc, Harari/Skorobogatov). In various contexts, class field theory (generalization of Gauss's law of quadratic reciprocity) yields a control on the cokernel of the maps $\phi : H^1(\mathbb{Q}, G) \rightarrow \prod'_p H^1(\mathbb{Q}_p, G)$.

For G finite abelian, Poitou-Tate exact sequence

$$H^1(\mathbb{Q}, G) \rightarrow \prod_p' H^1(\mathbb{Q}_p, G) \rightarrow \text{Hom}(H^1(\mathbb{Q}, \hat{G}), \mathbb{Q}/\mathbb{Z})$$

For G a torus, Tate-Nakayama exact sequence

$$H^1(\mathbb{Q}, G) \rightarrow \bigoplus_p H^1(\mathbb{Q}_p, G) \rightarrow \text{Hom}(H^1(\mathbb{Q}, \hat{G}), \mathbb{Q}/\mathbb{Z})$$

For G an arbitrary connected linear algebraic group,
Kottwitz exact sequence of pointed sets:

$$H^1(\mathbb{Q}, G) \rightarrow \bigoplus_p H^1(\mathbb{Q}_p, G) \rightarrow \text{Hom}(\text{Pic}(G), \mathbb{Q}/\mathbb{Z})$$

There then arises the question : are the constraints coming from these various reciprocity laws the only ones preventing density of $X(\mathbb{Q})$ in $X_{\bullet}(A_{\mathbb{Q}})$?

For $F(X) = \text{Br}(X)$, this is the question whether the Brauer-Manin obstruction is the only obstruction (to existence of rational points, to weak approximation, to strong approximation).

Let me review the situation for **projective** varieties.

The density of $X(\mathbb{Q})$ in $X(A_{\mathbb{Q}})^{\text{Br}(X)}$ has been established for any smooth, projective, geometrically integral variety X birational to :

- a homogeneous space of a connected linear algebraic groups, if all geometric isotropy groups are connected (Sansuc 1981; Borovoi 1996)
- a conic bundle over \mathbb{P}^1 with at most 4 singular geometric fibres, for example $y^2 - az^2 = P(x)$ with $P(x)$ of degree 4 (special case CT, Coray, Sansuc 1981; CT, Sansuc, Swinnerton-Dyer 1987)
- a smooth intersection of two quadrics in \mathbf{P}^n , $n \geq 8$ (CT, Sansuc, Swinnerton-Dyer 1987)

The proofs involve several techniques :

- Fibration method (reduction to subvarieties)
- Descent method (reduction to the total space of a torsor over the given variety)
- Systematic use of class field theory (Tate-Nakayama).

In particular, the **exactness** of the sequence

$0 \rightarrow \text{Br}(\mathbb{Q}) \rightarrow \bigoplus_{p \cup \infty} \text{Br}(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ is fully used
(whereas to produce counterexamples one need only know that this is a complex.)

- use of the existing stock of varieties which satisfy the Hasse principle and weak approximation.

If one is willing to grant certain standard – but very difficult – conjectures, then there are many more classes of smooth, projective varieties for which one may prove

$$X(A_{\mathbb{Q}})^{\text{Br}(X)} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset \text{ (existence)}$$

or even better

$$X(\mathbb{Q}) \text{ dense in } X(A_{\mathbb{Q}})_{\bullet}^{\text{Br}(X)} \text{ (density).}$$

Under the finiteness of Tate-Shafarevich groups :

Curves of genus 1, more generally homogeneous spaces of abelian varieties (Manin 1970, L. Wang).

Let $C \hookrightarrow J$ be a curve of genus at least 2 embedded in its jacobian. Under the finiteness assumption of Sha,

$$X(A_{\mathbb{Q}})_{\bullet}^{\text{Br}X} = X(A_{\mathbb{Q}})_{\bullet} \cap J(\mathbb{Q})^{\text{closure}} \subset J(A_{\mathbb{Q}})_{\bullet}.$$

If $J(\mathbb{Q})$ is finite, this gives $X(\mathbb{Q}) = X(A_{\mathbb{Q}})_{\bullet}^{\text{Br}X}$
(Scharashkin, Skorobogatov)

Most diagonal cubic surfaces over \mathbb{Q} (existence, Swinnerton-Dyer 2000)

Under the Bouniakowsky-Dickson-Schinzel hypothesis :

Conic bundles over \mathbb{P}^1 with an arbitrary number of singular fibres
(CT-Sansuc, Serre, Swinnerton-Dyer)

Proof : Generalisation of Hasse's argument to prove the Hasse principle for quadratic forms in 4 variables from the case of 3 variables

Under both conjectures :

Certain surfaces with a fibration over \mathbb{P}^1 whose generic fibre is a curve of genus 1, including some $K3$ surfaces (existence, CT, Skorobogatov, Swinnerton-Dyer 1998, ...)

Most smooth intersections of two quadrics in \mathbf{P}^4 (existence, Wittenberg 2007; then density, Salberger/Skorobogatov)
Hasse principle for smooth intersections of two quadrics in \mathbf{P}^n , $n \geq 5$ (Wittenberg 2007)

Numerical support for $X(A_{\mathbb{Q}})^{\text{Br}(X)} \neq \emptyset \implies X(\mathbb{Q}) \neq \emptyset$ exist for :

- Diagonal cubic surfaces (CT, Kanevsky, Sansuc 1987; ...)
- Curves $y^2 = f_6(x)$ (Bruin and Stoll 2008)
[For curves of genus at least 2 over a global field of positive characteristic, the implication above has been established by Poonen and Voloch (2008) under very minor restrictions.]
- Some Shimura curves (Skorobogatov, ...)
- Some $K3$ -surfaces, in particular diagonal ones (Swinnerton-Dyer, Bright)

However : There exist smooth projective varieties X over \mathbb{Q} for which $X(A_{\mathbb{Q}})^{\text{Br}(X)} \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$.

– Skorobogatov (1999) (a twisted bielliptic surface)

This example, and others may be explained (Harari, Skorobogatov) by means of a functor $F(X) = H_{\text{ét}}^1(X, G)$ for G a finite, noncommutative group.

The technique has been further analyzed (Stoll, Demarche, Skorobogatov)

– Poonen (2009) (new type, not covered by the previous analysis)

In the rest of the talk, I shall discuss integral points

Modest start : \mathbf{P}^1 minus a point

A nearly trivial result :

Let $a, b, c \in \mathbb{Z}$ not all zero. If the \mathbb{Z} -curve X defined by $ax + by = c$ has solutions in all \mathbb{Z}_p , then it has solutions in \mathbb{Z} .

Here $X_{\mathbb{Q}} \simeq \mathbf{P}_{\mathbb{Q}}^1 \setminus \{\infty\}$. Hence $\text{Br}(X_{\mathbb{Q}})/\text{Br}(\mathbb{Q}) = 0$ creates no obstruction!

The strong approximation theorem (here : the Chinese remainder theorem) yields the much more precise result :

$X(\mathbb{Z})$ is dense in $\prod_{p < \infty} X(\mathbb{Z}_p)$

(Note that the real completion is omitted.)

A more difficult, but in the end classical case : \mathbf{P}^1 minus two points

The \mathbb{Z} -curve X defined by

$$2x - 5y = 1, xt = 1$$

has solutions in all \mathbb{Z}_p but not in \mathbb{Z} .

Here $X_{\mathbb{Q}} \simeq \mathbf{P}_{\mathbb{Q}}^1 \setminus \{0, \infty\}$. Hence $\text{Br}(X_{\mathbb{Q}})/\text{Br}(\mathbb{Q}) = H^1(\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$.

There is a Brauer-Manin obstruction attached to the quaternion class $(x, 5) \in \text{Br}(X_{\mathbb{Q}})$.

The same argument shows that for K/\mathbb{Q} field extension of odd degree, unramified and totally split at 2 and 5, $X(O_K) = \emptyset$.

In a not completely immediate fashion, class field theory yields

Theorem (Harari 2008) *Let X be a curve over \mathbb{Q} which over an algebraic closure of \mathbb{Q} is isomorphic to \mathbf{P}^1 minus two points. Then $X(\mathbb{Q})$ is dense in $X(A_{\mathbb{Q}})_{\bullet}^{\text{Br}X}$.*

[Harari's result deals with arbitrary homogeneous spaces of tori.]

This holds in particular for equations

$$a = q(x, y)$$

with $a \in \mathbb{Q}^*$ and $q(x, y)$ a nondegenerate binary quadratic form.

Difficulty for application : the quotient $\text{Br}(X)/\text{Br}(\mathbb{Q})$ is infinite !

For a given X/\mathbb{Z} given by $a = q(x, y)$, it is thus not clear how to decide whether or not $(\prod_p X(\mathbb{Z}_p))^{\text{Br}(X_{\mathbb{Q}})} \neq \emptyset$.

There are nevertheless partial results in this direction (Wei, Xu) which generalize results such as Gauß' result on $p = x^2 + 27y^2$ (a prime p is of this shape if and only if it is so locally AND $2 = z^3$ may be solved in \mathbb{F}_p).

The situation improves if one looks at the problem of representation of an integer by a (\mathbb{Q} -nondegenerate) integral quadratic form in $n \geq 3$ variables, if one moreover assumes that q is indefinite over \mathbb{R} .

Let X be the \mathbb{Z} -scheme defined by $a = q(x_1, \dots, x_n)$.

For $n \geq 4$, $\text{Br}(X_{\mathbb{Q}})/\text{Br}(\mathbb{Q}) = 0$.

For $n = 3$, $\text{Br}(X_{\mathbb{Q}})/\text{Br}(\mathbb{Q}) \subset \mathbb{Z}/2$.

Theorem Let $q(x_1, \dots, x_n)$ be an integral quadratic form of rank n , indefinite over \mathbb{R} , and let $a \in \mathbb{Z}$, $a \neq 0$. Let X/\mathbb{Z} be the \mathbb{Z} -scheme defined by $q(x_1, \dots, x_n) = a$.

(a) If $n \geq 4$ then $X(\mathbb{Z})$ is dense in $\prod_p X(\mathbb{Z}_p)$.

(b) Assume $n = 3$. Then $X(\mathbb{Z})$ is dense in $[\prod_p X(\mathbb{Z}_p)]^{\text{Br}X_{\mathbb{Q}}}$.

If $-a \cdot \det(q)$ is a square, $\text{Br}(X_{\mathbb{Q}})/\text{Br}(\mathbb{Q}) = 0$.

If $-a \cdot \det(q)$ is not a square, $\text{Br}(X_{\mathbb{Q}})/\text{Br}(\mathbb{Q}) = \mathbb{Z}/2$. Let $A \in \text{Br}(X_{\mathbb{Q}})$ generate this quotient. Then $X(\mathbb{Z}) \neq \emptyset$ if and only if the map

$$\prod_p X(\mathbb{Z}_p) \rightarrow \mathbb{Q}/\mathbb{Z}$$
$$\{M_p\} \mapsto \sum_p \text{ev}_A(M_p)$$

contains 0 in its image.

Theorem (a) goes back to the 1950's (Eichler, Kneser, Watson).
Theorem (b) is a variant (CT/Xu 2009) of a result of Borovoi et Rudnick (1995).

The main points of the proof of (b) are :

- strong approximation for the spinor group of an indefinite quadratic form
- representation of an affine quadric $q = a$ over \mathbb{Q} , with a \mathbb{Q} -rational point, as a quotient G/T , where G is the spinor group of q and T is a 1-dimensional algebraic torus over \mathbb{Q} .

In the case $n = 3$, one may produce the algebra A . Let M be a \mathbb{Q} -point on

$$q(x, y, z) = a.$$

(Denis Simon has an algorithm to find such a point). Let $l(x, y, z) = 0$ be the equation for the tangent plane to the affine quadric $X_{\mathbb{Q}}$ at the point M .

As A one may take the quaternion algebra

$$A = (l(x, y, z), -a \cdot \det(q)).$$

With $M = (0, -1/n^k, 0)$ and $A = (1 + n^k y, n)$, we recover :

Theorem (R. Schulze-Pillot and F. Xu, 2004)

Let n, m, k be positive integers, $(n, m) = 1$. Let $X_{m,n,k}$ be the scheme over \mathbb{Z} defined by

$$m^2 x^2 + n^{2k} y^2 - nz^2 = 1$$

or

$$(1 + n^k y)(1 - n^k y) = m^2 x^2 - nz^2.$$

(a) For all n, m, k , $\prod_{p \in \mathbb{P}} X_{m,n,k}(\mathbb{Z}_p) \neq \emptyset$.

(b) $X_{m,n,k}(\mathbb{Z}) = \emptyset$ if and only if either

(i) 2 divides m exactly and $n \equiv 5 \pmod{8}$

or

(ii) 4 divides m and $n \equiv 3$ or $5 \pmod{8}$.

The above results on the representation of an integer by an integral quadratic form have been generalized in various directions. Here is the present utmost generalisation.

Theorem (Borovoi/Demarche 2009) *Let G be a connected (not necessarily linear) algebraic group over \mathbb{Q} . Let X be a homogeneous space with connected geometric stabilizers. Under a noncompactness assumption over \mathbb{R} for all simple factors of the derived group of G , and under the assumption that the Tate-Shafarevich group of the maximal abelian variety quotient of G is finite, then*

$$X(\mathbb{Q}) \text{ is dense in } X(A_{\mathbb{Q}})_{\bullet}^{\text{Br}(X_{\mathbb{Q}})}.$$

This builds upon work of Borovoi/CT/Skorobogatov, CT/Xu, Harari-Szamuely, Harari, Demarche (2005/2010)

And when there is no homogeneous space structure ?

\mathbb{P}^1 minus three points

F. Voloch pointed out the following conjecture of Skolem (1937). Let S be a finite set of prime numbers $p_i, i = 1, \dots, n$. Let $R \subset \mathbb{Q}^\times$ be the subgroup generated by the p_i . Let a_1, a_2, a_3 be elements in R .

Skolem's conjecture :

The equation $\sum_{i=1}^3 a_i x_i = 0$ has solutions with $x_i \in R$ if and only if for all integer m prime to S , the equation

$\sum_{i=1}^3 a_i x_i = 0 \pmod{m}$ has a solution for all $x_i \in R$.

Let $X \subset \mathbb{P}_{\mathbb{Q}}^1$ be an open set whose geometric complement consist of at least 3 points. One may view X as a closed curve in a \mathbb{Q} -torus T . The whole situation may be realized over the ring O_S of S -integers, for some finite set S of places. We thus have $\mathcal{X} \subset \mathcal{T}$.

Conjecture (Harari and Voloch 2009)

$$\mathcal{X}(O_S) = \left[\prod_{v \notin S} \mathcal{X}(O_v) \right] \cap \mathcal{T}(O_S)^{closure} \subset \prod_{v \notin S} \mathcal{T}(O_v).$$

They show that $\left[\prod_{v \notin S} \mathcal{X}(O_v) \right] \cap \mathcal{T}(O_S)^{closure}$ may be interpreted as a Brauer-Manin set of \mathcal{X} (analogue of the result by Scharashkin and Skorobogatov).

One might be tempted to produce further conjectures of the kind for integral points of arbitrary hyperbolic curves.

Harari and Voloch however have a striking bad example.

They take the affine curve X/\mathbb{Z} given by $y^2 = x^3 + 3$. Over \mathbb{Q} , this is the complement of one rational point in an elliptic curve E . Let P be the point $(x, y) = (1, 2)$. One has $E(\mathbb{Q}) = \mathbb{Z} \cdot P$ and $X(\mathbb{Z}) = \{\pm P\}$. They show that there exists a sequence in $E(\mathbb{Q})$ which under the embedding $E(\mathbb{Q}) \hookrightarrow E(A_{\mathbb{Q}})$ converges to a point in $\prod_p X(\mathbb{Z}_p)^{\text{Br}X_{\mathbb{Q}}}$ which is neither P nor $-P$.

The equation $a = x^3 + y^3 + z^3$, with $a \in \mathbb{Z}$ nonzero.

There are solutions with $x, y, z \in \mathbb{Q}$.

For $a = 9n \pm 4$ with $n \in \mathbb{Z}$, there are no solutions with $x, y, z \in \mathbb{Z}$.

Famous open question : if a is not of the shape $9n \pm 4$, is there a solution with $x, y, z \in \mathbb{Z}$?

Open already for $a = 33$.

Theorem (CT/Wittenberg 2009) *Let X_a be the \mathbb{Z} -scheme defined by $x^3 + y^3 + z^3 = a$, with $a \neq 0$. If $a \neq 9n \pm 4$, then*

$$\left(\prod_p X_a(\mathbb{Z}_p)\right)^{\text{Br}(X_a, \mathbb{Q})} \neq \emptyset.$$

In other words, no reciprocity law whatsoever will prevent this equation from having an integral solution.

To prove such a result, one must compute $\text{Br}(X_{a,\mathbb{Q}})/\text{Br}(\mathbb{Q})$.
Let $X_{a,\mathbb{Q}}^c \subset \mathbf{P}_{\mathbb{Q}}^3$ be the cubic surface with homogeneous equation $x^3 + y^3 + z^3 = at^3$. Let E be the elliptic curve over \mathbb{Q} with equation $x^3 + y^3 + z^3 = 0$. This is the complement of $X_{a,\mathbb{Q}}$ in $X_{a,\mathbb{Q}}^c$. There is a localisation exact sequence

$$0 \rightarrow \text{Br}(X_{a,\mathbb{Q}}^c) \rightarrow \text{Br}(X_{a,\mathbb{Q}}) \rightarrow H^1(E, \mathbb{Q}/\mathbb{Z}).$$

The last group classifies abelian unramified covers of E . We may assume that a is not a cube. An algebraic computation yields $\text{Br}(X_{a,\mathbb{Q}}^c)/\text{Br}(\mathbb{Q}) = \mathbb{Z}/3$, with an explicit generator $\beta \in \text{Br}(X_{a,\mathbb{Q}}^c)$, of order 3.

An algebraic argument shows that the image of $\text{Br}(X_{a,\mathbb{Q}}) \rightarrow H^1(E, \mathbb{Q}/\mathbb{Z})$ consist of classes which vanish at each of the points $(1, -1, 0)$, $(0, 1, -1)$, $(1, 0, -1)$.

One then uses arithmetic for the elliptic curve E over \mathbb{Q} (knowledge of all isogeneous curves) to show that such a class in $H^1(E, \mathbb{Q}/\mathbb{Z})$ is zero. Thus $\text{Br}(X_{a,\mathbb{Q}}^c) = \text{Br}(X_{a,\mathbb{Q}})$.

One then shows that for any $a \in \mathbb{Z}$ not a cube and not of the shape $9n \pm 4$, there exists a prime p such that β takes three distinct values on $X_a(\mathbb{Z}_p)$.

Thus

$$\left(\prod_p X_a(\mathbb{Z}_p)\right)^{\text{Br}(X_{a,\mathbb{Q}})} = \left(\prod_p X_a(\mathbb{Z}_p)\right)^\beta \neq \emptyset$$

It is an open question whether any integer a may be written as $x^3 + y^3 + 2z^3$, with $x, y, z \in \mathbb{Z}$.

Theorem (CT/Wittenberg 2009)

Let Y_a be the \mathbb{Z} -scheme defined by $x^3 + y^3 + 2z^3 = a$, with $a \neq 0$.

Then

$$\left(\prod_p Y_a(\mathbb{Z}_p)\right)^{\text{Br}(X_a, \mathbb{Q})} \neq \emptyset.$$

In other words, no reciprocity law whatsoever will prevent this equation from having an integral solution.

The proof here is more delicate : the restriction map $\mathrm{Br}(Y_{a,\mathbb{Q}}^c) \rightarrow \mathrm{Br}(Y_{a,\mathbb{Q}})$ is not onto. We have $\mathrm{Br}(Y_{a,\mathbb{Q}})/\mathrm{Br}(\mathbb{Q}) \simeq \mathbb{Z}/3 \oplus \mathbb{Z}/2$.

For $U \subset X$ the complement of a smooth curve C in say a geometrically rational smooth projective surface X , the quotient $\text{Br}(U)/\text{Br}(\mathbb{Q})$ need not be finite.

Example : complement U of a smooth conic in $\mathbb{P}_{\mathbb{Q}}^2$ (a log del Pezzo surface). In this case $\text{Br}(U)/\text{Br}(\mathbb{Q}) = \mathbb{Q}^*/\mathbb{Q}^{*2}$.

Let $q(x, y, z) = 16x^2 + 9y^2 - 3z^2$. Consider the \mathbb{Z} -scheme $X \subset \mathbb{P}_{\mathbb{Z}}^2$ defined by $q(x, y, z) \neq 0$. Let Q be the affine quadric over \mathbb{Z} defined by $q(x, y, z) = 1$.

Using the obvious μ_2 -covering $Q_{\mathbb{Q}} \rightarrow X_{\mathbb{Q}}$, one shows :

$$[\prod_p X(\mathbb{Z}_p)]^{\text{Br}X_{\mathbb{Q}}} \neq \emptyset \text{ but } X(\mathbb{Z}) = \emptyset.$$

This provides a rather simple “Skorobogatov” type of example in the affine context. Other examples were found by Kresch and Tschinkel.

The equation $q(x, y) = P(t)$ over \mathbb{Z}

Here q is a binary quadratic form, $P(t)$ a polynomial.

Over \mathbb{Q} , we had more theoretical success with these equations than with cubic surfaces.

One would like to investigate such equations over \mathbb{Z} . But this looks hard, even for $P(t)$ of degree at most 4.

The first step will be to determine the Brauer-Manin set.

Let us for now look at a simpler problem, one which would be trivial over the rationals.

The equation $q(x, y, z) = P(t)$ over \mathbb{Z}

Proposition (CTXu, 2010)

Let $q(x, y, z)$ be an indefinite, non degenerate quadratic form with coefficients in \mathbb{Z} . Let $P(t) \in \mathbb{Z}[t]$ be nonconstant and separable as a polynomial in $\mathbb{Q}[t]$. Let X/\mathbb{Z} be defined by the affine equation $q(x, y, z) = P(t)$.

Then $X(\mathbb{Z})$ is dense in $\prod_p X(\mathbb{Z}_p)$.

In particular, the Hasse principle holds for integral points.

The key idea is that for a given indefinite form $q(x, y, z)$ as above, the integers n for which the integral Hasse principle for $q(x, y, z) = n$ fail fall into finitely many classes in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. This is a classical result, and may be deduced from the theory developed above.

Given a family $\{M_p\} \in \prod_p X(\mathbb{Z}_p)$, with associated family $\{t_p\}$ in $\prod_p \mathbb{Z}_p$, and a fixed set S of finite places, which one may assume contains all the dyadic and bad places for q , an application of the Chinese remainder theorem yields a $t_0 \in \mathbb{Z}$ very close to t_p for $p \in S$ and such that moreover $P(t_0)$ is not in one of the exceptional classes in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. One then uses the density result for

$$q(x, y, z) = P(t_0).$$

Appendix : The classical (German) language for integral quadratic forms (Eichler, Kneser), as reviewed in CT/Xu

Let $f(x_1, \dots, x_n)$ et $g(y_1, \dots, y_m)$ be integral quadratic forms, $1 \leq n < m$ and $m \geq 3$.

One looks for linear forms $l_i(x_1, \dots, x_n), i = 1, \dots, m$ such that

$$g(x_1, \dots, x_n) = f(l_1(x_1, \dots, x_n), \dots, l_m(x_1, \dots, x_n)).$$

This defines a scheme $X = X(g, f)$ over \mathbb{Z} . One assumes that it has points over each \mathbb{Z}_p and one asks if it has points in \mathbb{Z} .

To f and g one classically associates lattices (Gitter) N et M .

Das Gitter N wird von der Klasse des Gitters M dargestellt.

Translation :

$$X(\mathbb{Z}) \neq \emptyset$$

Das Gitter N wird von dem Geschlecht des Gitters M dargestellt.

Translation :

$$\prod_p \mathcal{X}(\mathbb{Z}_p) \neq \emptyset$$

Das Gitter N wird von dem Spinorgeschlecht des Gitters M dargestellt.

Translation :

$$(\prod_p X(\mathbb{Z}_p))^{\text{Br}X_{\mathbb{Q}}} \neq \emptyset$$

Assume $m - n = 2$ and $-\text{disc}(f) \cdot \text{disc}(g)$ not a square.

Ein Gitter N , das zwar von dem Geschlecht von M dargestellt ist, nicht aber von allen Spinorgeschlechtern im Geschlecht von M dargestellt wird, nennt man eine Spinorausnahme.

Translation :

Let $A \in \text{Br}X_{\mathbb{Q}}$ be a generator of $\text{Br}X_{\mathbb{Q}}/\text{Br}\mathbb{Q} = \mathbb{Z}/2$. Then for each prime p , A takes only one value on $X(\mathbb{Z}_p)$.