Brauer–Manin obstruction and integral points

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

VU Amsterdam

February 26, 2010

The basic diophantine questions

Let $f(x_1, \cdots, x_n)$ be a polynomial with integral coefficients. Can we decide if the equation

$$f(x_1, \cdots, x_n) = 0$$

has integral solutions ($x_i \in \mathbb{Z}$) rational solutions ($x_i \in \mathbb{Q}$) ?

For homogeneous equations, one asks for primitive solutions and then there is just one problem.

In the language of schemes, one has a scheme X over $\mathbb{Z}$, resp. over $\mathbb{Q}$. One wants to decide if the set of integral points $X(\mathbb{Z})$, resp. the set of rational points $X(\mathbb{Q})$, is nonempty.

There are immediate conditions to be satisfied.
The equation $x^2 + y^2 - 3z^2 = 0$ has no nontrivial solutions, as may be seen either by congruences modulo 9 or by congruences modulo 4.
No congruence must be in the way. We know since Hensel that this condition translates as : for any prime p, the set $X(\mathbb{Z}_p)$, resp. the set $X(\mathbb{Q}_p)$, is not empty, where $\mathbb{Z}_p$ is the ring of p-adic integers and $\mathbb{Q}_p$ is its fraction field, the field of p-adics.
There must also exist real points, i.e. $X(\mathbb{R}) \neq \emptyset$.

For a given separated scheme of finite type over $\mathbb{Z}$, resp. over $\mathbb{Q}$, the inclusions

$$X(\mathbb{Z}) \subset \prod_p X(\mathbb{Z}_p) \subset X(A_{\mathbb{Q}})$$

$$X(\mathbb{Q}) \subset X(A_{\mathbb{Q}}) \subset \prod_p X(\mathbb{Q}_p)$$

summarize all the possible congruence conditions.
For $p = \infty$,we have set $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.
The set $X(A_{\mathbb{Q}})$, the space of adèles consits of families of local points which are integral for almost all p. If $X/\mathbb{Q}$ is projective, this is just $\prod_p X(\mathbb{Q}_p)$.

Whether the middle and right sets are not empty can be decided in a finite amount of time.

Legendre's theorem

Theorem (Legendre, 1785) *Let $q(x, y, z)$ be an integral quadratic form. If $q(x, y, z) = 0$ has nontrivial solutions in each $\mathbb{Z}_p$, including $\mathbb{R}$, then it has a nontrivial solution in $\mathbb{Z}$.*
Proof : geometry of numbers. One gets an upper estimate for the size of a solution.

The various proofs do not use the full hypothesis. For instance one may forget the hypothesis $X(\mathbb{R}) \neq \emptyset$. It turns out to be imposed by the hypothesis $X(\mathbb{Z}_p) \neq \emptyset$ for all finite p.

The law of quadratic reciprocity (theorema fundamentale)

Let $p \neq 2$ be an odd prime, $a \in \mathbb{Z}$ prime to p,
Recall the Legendre symbol $(a/p) = \pm 1$:
$(a/p) = 1$ iff a is a square mod. p.

Let p, q be odd primes. Then

$$(p/q)(q/p) = (-1)^{(p-1)/2.(q-1)/2}$$

Conjectured by Euler and by Legendre (1785). Proved by Gauß (1796).

The Hasse principle for quadratic forms

Theorem (Minkowski; Hasse 1920) *Let $n \geq 2$. Let $q(x_1, \cdots, x_n)$ be an integral quadratic form. If*

$$q(x_1, \cdots, x_n) = 0$$

has nontrivial solutions in all $\mathbb{Z}_p$, also in $\mathbb{R}$, then it has a nontrivial solution in $\mathbb{Z}$.

In Hasse's proof, the main ingredient occurs when passing from the case of 3 variables to the case of 4 variables. Hasse combines Dirichlet's theorem on primes in an arithmetic progression with the law of quadratic reciprocity.

As for local-global principles for *integral points*, here are some celebrated cases.

A prime congruent to 1 modulo 4 is a sum of two squares of integers (Fermat).

Let n be an integer. If the equation $n = x^2 + y^2 + z^2$ has solutions in $\mathbf{R}$ and in $\mathbb{Z}_2$, then it has a solution in $\mathbb{Z}$ (Legendre, Gauß)

Let n be an integer. The equation $n = x^2 + y^2 + z^2 + t^2$ has a solution in integers if $n > 0$ (Lagrange)

Basic question : **Are there such local-global theorems ("Hasse principles'), or appropriate substitutes, for other classes of schemes ?**

Here are classical results in this direction.

The Hasse principle for rational points holds for :

Projective homogeneous spaces of connected linear algebraic groups (Eichler, Landherr, Kneser, Harder).

Projective hypersurfaces $F_d(x_0, \cdots, x_n) = 0$ with n big with respect to d and singular locus not too big : circle method (Hardy-Littlewood, Birch, Heath-Brown, Hooley ...)

The Hasse principle for integral points holds for :

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

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

But many examples show that the “Hasse principle” in general does not hold. Most textbooks stop here.

Counterexamples to the Hasse principle for rational points

Norm form equations $\mathrm{Norm}_{K/\mathbb{Q}}(\xi) = c$ (Hasse, Witt),
more generally, homogeneous spaces of connected linear algebraic groups (Serre).

Curves of genus 1 (homogeneous spaces of elliptic curves)
$2y^2 = x^4 - 17$ (Reichard, Lind)

(Geometrically) rational surfaces :

Surfaces with a pencil of conics $a(t)x^2 + b(t)y^2 + c(t)z^2 = 0$, for example (Iskovskikh) $x^2 + y^2 + (3 - t^2)(2 - t^2)z^2 = 0$.

Cubic surfaces (Swinnerton-Dyer 1962), diagonal cubic surfaces (Cassels–Guy 1966) $5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$.

Counterexamples to the Hasse principle for integral points

Classical question : given an integral binary quadratic form $q(x, y)$ and an integer n, is there a systematic method to decide if the equation $n = q(x, y)$ has a solution with $x, y \in \mathbb{Z}$?

Congruences in general do not suffice, as the following examples reveal.

$$23 = x(x + 7y)$$

$$1 = 4x^2 + 25y^2$$

$$1 = 4x^2 - 475y^2$$

which also reads

$$(1 - 2x)(1 + 2x) = -25.19y^2$$

The proof that there are no integral solutions in the first two cases is elementary : use divisibility arguments and size arguments, together with the fact that the only units in $\mathbb{Z}$ are ± 1.
For an equation of the shape $n = l(x, y).m(x, y)$, l and m linear, there is a finite process to decide existence of an integral solution.
This uses $\mathbb{Z}^\times = \pm 1$. What about the analogous probem over a number field ?
What about equations $n = q(x, y)$ when q is irreducible ?
Here is a striking theorem (described in Cox's book *Primes of the form* $x^2 + ny^2$).
For q prime congruent to 1 mod. 3, the equation $q = x^2 + 27y^2$, which has solutions in all $\mathbb{Z}_p$, has solutions in $\mathbb{Z}$ if and only if 2 is a cube in the finite field $\mathbb{F}_q$ (conjectured by Euler, proved by Gauß).

Around 1970, there were quite a few counterexamples to the Hasse principle in the literature. If you looked at these, you could see that at some point in the proof that there are no rational points, the law of quadratic reciprocity, or sometimes a higher reciprocity law, was used. In 1970, Manin showed how to put (nearly) all the known counterexamples into a common framework.

Let me describe the Brauer–Manin obstruction to the Hasse principle.

The Brauer group of a field

Let k be a field, let $\overline{k}$ be a separable closure of k.
Assume $\mathrm{char}(k) \neq 2$. Let $a, b \in k^*$. Imposing the relations

$$i^2 = a, j^2 = b, ij = -ji$$

yield a 4-dimension k-algebra $A = (a, b)_k$ over k. It is a "twisted form" of the 2×2 matrices :

$$A \otimes \overline{k} \simeq M_2(\overline{k}).$$

For $k = \mathbf{R}$, $a = b = -1$, these are the Hamilton quaternions.

Quite generally, a finite dimensional k-algebra is called a central simple algebra (Hyperkomplexensystem) if there exists an integer $n \geq 1$ such that

$$A \otimes_k \overline{k} \simeq M_n(\overline{k}).$$

The tensor product of two central simple k-algebras is a central simple k-algebra.
Two such k-algebras are called equivalent if there exist integers $r, s \geq 1$ such that $M_r(A) \simeq M_s(B)$. Tensor product gives the set of equivalence classes of central simple k-algebras an abelian group structure. This is the Brauer group $\mathrm{Br}(k)$ of k (R. Brauer, A. A. Albert).

Class field theory

Local class field theory

$$\mathrm{Br}(\mathbb{Q}_p) \simeq \mathbb{Q}/\mathbb{Z}.$$

$$\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2$$

The fundamental exact sequence of global class field theory

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{p \cup \infty} \mathrm{Br}(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

The formula $\sum_p (a, b)_p = 0$ contains as a special case the law of quadratic recriprocity.

A conic $x^2 - ay^2 - bt^2 = 0$ over a field k (char.$(k) \neq 2$) has a rational point if and only if the class of the "associated" quaternion algebra $(a, b)_k \in \mathrm{Br}(k)$ vanishes.

Legendre's theorem in this context : If for each prime p (finite or infinite) $(a, b)_p \in \mathbb{Z}/2 \subset \mathrm{Br}(\mathbb{Q}_p)$ vanishes, then $(a, b) = 0 \in \mathrm{Br}(\mathbb{Q})$.

From $\sum_p (a, b)_p = 0$ we see that the vanishing of $(a, b)_p$ for all p (finite or infinite) *except possibly one* is enough to guarantee the vanishing of *all* $(a, b)_p$ and of $(a, b) = 0 \in \mathrm{Br}(\mathbb{Q})$.

The Brauer group of a scheme

A field k determines a scheme $\mathrm{Spec}(k)$.

On an algebraic variety and more generally over a scheme X, vector bundles are the analogues of vector spaces over a field.

Azumaya algebras over a scheme X are the natural generalisations of central simple agebras over a field.

One may introduce an equivalence relation on the Azumaya algebras over a given scheme X, analogous to the one we described earlier. Tensor product gives the equivalence classes the structure of an abelian group, the Brauer group $\mathrm{Br}(X)$ of X.

The construction is functorial in X. If X is a scheme over a ring R, there is a natural pairing $X(R) \times \mathrm{Br}(X) \to \mathrm{Br}(R)$.

The Brauer-Manin condition

Theorem (Manin, 1970). *Let X be a projective variety over $\mathbb{Q}$. Let $X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \subset X(A_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$ denote the left kernel of the (well defined) pairing*

$$X(A_{\mathbb{Q}}) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

Then

$$X(\mathbb{Q}) \subset X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \subset X(A_{\mathbb{Q}}).$$

The middle set is referred to as the Brauer-Manin set of X.

The integral version received attention only recently.

Theorem *Let X be a separated $\mathbb{Z}$-scheme of finite type. Let $(\prod_p X(\mathbb{Z}_p))^{\mathrm{Br}(X_{\mathbb{Q}})} \subset \prod_p X(\mathbb{Z}_p)$ be the left kernel of the (well defined) pairing*

$$\prod_p X(\mathbb{Z}_p) \times \mathrm{Br}(X_{\mathbb{Q}}) \to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

Then

$$X(\mathbb{Z}) \subset (\prod_p X(\mathbb{Z}_p))^{\mathrm{Br}(X_{\mathbb{Q}})} \subset \prod_p X(\mathbb{Z}_p).$$

Note that we pair with $\mathrm{Br}(X_{\mathbb{Q}})$. A more obvious pairing would have been with $\mathrm{Br}(X)$, but it would give less information.

After some work, it turned out that all the counterexamples to the Hasse principle for *rational points* known until 1970, and indeed until 1999, could be explained by the Brauer-Manin obstruction.

One then started looking for *classes* of smooth, projective, geometrically connected algebraic varieties over $\mathbb{Q}$ for which the Brauer-Manin obstruction "is the only one", that is, for any variety X in such a class, one has

$$X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbb{Q}) \neq \emptyset$$

Note the subsidiary question : It is easy to check whether $X(A_{\mathbb{Q}}) \neq \emptyset$, but what about decision procedures for $X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset$?

The implication $X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbb{Q}) \neq \emptyset$ has been established for 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 (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
$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{p \cup \infty} \mathrm{Br}(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z} \to 0$ 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

If one is willing to grant certain standard – but very difficult – conjectures, then there are many more classes of varieties for which one may prove the implication $X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbb{Q}) \neq \emptyset$.

Under the finiteness of Tate-Shafarevich groups :

Curves of genus 1 (Manin 1970)

Curves of arbitrary genus whose Jacobian has only finitely many rational points (Scharashkin)

Many diagonal cubic surfaces over $\mathbb{Q}$ (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 (CT, Skorobogatov, Swinnerton-Dyer 1998, ...)

Most smooth intersections of two quadrics in $\mathbf{P}^4$
Hasse principle for smooth intersections of two quadrics in $\mathbf{P}^n, n \geq 5$
(Wittenberg 2007)

Numerical support for $X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset \Longrightarrow X(\mathbb{Q}) \neq \emptyset$ 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 projective varieties X over $\mathbb{Q}$ for which $X(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$.

– Skorobogatov (1999) (a twisted bielliptic surface)
The technique has been analyzed (Harari, Skorobogatov, Demarche)
In Brief : One takes into account Galois unramified covers whose Galois group need not be commutative, and one involves the Brauer group of the covering spaces). Such covers are also of interest in the analysis of rational points on curves (Stoll).

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

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

The integral Brauer-Manin obstruction : a family of examples

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

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

or

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

F. Xu and R. Schulze-Pillot studied the integral solutions, i.e. the points of $X(\mathbb{Z})$. Let us apply the Brauer–Manin method.
One checks that $\prod_{p \cup \infty} X(\mathbb{Z}_p) \neq \emptyset$.

Let $U_{\mathbb{Q}} \subset X_{\mathbb{Q}}$ be the Zariski open set $1 + n^k y \neq 0$.
Algebraic fact : The (Azumaya) quaternion algebra $(1 + n^k y, n) \in \mathrm{Br}(U_{\mathbb{Q}})$ extends to $A \in \mathrm{Br}(X_{\mathbb{Q}})$, and spans $\mathrm{Br}(X_{\mathbb{Q}})/\mathrm{Br}(\mathbb{Q})$.
For $p \neq 2$, the image of $ev_A : X(\mathbb{Z}_p) \to \mathrm{Br}(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$ vanishes.
For $p = 2$, the image of this map coincides with $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$ if and only if
(i) 2 divides m exactly and $n \equiv 5$ (8)
or
(ii) 4 divides m and $n \equiv 3 \text{ or } 5$ (8)
In case (i) and (ii) we thus conclude : $(\prod_p X_{m,n,k}(\mathbb{Z}_p))^{\mathrm{Br}(X_{\mathbb{Q}})} = \emptyset$, hence $X_{m,n,k}(\mathbb{Z}) = \emptyset$.

Using genus theory, F. Xu and R. Schulze-Pillot (2004) proved :

Theorem *In all other case* $X_{m,n,k}(\mathbb{Z}) \neq \emptyset$.

Is this a special case of a general theorem ?

Are there classes of schemes X of finite type over $\mathbb{Z}$ for which

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

holds ?

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 $X_{\mathbb{Q}} \simeq \mathbf{P}^1_{\mathbb{Q}} \setminus \{\infty\}$. Hence $\mathrm{Br}(X_{\mathbb{Q}})/\mathrm{Br}(\mathbb{Q}) = 0$ 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.)

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

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

In a not completely immediate fashion, class field theory yields

Theorem (Harari 2008) *Let X be a separated $\mathbb{Z}$-scheme of finite type. If $X_{\mathbb{Q}}$ becomes isomorphic to $\mathbf{P}^1$ minus two points over an algebraic closure of $\mathbb{Q}$, then*

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

This holds in particular for equations

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

with $a \in \mathbb{Z}$ and $q(x, y)$ an integral binary quadratic form.

Difficulty for application : the quotient $\mathrm{Br}(X_{\mathbb{Q}})/\mathrm{Br}(\mathbb{Q})$ 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 $(\prod_p X(\mathbb{Z}_p))^{\mathrm{Br}(X_{\mathbb{Q}})} \neq \emptyset$.

There are nevertheless partial results in this direction (Wei, Xu) which generalize results such as Gauß's result on $p = x^2 + 27y^2$ (a result which Cox explains from the point of view of class field theory and complex multiplication).

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 $a = q(x_1, \ldots, x_n)$.

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

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

Theorem *Let $q(x_1, \cdots, x_n)$ 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 $q(x_1, \cdots, x_n) = a$. Assume $\prod_p X(\mathbb{Z}_p) \neq \emptyset$.*
(a) If $n \geq 4$, then $X(\mathbb{Z}) \neq \emptyset$.
(b) Assume $n = 3$ and $-a \cdot det(q)$ not a square. Then $\mathrm{Br}(X_{\mathbb{Q}})/\mathrm{Br}(\mathbb{Q}) = \mathbb{Z}/2$. Let $A \in \mathrm{Br}(X_{\mathbb{Q}})$ generate this quotient. Then $X(\mathbb{Z}) \neq \emptyset$ if and only if the map

$$\prod_p X(\mathbb{Z}_p) \to \mathbb{Q}/\mathbb{Z}$$

$$\{M_p\} \mapsto \sum_p \mathrm{ev}_A(M_p)$$

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

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

This yields an alternative proof to the theorem of F. Xu and Schulze-Pillot, thanks to a method which may applied in a mechanical way to any equation $a = q(x, y, z)$ with q indefinite.

The above results on the representation of an integer by an integral quadratic form admit of the following generalization. Let X be a $\mathbb{Z}$-scheme such that $X_{\mathbb{Q}} \simeq G/H$ with G and H connected linear algebraic groups over $\mathbb{Q}$. Under a noncompacity assumption at infinity for the derived group of G, one has the following theorem (2005/2009)

$$(\prod_{p} X(\mathbb{Z}_p))^{\mathrm{Br}(X_{\mathbb{Q}})} \neq \emptyset \Longrightarrow X(\mathbb{Z}) \neq \emptyset.$$

(CT/Xu, Harari, Demarche, Borovoi/Demarche)

And when there is no homogenous space structure ?

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*

$$(\prod_p X_a(\mathbb{Z}_p))^{\mathrm{Br}(X_{a,\mathbb{Q}})} \neq \emptyset.$$

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

To prove such a result, one must compute $\mathrm{Br}(X_{a,\mathbb{Q}})/\mathrm{Br}(\mathbb{Q})$.
Let $X^c_{a,\mathbb{Q}} \subset \mathbf{P}^3_{\mathbb{Q}}$ 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 $X^c_{a,\mathbb{Q}}$.
There is a localisation exact sequence

$$0 \to \mathrm{Br}(X^c_{a,\mathbb{Q}}) \to \mathrm{Br}(X_{a,\mathbb{Q}}) \to H^1(E, \mathbb{Q}/\mathbb{Z}).$$

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

An algebraic argument shows that the image of $\mathrm{Br}(X_{a,\mathbb{Q}}) \to H^1(E, \mathbb{Q}/\mathbb{Z})$ 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 $\mathrm{Br}(X^c_{a,\mathbb{Q}}) = \mathrm{Br}(X_{a,\mathbb{Q}})$.

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

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

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

$$(\prod_p Y_a(\mathbb{Z}_p))^{\mathrm{Br}(X_{a,\mathbb{Q}})} \neq \emptyset.$$

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 $\mathrm{Br}(Y^c_{a,\mathbb{Q}}) \to \mathrm{Br}(Y_{a,\mathbb{Q}})$ is not onto. We have $\mathrm{Br}(Y_{a,\mathbb{Q}})/\mathrm{Br}(\mathbb{Q}) \simeq \mathbb{Z}/3 \oplus \mathbb{Z}/2$.

Hyperbolic curves

$\mathbb{P}^1$ minus three points

Conjecture (Harari and Voloch 2009)
Let X be a $\mathbb{Z}$-scheme such that $X_{\mathbb{Q}}$ is isomorphic to $\mathbf{P}^1$ minus at least three points.
If $\prod_p X(\mathbb{Z}_p))^{\mathrm{Br}(X_{a,\mathbb{Q}})}$ is not empty, then $X(\mathbb{Z}) \neq \emptyset$.

There is a slightly more general version of the conjecture. It is then related to a question of T. Skolem on exponential equations (1937).
Let S be a finite set of prime numbers $p_i, i = 1, \cdots, n$. 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 $\sum_{i=1}^{3} a_i x_i = 0 \ \ mod\ m$ has a solution with all $x_i \in R$.

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

Let $f(x_1, \ldots, x_n)$ et $g(y_1, \ldots, y_m)$ be integral quadratic forms, $1 \leq n < m$ and $m \geq 3$.
One looks for linear forms $l_i(x_1, \ldots, x_n), i = 1, \ldots, m$ such that

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

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 :

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

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

Translation :

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

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

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

Translation :

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

Bonus II : The Iskovskikh counterexample to the Hasse principle for rational points (1971)

This is a geometrically rational surface which has points in all $\mathbb{Q}_p$ and in $\mathbb{R}$ but which has no point in $\mathbb{Q}$.

$$y^2 + z^2 = (3 - x^2)(x^2 - 2)$$

Solution with $x, y, z \in \mathbb{Q}$?

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0,$$

with $u, v, x, y \in \mathbb{Z}, (x, y) = 1$, hence $(3y^2 - x^2, x^2 - 2y^2) = 1$
Modulo 4, the pair $(3y^2 - x^2, x^2 - 2y^2)$ takes one of the following values :

$$(2, -1), (-1, 1), (3, 2)$$

In $\mathbb{R}$ we have $3y^2 - x^2 > 0, \;\; x^2 - 2y^2 > 0.$

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0,$$

Let p be an odd prime. If p^{2n+1} exactly divides either $3y^2 - x^2$ or $x^2 - 2y^2$, then p^{2n+1} divides $u^2 + v^2$ exactly, thus -1 is a square mod. p, thus (first complementary law) $p \equiv 1$ mod. 4.
Thus the pair $(3y^2 - x^2, x^2 - 2y^2)$ takes one the following values modulo 4 :

$$(1, 1), (2, 1), (1, 2)$$

hence none of the previous values

$$(2, -1), (-1, 1), (3, 2)$$

Contradiction, $X(\mathbb{Q}) = \emptyset$.

The Iskovskikh example in the light of the Brauer-Manin obstruction
(CT,Coray, Sansuc 1981)

Let $c \in \mathbb{Z}, c > 0, c$ be odd. The equation

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

defines an open set U_c in a smooth projective surface $X_c/\mathbb{Q}$.
We have $\prod_{p \cup \infty} X_c(\mathbb{Q}_p) \neq \emptyset$.
The Azumaya quaternion algebra $(c - x^2, -1) \in \mathrm{Br}(U_c)$ extends to an $A \in \mathrm{Br}(X_c)$.

For $p \neq 2$, the image of

$$ev_A : X_c(\mathbb{Q}_p) \to \mathrm{Br}(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$$

is zero.
For $p = 2$, this image is $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$ if and only if $c \equiv 3(4)$.
Thus : *If* $c \equiv 3(4)$, *then* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}(X)} = \emptyset$, *hence* $X_c(\mathbb{Q}) = \emptyset$.
The same computation shows : *If* $c \equiv 1(4)$, *then* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset$.

Theorem *If* $c \equiv 1(4)$ *then* $X_c(\mathbb{Q}) \neq \emptyset$.
(special case of a theorem of CT, Coray and Sansuc, 1981)