Rational points on algebraic varieties : a survey

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

Colloquium, Steklov Institute, Moscow

October 6th, 2017

The aim of this talk is to explain the content, background, and status of the following conjecture.

Conjecture on rational points

Let X be a smooth, projective, geometrically **rationally connected** *algebraic variety over a number field k. Then the set $X(k)$ of rational points of X is dense in the Brauer–Manin set $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$ of X.*

CT-Sansuc 1980 in dimension 2; CT in arbitrary dimension, 1999

For simplicity, I shall mainly discuss the question for the case $k = \mathbb{Q}$, the field of rational numbers. Many results, but not all, have been proved over arbitrary number fields.

Let $\mathbb{Z}$ denote the ring of integers, $\mathbb{Q}$ the field of rational numbers.
Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with coefficients in $\mathbb{Z}$.
One would like to decide if the equation

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

has solutions with coordinates in $\mathbb{Z}$ or at least in $\mathbb{Q}$.
If f is homogeneous, one asks for nontrivial solutions, i.e. not all coordinates zero.
There are several variants :
– Prove or disprove existence of solutions
– Produce some explicit, numerical solutions
– Produce all the solutions (e.g. by parametrizations)

It is known (Davis, Putnam, Robinson, and Matiyasevich) that the existence problem over $\mathbb{Z}$ is undecidable. there is no general answer for coordinates in $\mathbb{Z}$. The problem over $\mathbb{Q}$ is open.

One general aim of arithmetic algebraic geometry is to get solutions of these problems for systems of equations whose geometry (when one goes over the complex field) is under control.

What can prevent a diophantine equation from having solutions ?

Let p be a prime number. The homogeneous equation

$$x^3 + py^3 + p^2z^3 = 0$$

has no solution $(x, y, z) \neq (0, 0, 0)$ in $\mathbb{Q}$.

Proof
If there were a solution, one could chose it with $x, y, z \in \mathbb{Z}$ without common factor (this is a "primitive solution"). From the equation we deduce : p divises x^3, thus p divise x, thus p^2 divises py^3, thus p divides y, thus p^3 divides p^2z^3, thus p divides z, contradiction.
This argument shows that there is no primitive solution of $x^3 + py^3 + p^2z^3 = 0$ in the ring $\mathbb{Z}/p^3$.

A necessary condition for a (homogeneous) polynomial equation $f(x_1, \ldots, x_n) = 0$ with integral coefficients to have a (primitive) solution with coordinates in $\mathbb{Z}$ is that all associated congruences have (primitive) solutions, i.e. that there are (primitive) solutions in all quotient rings $\mathbb{Z}/m$. This is equivalent to the same requirement for all rings $\mathbb{Z}/p^r$ for varying prime powers p^r.

Another necessary condition is existence of solutions in the field $\mathbb{R}$ of real numbers. Certainly $x^2 + y^2 + 1 = 0$ has no solution over $\mathbb{Q}$.

One may reformulate the congruence conditions in a manner parallel to the real condition. This goes back to K. Hensel (1897). For each prime p, one construct the ring of p-adic integers $\mathbb{Z}_p = \mathrm{limproj}_r \mathbb{Z}/p^r$. This ring is a discrete valuation ring; it has no zero-divisors. Its field of fraction is the field $\mathbb{Q}_p$ of p-adic numbers, which can also be defined as the completion of $\mathbb{Q}$ with respect to the p-adic valuation. This is a topological field.
Given a (homogeneous) polynomial f with integral coefficients, the following conditions are equivalents ;
– $f = 0$ has (primitive) solutions modulo all prime powers p^r
– $f = 0$ has a (primitive) solution in the ring $\mathbb{Z}_p$ (here primitive means that at least one coordinate is a unit in $\mathbb{Z}_p$). For f homogeneous, this simply means: f has nonzero solutions over $\mathbb{Q}_p$.

Let us write $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.

For $X/\mathbb{Q}$ an algebraic variety over $\mathbb{Q}$, i.e. for a system of polynomial equations

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, m$$

with coefficients in $\mathbb{Q}$ (or $\mathbb{Z}$), and any field F containing $\mathbb{Q}$ one writes $X(F)$ for the set of solutions with coordinates in F of the equation. One calls $X(F)$ the set of F-rational points of X. One sometimes calls $X(\mathbb{Q})$ the set of rational points of X.

For $X/\mathbb{Q}$ an algebraic variety over $\mathbb{Q}$, the set of all congruence conditions and real condition may be reformulated as the diagonal inclusion

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{A}_{\mathbb{Q}}) \subset \prod_{p} X(\mathbb{Q}_p),$$

where $X(\mathbb{A}_{\mathbb{Q}})$ is the set of adèles of X : families $\{M_p\}$ (p finite prime or ∞) with M_p integral point for almost all primes p.
For X a *projective* variety, i.e. for a system given by a finite system of homogeneous equations, and one only considers non-zero solutions, one has $X(\mathbb{A}_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$.

Let $\mathcal{C}$ be a class of algebraic varieties over $\mathbb{Q}$. One says that the local-global principle, or Hasse principle, holds for (rational points of) varieties in that class if for $X/\mathbb{Q}$ in that class,

$$\prod_p X(\mathbb{Q}_p) \neq \emptyset \text{ implies } X(\mathbb{Q}) \neq \emptyset.$$

One says that weak approximation holds for a given variety $X/\mathbb{Q}$ if $X(\mathbb{Q}) \subset \prod_p X(\mathbb{Q}_p)$ is dense in the topological product.

For varieties which are not projective, e.g. for affine varieties, the inclusion

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{A}_{\mathbb{Q}})$$

leads to the study to the study of the Hasse principle for points with integral coordinates, and of "strong approximation". This will not be discussed today.

The classical example (Legendre, Hilbert, Minkowski, Hasse) :

Theorem. *The local-global principle holds for quadrics, i.e. for subvarieties of n-dimensional projective space* $\mathbb{P}^n$, $n \geq 2$, *defined by the vanishing of a nonsingular quadratic form* $q(x_0, \ldots, x_n) = 0$ *with coefficients in* $\mathbb{Q}$.

Coniques $q(x_0, x_1, x_2) = 0$ (Legendre, Paris, An VI (1797-1798); Gauß 1801; Hilbert 1899 over number fields)

If a conic has points in all $\mathbb{Q}_p$, then it has points in $\mathbb{Q}$ (proof by geometry of numbers).

As a matter of fact, it is enough to assume existence of points in all $\mathbb{Q}_p$ but possibly one. This is clear on specific proofs. More generally, to each nonsingular conic $C/\mathbb{Q}$ and to each prime p (including ∞) one associates a "local invariant" in $\mathbb{Z}/2$, which is zero if and only if C has a point over $\mathbb{Q}_p$. The theorem:

The (finite) sum of these invariants vanishes in $\mathbb{Z}/2$

is a generalization of Gauß's law of quadratic reciprocity.

Quadrics (Hasse, 1922-1924)
Let $P(t) = \alpha t + \beta$, $\alpha, \beta \in \mathbb{Z}, \alpha.\beta \neq 0$. Consider the affine equation

$$ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 = P(t) \neq 0$$

with $a, b, c, d \in \mathbb{Z}$ nonzero. Suppose we have solutions

$$ax_{0,p}^2 + bx_{1,p}^2 = cx_{2,p}^2 + dx_{3,p}^2 = P(t_p) \neq 0$$

over each $\mathbb{Q}_p$.
One defines a finite set S of "bad primes" for the equation. It is determined by the coefficients of the system, in particular it contains 2 and the primes dividing one of the a, b, c, d.
Using *Dirichlet's theorem on primes in arithmetic progressions* for the degree one polynomial $P(t)$, one finds $t_0 \in \mathbb{Q}$ with $P(t_0) \neq 0$ such that $P(t_0) \in \mathbb{Q}$ is the product of a unique prime $\ell \notin S$ and of powers of primes in S, has a suitable sign and is very close p-adically to each $P(t_p)$ for $p \in S$.

Then the system

$$ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 = P(t_0)$$

has solutions $\{x_i\}$ in each $\mathbb{Q}_p$ except possibly $\mathbb{Q}_\ell$. By our earlier discussion of conics, each of the two conics $ax_0^2 + bx_1^2 = P(t_0)$ et $cx_2^2 + dx_3^2 = P(t_0)$ then has $\mathbb{Q}$-points. This gives a solution of

$$ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 = P(t) \neq 0$$

over $\mathbb{Q}$.

Diagonalisation of quadratic forms reduces the proof of the Hasse principle for quadrics given by $q(x_0, x_1, x_2, x_3) = 0$ to systems of the previous type.
The local-global principle for $q(x_0, \ldots, x_n) = 0$ and $n \geq 4$ follows from the case $n \leq 3$ and a general "fibration method" which proves the Hasse principle (and weak approximation) for any affine equation

$$\sum_{i=1}^{r} a_i x_i^2 = P(t) \neq 0$$

with all $a_i \in \mathbb{Q}^\times$, $P(t) \in \mathbb{Q}[t]$ nonzero of arbitrary degree, and $r \geq 3$. [This does not hold in general for $r = 2$, as we shall see.]

What about "higher degree" equations ?

A very powerful analytic method, the "circle method", initiated by Hardy and Littlewood, and still very active, in particular in Britain, has led to general theorems on the existence of rational solutions of homogeneous equations

$$f(x_0, \ldots, x_n) = 0$$

of degree d when n is relatively big with respect to d.
Birch (1961) gives one such general theorem. For nonsingular forms, Birch proves the local-global principle under the assumption $n + 1 > (d - 1)2^d$.

For $d = 3$, this implies the existence of rational points on nonsingular cubic hypersurfaces $X \subset \mathbb{P}^n_{\mathbb{Q}}$, for $n > 15$: in this case there always exist solutions over all $\mathbb{Q}_p$.

Still for $d = 3$, subtle refinements involving Deligne's results on the Weil conjectures for varieties over a finite field have led to more precise results :
Let $f(x_0, \ldots, x_n)$ be a cubic form whose associated cubic hypersurface $X \subset \mathbb{P}^n_{\mathbb{Q}}$ is nonsingular.
For $n \geq 9$, $X(\mathbb{Q}) \neq \emptyset$ (Heath-Brown).
For $n = 8$, the Hasse principle holds (Hooley).

For $n \geq 4$, one conjectures that the Hasse principle holds.
It does not for $n = 3$, as we shall see.

Hypothesis (H)

Hypothesis (H) (Bouniakowsky; Dickson; Hardy and Littlewood; Schinzel 1958)

Let $P_i(t), i = 1, \ldots, r$ in $\mathbb{Z}[t]$ be irreducible polynomial with positive leading coefficient, prime to one another, and such that there is no common divisor to all $\prod_{i=1}^{r} P_i(m)$ for m varying in $\mathbb{Z}$. Then there exist infinitely many integers n such that each $P_i(n)$ is a prime number.

Example 1 (only case known) One polynomial of degree 1, $P(t) = at + b$. Dirichlet's theorem on primes in an arithmetic progression.
Example 2. One polynomial $P(t) = t^2 + 1$.
Example 3. Twin prime conjecture. $P_1 = t$, $P_2(t) = t + 2$.

Observation (CT/Sansuc, 1979; further developed 1991-1998, Serre, Swinnerton-Dyer, CT, Skorobogatov)
Hasse's argument to deduce the local-global principle for quadratic forms in 4 variables from the principle in 3 variables relies on Dirichlet's theorem for primes in an arithmetic progression. The same argument yields :

Under Hypothesis (H), the Hasse principle holds for equations

$$y^2 - az^2 = P(t)$$

with $a \in \mathbb{Q}^\times$ *and* $P(t) \in \mathbb{Q}[t]$ **irreducible**.

More generally, *under Hypothesis (H), the Hasse principle holds for equations*

$$Norm_{K_i/\mathbb{Q}}(\Xi_i) = P_i(t), i = 1, \ldots, m$$

with $K_i/\mathbb{Q}$ **cyclic** *field extensions and all* $P_i(t)$ *in* $\mathbb{Q}[t]$ **irreducible** *and coprime to one another.*
Here Ξ_i denotes a "variable in K_i", that is, once a basis of the vector space $K_i/\mathbb{Q}$ is fixed, a linear combination on this basis with coefficients in $\mathbb{Q}$.

Arithmetic combinatorics

Hypothesis (H) is still wide open. But a spectacular two variable version of a special case has been established.

Theorem (Green, Tao, Ziegler, 2010-2012)
Let $L_i(x, y), i = 1, \ldots, r$ be nonproportional linear forms with integral coefficients, and let $c_i \in \mathbb{Z}, i = 1, \ldots, r$. Assume that for each prime p, there exist $(m, n) \in \mathbb{Z}^2$ such that p divides none of the $L_i(m, n) + c_i$. Let $K \subset \mathbb{R}^2$ be an open convex cone in which there lies a point $(m, n) \in \mathbb{Z}^2$ with each $L_i(m, n) > 0$. Then there exist infinitely many pairs $(m, n) \in K \cap \mathbb{Z}^2$ such that each $L_i(m, n) + c_i$ is a prime number.

The above theorem may be used nearly directly as a substitute in the would-be generalization of Hasse's method for quadratic forms (from 3 to 4 variables).

Theorem (Harpaz, Skorobogatov, Wittenberg 2013)
Let $K_i/\mathbb{Q}$, $i = 1, \ldots, r$ be **cyclic** *field extensions of $\mathbb{Q}$ and let $e_i \in \mathbb{Q}$ et $b_i \in \mathbb{Q}^\times$ pour $i = 1, \ldots, r$. Then the Hasse principle holds for systems of equations*

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(\Xi_i) = b_i(u - e_i v) \neq 0.$$

Here $K_i = \oplus_j \mathbb{Q}\omega_{i,j}$ and $\Xi_i = \sum_j x_{i,j}\omega_{i,j}$. The variables are $\{x_{ij}, u, v\}$.

The first series of results combining the results and methods of arithmetic combinatorics had been obtained by Browning, Matthiesen and Skorobogatov (Ann. Math. 2014). Further work has led to :

Theorem (Browning-Matthiesen 2013-2016) *Let $K_i/\mathbb{Q}$, $i = 1, \ldots, r$ be* **arbitrary** *finite field extensions of $\mathbb{Q}$ and let $L_i(u_1, \ldots, u_s)$ with $s \geq 2$ be linear forms with coefficients in $\mathbb{Q}$, nonproportional with one another. Then the Hasse principle holds for the system*

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(\Xi_i) = L_i(u_1, \ldots, u_s) \neq 0.$$

Here $K_i = \oplus_j \mathbb{Q}\omega_{i,j}$ and $\Xi_i = \sum_j x_{i,j}\omega_{i,j}$. The variables are $\{x_{ij}, u_1, \ldots, u_s\}$.
To prove this theorem, the authors go into the machinery of the Hardy-Littlewood nilpotent circle method, as developed by Green, Tao, Zieglier, and use work of Matthiesen.

The Hasse principle does not always hold

Some counterexamples to the Hasse principle

- $Norm_{K/\mathbb{Q}}(\Xi) = c$ and $K/\mathbb{Q}$ *non cyclic*, e.g. $K/\mathbb{Q}$ Galois with group $\mathbb{Z}/2 \times \mathbb{Z}/2$ (Hasse, 1930s).
- $2y^2 = x^4 - 17$, genus one curve (Reichardt, Lind, 1940)
- $3x^3 + 4y^3 + 5z^3 = 0$, genus one curve, (Selmer, 1951)
- $y^2 - az^2 = P(t)$, geometrically rational surface with $P(t)$ **reducible**, e.g.

$$y^2 + z^2 = (3 - x^2)(x^2 - 2) \text{ (Iskovskikh 1970)}$$

- $5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$ (Cassels-Guy, 1966)

The Brauer-Manin obstruction

The Brauer group of a field

Let k be a field, $\mathrm{car}(k) = 0$, and let $\overline{k}$ be an algebraic closure of k. Let $a, b \in k^\times$. The relations

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

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

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

For $k = \mathbf{R}$, $a = b = -1$, this is Hamilton's quaternion algebra.

Quite generally, a finite dimensional k-algebra is algebra is a central simple algebra if there exists $n \geq 1$ such

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

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

Class field theory (Hilbert, Takagi, Hasse, ...)

Local class field theory

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

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

Fundamental exact sequence of global class field theory (Brauer, Hasse, Noether)

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

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

For $k = \mathbb{Q}$, the formula $\sum_p (a, b)_p = 0$ contains as special cases Gauss's laws of quadratic reciprocity.

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

The Brauer group of a scheme

Over an algebraic variety X, and more generally over a scheme X, we have vector bundles: these are the generalisations of vector spaces over a field.

we have Azumaya algebras: these are the generalisations of central simple over a field.

One extends the definition of equivalence of central simple algebras to Azumaya algebras over a scheme X. This gives rise to an abelian group, the (Azumaya) Brauer group $\mathrm{Br}(X)$ of X.

Let X be a scheme and $X(R)$ the set of its points " with coordinates in R ". For any commutative ring R, there is a natural evaluation pairing $X(R) \times \mathrm{Br}(X) \to \mathrm{Br}(R)$.

The Brauer-Manin obstruction for rational points

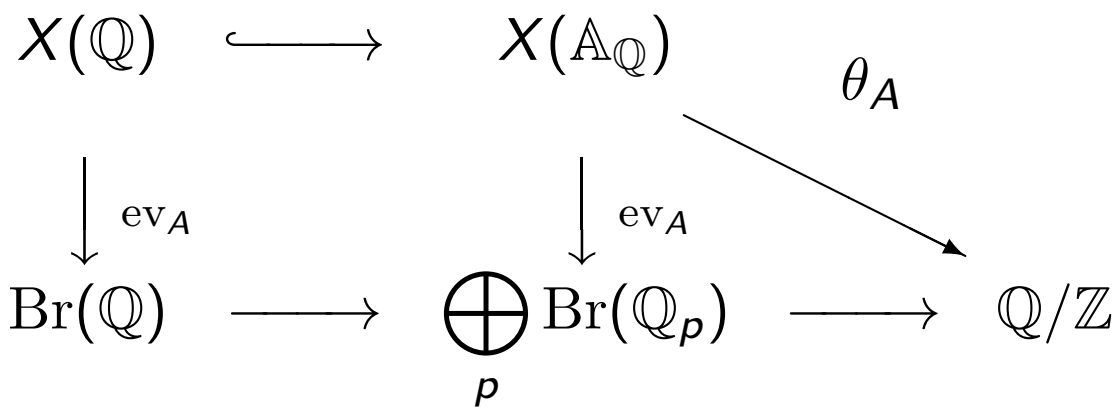
Theorem (Manin, 1970). *Let X be a projective variety over $\mathbb{Q}$. The diagonal image of $X(\mathbb{Q})$ in $X(A_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$ lies in the left kernel of the (well defined) pairing*

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

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

This kernel $X(A_{\mathbb{Q}})^{\mathrm{Br}}$ is the Brauer–Manin set of X. It only depends on the quotient $\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q})$. This group is in general not easy to compute. It may be infinite. A (useless) compacity argument shows that if $X(A_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$ then this can be detected using finitely many elements in $\mathrm{Br}(X)$.

The Brauer-Manin set $X(A_{\mathbb{Q}})^{\mathrm{Br}} \subset X(A_{\mathbb{Q}})$ is the intersection of the kernels of all (set-theoretic) maps θ_A for A runnning through $\mathrm{Br}(X)$:



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

The Reichardt and Lind example

The equation

$$2y^2 = x^4 - 17 \neq 0$$

defines an open set U of a smooth projective curve $X/\mathbb{Q}$.
One easily checks $\prod_{p \cup \infty} X(\mathbb{Q}_p) \neq \emptyset$.
Fact : The Azumaya algebra $(y, 17) \in \mathrm{Br}(U)$ extends to an Azumaya algebra $A \in \mathrm{Br}(X)$.
For each $p \neq 17$ the map $ev_A : X(\mathbb{Q}_p) \to \mathrm{Br}(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$ vanishes.
For $p = 17$ the map $ev_A : X(\mathbb{Q}_{17}) \to \mathrm{Br}(\mathbb{Q}_{17}) \subset \mathbb{Q}/\mathbb{Z}$ has $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$ for its image.
Hence $X(\mathbb{Q}) = \emptyset$.

Generalized Iskovskikh example

Let $c \in \mathbb{Z}, c > 0, c$ 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 $X_c/\mathbb{Q}$.
One easily checks $\prod_{p \cup \infty} X_c(\mathbb{Q}_p) \neq \emptyset$.
Fact : The Azumaya algebra $(c - x^2, -1) \in \mathrm{Br}(U_c)$ extends to $A \in \mathrm{Br}(X_c)$.

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

For each $p \neq 2$, the map

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

vanishes.
For $p = 2$, the image of that map is reduced to $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$ if and only if $c \equiv 3(4)$.
Thus : *If* $c \equiv 3(4)$, *then* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$, *hence* $X_c(\mathbb{Q}) = \emptyset$.

The same computation shows : *Si* $c \equiv 1(4)$, *then* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$.
Theorem (special case of CT, Coray, Sansuc, 1981) *Si* $c \equiv 1(4)$ *then* $X_c(\mathbb{Q}) \neq \emptyset$.

Is the Brauer–Manin obstruction ($X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$) the ultimate obstruction to the Hasse principle ?

For arbitrary smooth projective varieties, no. But it took some time to produce examples.

• Skorobogatov 1999. Bielliptic surface with $X(\mathbb{Q}) = \emptyset$ and $X(\mathbb{A}_Q)^{\mathrm{Br}} \neq \emptyset$. New condition

$$X(\mathbb{Q}) \subset X(\mathbb{A}_{\mathbb{Q}})^{\text{ét},\mathrm{Br}} \subset X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset X(\mathbb{A}_{\mathbb{Q}})$$

• Harari–Skorobogatov, other obstruction : noncommutative descent.

• Poonen 2010. Threefolds with $X(\mathbb{Q}) = \emptyset$ and $X(\mathbb{A}_{\mathbb{Q}})^{\text{ét},\mathrm{Br}} \neq \emptyset$. Albanese variety nontrivial.

• Comparison between étale-Brauer obstruction, descent obstruction, and iterated versions of these obstructions : Harari, Skorobogatov, Demarche, Xu, final result : Yang Cao 2017.

There are further examples.

• Some surfaces of general type (Harpaz and Skorobogatov 2012); Nontrivial Albanese variety.

• CT-Pál-Skorobogatov 2016. Surfaces X with a conic bundle fibration over a curve, with $X(\mathbb{Q}) = \emptyset$ and $X(\mathbb{A}_{\mathbb{Q}})^{\text{ét,Br}} \neq \emptyset$. Nontrivial Albanese variety.

• Smeets 2016. Varieties with $X(\mathbb{Q}) = \emptyset$ and $X(\mathbb{A}_{\mathbb{Q}})^{\text{ét,Br}} \neq \emptyset$ and trivial Albanese variety. Under ABC conjecture, surfaces with trivial geometric fundamental group.

In the examples on this slide it seems difficult to formally define the obstruction.

Varieties for which we wonder whether the Brauer-Manin obstruction is the only obstruction to the Hasse principle

- Curves and homogeneous spaces of abelian varieties
- Higher dimensional analogues of curves of genus zero : rationally connected varieties
- $K3$-surfaces

Smooth projective curves

$g = 0$, these are conics, the Hasse principle holds.

For $g \geq 1$, let $J = J(X)$ be the jacobian of X. Then $\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q}) = H^1(\mathbb{Q}, J)$ is infinite.

For $g = 1$, under the hypothesis that the Tate-Shafarevich group $Ш^1(\mathbb{Q}, J(X))$ is finite, Manin shows (1970)

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

Plus précisément, one then has $X = J(X)$ and

$$\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}_{\bullet}$$

where $\bullet$ means one contracts the connected components.
The same conditional result holds more generally for X a principal homogeneous space of an abelian variety.

For any smooth projective curve X of genus $g > 1$, one later went on to conjecture:

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

This has a down-to-earth translation ("Mordell-Weil sieve", Poonen) which has been tested numerically (Bruin and Stoll).

Skorobogatov and Scharaschkin proved that the conjecture holds for X a curve whose Jacobian J satisfies : $J(\mathbb{Q})$ if finite and $Ш^1(J)$ is finite.

Stoll used results of Serre to prove that certain slightly different looking obstructions are Brauer–Manin.

There is a connexion with Grothendieck's section conjecture (Stix, Wittenberg) : If the local version of Grothendieck's section conjecture holds for smooth projective curves over p-adic fields, and if the Brauer-Manin obstruction is the only obstruction, then Grothendieck's global section conjecture holds.

Function fields in one variable over a finite field such as $\mathbb{F}_p(t)$ have long been known to be analogues of the field $\mathbb{Q}$ and its extensions. For most curves of genus at least 2 over such a field as $\mathbb{F}_p(t)$, Poonen and Voloch (2008) proved the conjecture.

Rationally connected varieties

Over the complex field, rationally connected varieties appeared at the end of the 80s in the Mori classification programme of higher dimensional varieties as the good higher dimensional analogue of rational surfaces.
A smooth, projective variety X over the complex field is rationally connected if it satisfies : two general points A and B of $X(\mathbb{C})$ may be connected by a chain of rational curves lying on X.
A smooth, projective variety X over $\mathbb{Q}$ is called (geometrically) rationally connected if viewed over $\mathbb{C}$ it is rationally connected.

Examples of rationally connected varieties
Smooth projective models of :
– (geometrically) rational varieties (e.g. connected linear algebraic groups)
– for example, varieties given by a system of equations

$$Norm_{K_i/\mathbb{Q}}(\Xi_i) = P_i(t), i = 1, \ldots, m$$

as considered above.
– Unirational varieties (e.g. homogeneous spaces of connected linear algebraic groups)
– Fano hypersurfaces, i.e. smooth projective hypersurfaces $X \subset \mathbb{P}^n$ of degree d with $n \geq d$ (Campana, Kollár-Miyaoka-Mori)

A celebrated theorem of Graber, Harris and Starr asserts : if $X \to Y$ is a dominant map with basis rationally connected and general fibres rationally connected, then X is rationally connected.

On the basis of some theoretical and numerical evidence, the following very general conjecture was made (CT-Sansuc 1980 in dimension 2; CT in arbitrary dimension, 1999).

Conjecture : *Let X be a smooth, projective, geometrically* **rationally connected** *algebraic variety over a number field k. Then the set $X(k)$ of rational points of X is dense in the Brauer–Manin set $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$ of X.*

[That conjecture implies that for such an X, if X has at least one rational point, then the rational points are Zariski dense on X. This is very much an open question.]

The conjecture is known for :

• Compactifications of homogeneous spaces of connected linear algebraic groups with connected stabilizers (Sansuc 1981; Borovoi 1996)

• Conic bundles over $\mathbb{P}^1$ with 4 geometric singular fibres, e.g. $y^2 - az^2 = P(x)$ with $P(x)$ of degree 4 (CT, Sansuc, Swinnerton-Dyer 1987)

• Conic bundles over $\mathbb{P}^1$ with 5 geometric singular fibres, (Salberger, Skorobogatov)

• Smooth intersection of two quadrics in $\mathbb{P}^n$, $n \geq 7$ ($n \geq 8$ CT, Sansuc, Swinnerton-Dyer 1985-1987; $n = 7$ Heath-Brown)

• Under Schinzel's Hypothesis (H), any conic bundle over $\mathbb{P}^1$

Tools

• For X rationally connected, the group $\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q})$ is more or less under control. It is finite.
• Various duality theorems in class field theory (Tate-Nakayama) extending the fundamental sequence of Brauer-Hasse-Noether
• The *fibration method*
• The *descent method*
• (conditional) Use of Schinzel's Hypothesis (H)
• (unconditional) Use of arithmetic combinatorics (Green, Tao, Ziegler)
• (conditional) use of finiteness of $Ш$

• The *fibration method* Give conditions on maps of $\mathbb{Q}$-varieties $f : X \to Y$ such that if the conjecture holds for Y (e.g. Y is projective space) and for most fibres of f, then it holds for X. One thus reduces the conjecture for X to the conjecture for smaller dimension varieties.

This generalizes Hasse's method. CT-Sansuc-Swinnerton-Dyer 1987. Developed by Skorobogatov and by Harari (1994, 1997). There is more hope to make the method work when the fibres of f are rationally connected varieties.

• But one may also try to use fibrations into e.g. curves of genus one, and take for granted the finiteness of the Tate-Shafarevich group. This line of investigation was started by Swinnerton-Dyer (see below).

• The *descent method* (universal torsors, torsors under algebraic tori, CT-Sansuc 1977-1987).

This is an analogue of the usual descent for rational points on curves of genus one. Here one considers $f : Y \to X$ where the general fibre is a principal homogeneous space under a suitable torus and one tries to deduce the conjecture for X from the conjecture for the (higher dimensional) variety Y, supposedly simpler to handle if one made the right choice of map f, which ensures for instance that the relevant Brauer group of Y is trivial, hence creates no obstruction to the Hasse principle for Y. The condition $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$ ensures that there exists such an $f : Y \to X$ with $Y(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$. In very favourable cases, the Y one gets actually satisfy the Hasse principle.

Descent method, a simple case

Let X be a smooth projective surface over $\mathbb{Q}$ "defined" by an equation

$$y^2 - az^2 = \prod_{i=1}^{n} P_i(t) \neq 0$$

with all $P_i(t)$ all polynomials $P_i(t)$ irreducible and coprime in pairs. Using either **descent** (torsors under tori) or an easy special case of Harari's **formal lemma** (use of Brauer group of open varieties), one shows that the (necessary, cf. Iskovkikh's counterexample) condition $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$ *implies that there exist elements* $\alpha_i \in \mathbb{Q}^{\times}$ *with* $\prod_i \alpha_i = 1$ *such that the variety* Y *defined by the system*

$$y_i^2 - az_i^2 = \alpha_i P_i(t) \neq 0, \quad i = 1, \ldots, n$$

has solutions in all $\mathbb{Q}_p$.

Under Schinzel's Hypothesis (H), a system

$$y_i^2 - az_i^2 = \alpha_i P_i(t) \neq 0$$

with all $P_i(t)$ irreducible satisfies the Hasse principle.
Under multiplication, which is a map $Y \to X$, a solution of this sytem over $\mathbb{Q}$ gives a solution over $\mathbb{Q}$ of the original equation

$$y^2 - az^2 = \prod_{i=1}^{n} P_i(t) \neq 0.$$

The argument actually shows that under Hypothesis (H), one has $\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. This implies in particular that $X(\mathbb{Q})$ is Zariski dense in X as soon as $X(\mathbb{Q})$ is not empty.

Getting unconditional results

Let us consider the special case where all $P_i(t)$ are of degree 1. The smooth, projective variety X contains the open U defined by

$$y^2 - az^2 = c\prod_{i=1}^{n}(t - e_i) \neq 0$$

with $c \in \mathbb{Q}^\times$ and all $e_i \in \mathbb{Q}$ distinct.

Let us take $\{M_p\}$ in $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ which lies in U, and let S be a finite set of primes p. The analogous argument produces elements $\alpha_i \in \mathbb{Q}^\times$ whose product is c such that the variety V given by the system

$$y_i^2 - az_i^2 = \alpha_i(t - e_i) \neq 0, \quad i = 1, \ldots, n$$

which maps to U under multiplication, has solutions $\{N_p\}$ in all $\mathbb{Q}_p$, with the property that N_p maps to M_p for each $p \in S$.

If one sets $t = u/v$ and adds the equation $v = y_{n+1}^2 - az_{n+1}^2$, one finds that V is an algebraic retract of the variety W sur $\mathbb{Q}$ defined by the system

$$y_i^2 - az_i^2 = \alpha_i(u - e_i v), i = 1, \ldots, n$$

$$y_{n+1}^2 - az_{n+1}^2 = v.$$

As explained earlier in this talk, and as noticed by Browning, Matthiesen, Skorobogatov and by Harpaz, Skorobogatov, Wittenberg, the results of Green, Tao et Ziegler imply the Hasse principle and weak approximation for such a system. One thus gets the unconditional result:

$$\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}.$$

In particular rational points are Zariski dense on the surface $y^2 - az^2 = c\prod_{i=1}^{n}(t - e_i)$. For $n > 7$, this was a long-standing open problem (unirationality over $\mathbb{Q}$ is unknown).

Green-Tao-Ziegler and a reciprocity argument in the Hasse style also give

Theorem (Harpaz, Skorobogatov, Wittenberg 2013)
Let $K_i/\mathbb{Q}$, $i = 1, \dots, r$ be cyclic extensions of $\mathbb{Q}$ and let $e_i \in \mathbb{Q}$ et $b_i \in \mathbb{Q}^\times$ for $i = 1, \dots, r$. Then the Hasse principle and weak approximation hold for the system

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(\Xi_i) = b_i(t - e_i) \neq 0.$$

Fibrations into rationally connected varieties

Here is the ideal theorem one would like to obtain

(Would-be theorem) *Let X be a smooth, projective $\mathbb{Q}$-variety equipped with a morphism $p : X \to \mathbb{P}^1_{\mathbb{Q}}$ whose generic fibre is geometrically rationally connected. Assume that for smooth fibres $X_M = p^{-1}(M)$ above a $\mathbb{Q}$-rational point M the closure of $X_M(\mathbb{Q})$ in $X_M(\mathbb{A}_{\mathbb{Q}})$ is the Brauer-Manin set $X_M(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. Then the same holds for X, namely $\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.*

Here are two cases where this has been proved.

• (Harari 1994) The case where all fibres of $p : X \to \mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{A}^1 \subset \mathbb{P}^1$ are geometrically integral.

To prove this Harari developed a "formal lemma", which involves ramified elements of the Brauer group, i.e. elements of the Brauer group of open subsets of X which are not in $\mathrm{Br}(X)$.

• Under the combination of the following hypotheses :
(a) Hypothesis (H)
(b) (abelian splitting) For each closed point $M \in \mathbb{P}^1_{\mathbb{Q}}$, the fibre $X_M/\mathbb{Q}(M)$ contains a multiplicity one component which is split over an **abelian** extension of the residual field $\mathbb{Q}(M)$,
(c) Hasse principle and weak approximation hold for the smooth fibres of p.
(CT-Skorobogatov-Swinnerton-Dyer 1998, extending earlier results of CT-Sansuc 1979, Serre, Swinnerton-Dyer).

The abelian splitting condition is imposed by the ultimate use of Hasse's reciprocity trick.

Example : (b) and (c) hold for conic bundles over $\mathbb{P}^1_{\mathbb{Q}}$

One would like to combine the two approaches to handle the case $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ with generic fibre birational to a homogeneous space of a connected linear algebraic group.

Results in this direction were obtained by Browning, Heath-Brown, Dasheng Wei, Yongqi Liang, A. Smeets, U. Derenthal. Some of these works use the circle method.

The following theorem uses developments of the Green-Tao-Ziegler results (2010-2012) due to L. Matthiesen (2012-2013), and further analytic work, together with descent.

Theorem (Browning and Matthiesen 2016).

Let $K/\mathbb{Q}$ be an **arbitrary** finite field extension of $\mathbb{Q}$. Let $\omega_i \in K, i = 1, \ldots, d$ be a basis of the vector space K over $\mathbb{Q}$. Let $P(t) = c\prod_{i=1}^{n}(t - e_i)$ be a split polynomial (all roots in $\mathbb{Q}$). Let X be a smooth projective model of the affine variety with equation

$$\mathrm{Norm}_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_d\omega_d) = P(t).$$

Then the closure of $X(\mathbb{Q})$ in $X(\mathbb{A}_{\mathbb{Q}})$ is $X(\mathbb{A}_Q)^{\mathrm{Br}}$.

In the case where the only nonsmooth fibres of $p : X \to \mathbb{P}^1_{\mathbb{Q}}$ lie over $\mathbb{Q}$-rational points, Harpaz and Wittenberg (Ann. Math. 2016) have unconditionally established the would-be theorem.
They get rid of the abelian-split hypothesis on the singular fibres of $X \to \mathbb{P}^1$, by modelling components of the bad fibres on torsors under tori, somehow reducing to a situation like the one in the theorem of Browning and Matthiesen above, and using results of Matthiesen.
They combine this with Tate-Nakayama duality for tori, which gives a twisted, generalized version of the fundamental exact sequence for the Brauer group of a number field, and with a torsor version of Harari's formal lemma.

Fibrations into curves of genus one, and some $K3$-surfaces

In 1995, Swinnerton-Dyer initiated a new method, further developed by CT, Skorobogatov and him (1998), then by Wittenberg (2006), by Harpaz and Skorobogatov (2016), by Harpaz (2017). This method is conditional on the finiteness of Tate-Shafarevich groups of elliptic curves and often also on Hypothesis (H).

Typically, one has a fibration $X \to \mathbb{P}^1_{\mathbb{Q}}$ into curves of genus 1. One tries to find a rational point $M \in \mathbb{P}^1(\mathbb{Q})$ such that simultaneously :

(a) the fibre X_M has points in all completions of $\mathbb{Q}$, hence is an element of the Tate-Shafarevich group of its Jacobian J_M.

(b) The (supposedly finite) Tate-Shafarevich group is so small that the symplectic pairing on that group implies that the group must be zero.

This then implies that X_M contains a rational point.

Here is one application, which does not require Hypothesis (H) because the special case it uses is Dirichlet's theorem on primes in an arithmetic progression.

Theorem (Swinnerton-Dyer, 2001) Assuming finiteness of Tate-Shafarevich groups of elliptic curves over number fields, the Hasse principle holds for diagonal cubic hypersurfaces over $\mathbb{Q}$:

$$\sum_{i=0}^{n} a_i x_i^3 = 0, \quad n \geq 4.$$

This an easy consequence of the main result, which is a Hasse principle for diagonal cubic surfaces

$$ax^3 + by^3 + cz^3 + dt^3 = 0$$

under specific restrictions on the prime factors of the coefficients a, b, c, d.

The method leads to conditional result for some families of $K3$ surfaces (CT, Skorobogatov, Swinnerton-Dyer 1998; Swinnerton-Dyer 2000; Skorobogatov, Swinnerton-Dyer 2005). For instance one gets (conditional) results on diagonal quartics

$$ax^4 + by^4 + cz^4 + dt^4 = 0$$

when $abcd$ is a square in $\mathbb{Q}$. Two recent papers (Harpaz and Skorobogatov 2016, Harpaz 2017) handle some Kummer surfaces associated to a product of two elliptic curves – without using Hypothesis (H). The action of Galois on the torsion points of elliptic curves plays a big rôle here.

For $K3$ surfaces, Skorobogatov has conjectured that the Brauer-Manin obstruction to the Hasse principle is the only one. Work to test this hypothesis has been done.

By reduction to a study of the Brauer-Manin obstruction for intersection of two quadrics in $\mathbb{P}^4$ (also known as del Pezzo surfaces of degree 4) and use of Swinnerton-Dyer's technique, one has :

Theorem (Wittenberg 2007). Assuming both finiteness of Tate-Shafarevich groups and Hypothesis (H), the Hasse principle for rational points holds for smooth complete interesections of two quadrics in $\mathbb{P}^n_{\mathbb{Q}}$ for $n \geq 5$.

The result is unconditionally known only for $n \geq 7$ (CT-Sk-SwD 1987; Heath-Brown 2013).

Zero-cycles : a very general conjecture

Definition : The index $I(X)$ of an algebraic variety X over a field k is the greatest common divisor of the degrees $[K : k]$ of finite field extensions K/k such that $X(K) \neq \emptyset$, i.e. X acquires a rational point over K.

Conjecture on zero-cycles

Let X be any smooth, projective, geometrically connected algebraic variety over a number field k. If the Brauer–Manin set $X(\mathbb{A}_k)^{\mathrm{Br}}$ of X is not empty, then the index $I(X)$ of X is equal to one.

Special case of a more elaborate conjecture on Chow groups of zero-cycles : In essence, Cassels and Tate for curves; CT-Sansuc 1981 for geometrically rational surfaces; Kato-Saito 1986 ; S. Saito 1989 ; CT 1995. Reformulation, van Hamel 2003, Wittenberg 2012.

Theorem (Harpaz and Wittenberg 2016) *Let X be a smooth, projective variety over a number field k, equipped with a morphism $p : X \to \mathbb{P}^1_k$ whose generic fibre is rationally connected. Assume that for closed points $M \in \mathbb{P}^1_k$ with smooth fibre $X_M = p^{-1}(M)$, the conjecture on rational points of X_M (over the number field $k(M)$) holds. If $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ then the index of X is one.*

The conclusion holds more generally if there exists a family $z_v \in Z_0^1(X_{k_v})$ of zero-cycles of degree one such that for all $A \in \mathrm{Br}X$ one $\sum_v A(z_v) = 0 \in \mathbb{Q}/\mathbb{Z}$.
H & W actually prove the whole induction theorem ; "if the statement holds for the fibres (assumed to be rationally connected) then it holds for the total space" for the elaborate conjecture on the Chow group of zero-cycles.

Earlier cases :

Basic paper of Salberger for arbitrary conic bundles over $\mathbb{P}^1$, 1987. Lifted the conjecture off the ground. Introduces an easy but powerful unconditional index-version of Hypothesis (H).

Extensions of his work, using the abelian-split assumption on the bad fibres (CT, Swinnerton-Dyer, Skorobogatov 1994, 1998). Wittenberg 2012.

Wittenberg 2012, Yongqi Liang.

First special cases without the abelian-split assumption : Dasheng Wei.

A recent, thorough survey on the themes of this lecture :

O. Wittenberg, Rational points and zero-cycles on rationally connected varieties over number fields, to appear in Proceedings of AMS Summer Institute in Algebraic Geometry, Salt Lake City. (available on Wittenberg's homepage).