Reciprocity laws and integral solutions of polynomial equations

Jean-Louis Colliot-Thélène
CNRS, Université Paris-Sud
Clay Mathematical Institute, MSRI

Congruences, local fields

Let $f(x_1, \cdots, x_n)$ be a polynomial with integral coefficients.
The question whether there exist integral solutions to the equation

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

is of common interest.

Sometimes one can easily decide that there is no solution.
The equation $x^2 + y^2 + 1 = 0$ cannot be solved in the real field $\mathbf{R}$, hence not in $\mathbf{Z}$.
Congruences can also help decide that there are no solutions.
Using congruences modulo 9 one sees that the equation $x^2 + y^2 - 3z^2 = 0$ has no nontrivial solution. One can also see this by using congruences modulo 4.
Let p be a prime number. Using congruences modulo p^3 one shows that the equation

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

has no nontrivial solution.

Local fields were defined by Kurt Hensel. Given any prime p one defines an integral domain $\mathbf{Z}_p$. Its quotient field $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to the p-adic metric defined by

$$|p^n \cdot a/b|_p = 1/p^n$$

($a, b \in \mathbf{Z}$, a and b prime to p.)
An equation $f(x_1, \cdots, x_n) = 0$ with integral coefficients has a (primitive) solution in $\mathbf{Z}_p$ if and only if it has a (primitive) solution modulo an arbitrary power of p.

Let $X(R)$ denote the set of solutions of the equation $f(x_1, \cdots, x_n) = 0$ with coordinates in the commutative ring R.
There are natural embeddings

$$X(\mathbf{Z}) \subset \prod_p X(\mathbf{Z}_p)$$

$$X(\mathbf{Q}) \subset \prod_p X(\mathbf{Q}_p)$$

Here p is either a prime or $p = \infty$, in this last case we set $\mathbf{Z}_\infty = \mathbf{Q}_\infty = \mathbf{R}$.
There exists a more precise embedding

$$X(\mathbf{Q}) \subset X(A_\mathbf{Q}),$$

where $X(A_\mathbf{Q}) \subset \prod_p X(\mathbf{Q}_p)$ is the set of adèles of X.

Legendre's theorem

Theorem (Legendre, 1785) *Let $q(x, y, z)$ be an integral quadratic form. If the equation $q(x, y, z) = 0$ has nontrivial solutions in all $\mathbf{Z}_p$, including $\mathbf{R}$, then it has a nontrivial solution in $\mathbf{Z}$.*
The proof belongs to the geometry of numbers. It yields an upper bound for the size of the smallest solution.
The usual proofs do not use the full assumption : one may for instance omit the assumption $X(\mathbf{R}) \neq \emptyset$. In particular that condition is imposed by the assumption $X(\mathbf{Z}_p) \neq \emptyset$ for p finite.

The law of quadratic reciprocity (theorema fundamentale)

Let $p \neq 2$ be an odd prime, $a \in \mathbf{Z}$ prime to p,
We have the Legendre symbol $(a/p) = \pm 1$
$(a/p) = 1$ if and only if a is a square mod. p.

Let p, q be odd primes. Then

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

This was conjectured independently by Euler and Legendre (1785).
The first of many proofs was found by Gauß on April 18,1796.

Let p be an odd prime.
First complementary law

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

Thus : -1 is a square modulo p if and only if $p \equiv 1(4)$.

Second complementary law

$$(2/p) = (-1)^{(p^2-1)/8}$$

Thus : 2 is a square modulo p if and only if $p \equiv \pm 1(8)$.

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 the equation*

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

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

The main point in Hasse's proof occurs in the passage from 3 variables (Legendre) to 4 variables. At this point Hasse uses Dirichlet's theorem on primes in an arithmetic progression.

Main question : **Is there such a local-global theorem, or at least some substitute, for other families of equations ?**

There is a method, the circle method (Hardy, Littlewood) which gives such results.
In its present state, it gives results for homogeneous forms when the number of variables is quite big with respect to the degree.
A very good result in this direction is the following theorem of Hooley, which improves upon a breakthrough of Heath-Brown in the 10 variables case :
Satz *The Hasse principle holds for nonsingular cubic forms in at least 9 variables over* $\mathbf{Q}$.
This should be compared with the well-known open problem : does the same hold from 5 variables upwards ?

There are many examples which show that the “Hasse principle” does not generally hold. Let us describe a few.

The Lind example (1940)
This is a curve of genus 1 over $\mathbf{Q}$ with points in all $\mathbf{Q}_p$ and $\mathbf{R}$, but with no point in $\mathbf{Q}$.

$$2y^2 = x^4 - 17, \quad x, y \in \mathbf{Q}$$

$$2u^2 = v^4 - 17w^4 \neq 0, \quad u, v, w \in \mathbf{Z}, \quad (v, w) = 1$$

Reducing modulo 17^2, one sees that u is not divisible by 17. Since 2 is not a fourth power modulo 17, this implies : *u is not a square modulo 17*.
If p is an odd prime which divides u (thus $p \neq 17$), then 17 is a square modulo p, hence (quadratic reciprocity) p is a square modulo 17. Since 2 also is a square modulo 17, we conclude : *u is a square modulo 17*.
Contradiction, $X(\mathbf{Q}) = \emptyset$.

The Iskovskikh example (1971)

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

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

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

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

with $u, v, x, y \in \mathbf{Z}, (x, y) = 1$, 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 $\mathbf{R}$ 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, $X(\mathbf{Q}) = \emptyset$.

An integral example of Borovoi and Rudnick (1995)
Consider the equation over $\mathbf{Z}$:

$$q(x, y, z) = -9x^2 + 2xy + 7y^2 + 2z^2 = 1$$

that is

$$(x - y)^2 + 8(x - y)(x + y) = 2z^2 - 1$$

Solution in $\mathbf{Q}$

$$(x, y, z) = (-1/2, 1/2, 1)$$

thus solutions in all $\mathbf{Z}_p$ for $p \neq 2$.

Solution in $\mathbf{Z}_2$, from $q(4, 1, 1) = -127 \equiv 1(8)$.

$$(x-y)^2 + 8(x-y)(x+y) = 2z^2 - 1$$

Solution with $(x, y, z) \in \mathbf{Z}$?

If one studies the equation modulo powers of 2, one gets

$$x - y \equiv \pm 3 \,(8)$$

Let p be a prime.
If p divides $x - y$, then p divides $2z^2 - 1$.
Thus p is odd and 2 is a square mod. p
(second complementary law) $\Longrightarrow p \equiv \pm\, 1(8)$.
Thus $x - y \equiv \pm 1 \,(8)$.
Contradiction, $X(\mathbf{Z}) = \emptyset$.

The Brauer group of a field

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

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

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

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

For $k = \mathbf{R}$, $a = b = -1$, this is nothing else that Hamilton's quaternions.

Quite generally, a k-algebra is called a central simple algebra 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 algebra.
One decrees that two such k-algebras are equivalent if there exist integers $r, s \geq 1$ such that $M_r(A) \simeq M_s(B)$. The tensor product then defines a commutative group structure on the set of equivalence classes of such algebras. This is the Brauer group of k. It will be denoted $\mathrm{Br}(k)$.

Class field theory

Local class field theory

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

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

The fundamental exact sequence of class field theory

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

A conic $x^2 - ay^2 - bt^2 = 0$ over a field k (char.$(k) \neq 2$) has a rational point (coordinates in k) if and only if the class of the quaternion algebra $(a, b)_k \in \mathrm{Br}(k)$ is zero.
The summation formula $\sum_p (a, b)_p = 0$ subsumes the reciprocity law and its two complements.
Legendre's theorem can thus be reformulated : If for each prime p (finite or infinite) $(a, b)_p \in \mathbf{Z}/2 \subset \mathrm{Br}(\mathbf{Q}_p)$ vanishes, then $(a, b) = 0 \in \mathrm{Br}(\mathbf{Q})$.
From $\sum_p (a, b)_p = 0$ we see that the vanishing of $(a, b)_p$ for all but one p (finite or infinite) is enough to ensure $(a, b) = 0 \in \mathrm{Br}(\mathbf{Q})$.

The Brauer group of a scheme

On an algebraic variety, or more generally over a scheme X, vector bundles are the natural analogues of vector spaces over a field. Azumaya algebras over a scheme are the natural analogues of central simple algebras over a field.

Between Azumaya algebras one can introduce an equivalence relation which extends the one defined for central simple algebras over a field. The set of equivalence classes is an abelian group, the Brauer group $\mathrm{Br}(\mathrm{X})$ of X.

Let X be a $\mathbf{Z}$-scheme. For any commutative 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 $\mathbf{Q}$. The image of $X(\mathbf{Q})$ in $X(A_{\mathbf{Q}}) = \prod_p X(\mathbf{Q}_p)$ is in the left kernel of the (well-defined) pairing*

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

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

This kernel is denoted $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.

Integral variant :

Theorem *Let X be a $\mathbf{Z}$-scheme of finite type. The image of $X(\mathbf{Z})$ in $\prod_p X(\mathbf{Z}_p)$ is in the left kernel of the (well defined) pairing*

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

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

This kernel is denoted $(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})}$.
Note that we pair with $\mathrm{Br}(X_{\mathbf{Q}})$. The more natural pairing with $\mathrm{Br}(X)$ would give less information.

The Lind example in the light of the Brauer-Manin obstruction

The equation

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

defines an open set U of a smooth projective curve $X/\mathbf{Q}$.
We have $\prod_{p\cup\infty} X(\mathbf{Q}_p) \neq \emptyset$.
Fact : The Azumaya algebra $(y, 17) \in \mathrm{Br}(U)$ extends to an Azumaya algebra $A \in \mathrm{Br}(X)$.
For $p \neq 17$ the image of $ev_A : X(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$ is zero if $p \neq 17$.
For $p = 17$ the image of $ev_A : X(\mathbf{Q}_{17}) \to \mathrm{Br}(\mathbf{Q}_{17}) \subset \mathbf{Q}/\mathbf{Z}$ is $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$.
Thus $X(\mathbf{Q}) = \emptyset$.

The Iskovskikh example in the light of the Brauer-Manin obstruction

Let $c \in \mathbf{Z}, c > 0, c$ 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 $X_c/\mathbf{Q}$.
We have $\prod_{p \cup \infty} X_c(\mathbf{Q}_p) \neq \emptyset$.
The Azumaya algebra $(c - x^2, -1) \in \mathrm{Br}(U_c)$ extends to an $A \in \mathrm{Br}(X_c)$.

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

For $p \neq 2$, the image of

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

is zero.
For $p = 2$, this image is $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ if and only if $c \equiv 3(4)$.
Thus : *If* $c \equiv 3(4)$, *then* $X_c(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$, *hence* $X_c(\mathbf{Q}) = \emptyset$.
The same computation shows : *If* $c \equiv 1(4)$, *then* $X_c(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$.
Theorem *If* $c \equiv 1(4)$ *then* $X_c(\mathbf{Q}) \neq \emptyset$.
(special case of a theorem of CT, Coray and Sansuc, 1981)

The integral version of the Brauer-Manin condition : a family of examples

Let n, m, k be positive integers, $(n, m) = 1$. The equation

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

can be rewritten as

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

F. Xu und R. Schulze-Pillot studied the integral solutions of this equation. Let $X/\mathbf{Z}$ be the scheme which this equation defines. One checks $\prod_{p\cup\infty} X(\mathbf{Z}_p) \neq \emptyset$. Let $U_{\mathbf{Q}} \subset X_{\mathbf{Q}}$ be the open set defined by $1 + n^k y \neq 0$. Fact : The Azumaya algebra $(1 + n^k y, n) \in \mathrm{Br}(U_{\mathbf{Q}})$ extends to an $A \in \mathrm{Br}(X_{\mathbf{Q}})$.

For $p \neq 2$, the image of

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

is zero.
For $p = 2$, the image of this map coincides with $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ if and only if
(i) 2 divides m exactly and $n \equiv 5\ (8)$
or
(ii) 4 divides m and $n \equiv 3 \ \text{or} \ 5\ (8)$
Thus $X(\mathbf{Z}) = \emptyset$ in cases (i) and (ii).

Theorem (F. Xu and R. Schulze-Pillot, 2004). *In all other cases* $X(\mathbf{Z}) \neq \emptyset$.

The following, general result provides a proof of this result which avoids genus theory.

Theorem *Let $q(x_1, \cdots, x_n)$ be an integral quadratic form of rank n, indefinite over $\mathbf{R}$, and let $a \in \mathbf{Z}$, $a \neq 0$. Let $X/\mathbf{Z}$ be the $\mathbf{Z}$-Scheme defined by $q(x_1, \cdots, x_n) = a$. Assume $\prod_p X(\mathbf{Z}_p) \neq \emptyset$.*
(a) If $n \geq 4$, then $X(\mathbf{Z}) \neq \emptyset$: one can solve the equation $q(x_1, \cdots, x_n) = a$ in $\mathbf{Z}$.
(b) Assume $n = 3$ and $-a \cdot det(q)$ is not a square. Then $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = \mathbf{Z}/2$. Let $A \in \mathrm{Br}(X_{\mathbf{Q}})$ generate this quotient. We have $X(\mathbf{Z}) \neq \emptyset$ if and only if the map

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

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

contains zero in its image.

Theorem (a) was proven in the fifties (Eichler, Kneser, Watson).
Theorem (b) is a variant (CT/F.Xu, 2005) of a result of Borovoi and Rudnick (1995).
The main points of the proof of (b) are :
the strong approximation theorem for the spinor group of an indefinite quadratic form
the represention of an affine quadric surface $q = a$ over $\mathbf{Q}$ with a $\mathbf{Q}$-rational point as a quotient G/T, where G is the spinor group of q and T is a 1-dimensional algebraic torus over $\mathbf{Q}$.

One can make the algebra A explicit. Let M be a $\mathbf{Q}$-rational point on

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

Let $l(x, y, z) = 0$ be the equation of the tangent plane to the affine quadric $X_{\mathbf{Q}}$ at the point M.
For A one can take the quaternion algebra

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

Homogeneous spaces of linear algebraic groups

Over many years, a series of papers has established the Hasse principle for principal homogeneous spaces of semisimple simply connected linear algebraic groups (Hasse, Landherr, Eichler, Kneser, Harder, Chernousov).
A consequence is the following generalization of the Minkowski-Hasse theorem :
Theorem (Harder, 1970) *Let $X/\mathbf{Q}$ be a projective variety which is a homogeneous space of a connected linear algebraic group. The Hasse principle holds for X.*

Another consequence is

Theorem *Let $X/\mathbf{Q}$ be smooth projective variety. Assume there exists a nonempty open set $U \subset X$ which is a homogeneous space of a connected linear algebraic group with connected geometric stabilizers.*

Then $X(\mathbf{Q})$ is dense in $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.

In particular $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ implies $X(\mathbf{Q}) \neq \emptyset$.
(Sansuc 1981, Borovoi, 1996)

Curves of genus 1

Examples : nonsingular cubic curves in the plane $\mathbf{P}^2$, nonsingular intersections of two quadrics in space $\mathbf{P}^3$.
An elliptic curve over $\mathbf{Q}$ is a curve of genus 1 with a group structure, in particularly with a marked $\mathbf{Q}$-rational point.

To each nonsingular projective curve $X/\mathbf{Q}$ of genus 1 one associates an elliptic curve $J = J_X$ over $\mathbf{Q}$, the Jacobian of X. The curve X is a principal homogeneous space of J.

The set of isomorphy classes of curves $X/\mathbf{Q}$ of genus 1 with the same Jacobian $J_X = J$ has a natural structure of an abelian group. It is the Weil-Châtelet group $WC(J)$. The class of X in $WC(J)$ is zero if and only if $X(\mathbf{Q}) \neq \emptyset$.
The Tate-Shafarevich group

$$TS(J) \subset WC(J)$$

consists of the classes of curves which have points in all $\mathbf{Q}_p$'s.

Expectation *For any $J/\mathbf{Q}$, the group $TS(J)$ is finite.*

Theorem (Manin 1970). *Let $X/\mathbf{Q}$ be a curve of genus 1. Assume $TS(J_X)$ is finite. If $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$, then $X(\mathbf{Q}) \neq \emptyset$.*

This is a consequence of results of Cassels. Cassels defined an alternate form on $TS(J)$, with value in $\mathbf{Q}/\mathbf{Z}$. He showed : if $TS(J)$ is finite, then the form is nondegenerate. Under the finiteness assumption, this implies that for any $r \geq 1$ the subgroup ${}_rTS(J)$ of r-torsion elements in $TS(J)$ is a direct sum of groups of the shape $(\mathbf{Z}/n)^2$. In particular the order of ${}_rTS(J)$ is a square.

This implies a modest Hasse principle :

Theorem

Let $X/\mathbf{Q}$ be a curve of genus 1 and l a prime. The combination of the following assumptions

(i) the group $TS(J_X)$ is finite
(ii) for all primes p, we have $X(\mathbf{Q}_p) \neq \emptyset$
(iii) the group ${}_lTS(J_X)$ has at most l elements
(iv) the class of X in $TS(J_X)$ is l-torsion

implies $X(\mathbf{Q}) \neq \emptyset$.

Curves of genus ≥ 2

Let $X/\mathbf{Q}$ be a smooth projective curve of genus $g \geq 2$. To such a curve one associates its Jacobian $J_X/\mathbf{Q}$. This is an abelian variety of dimension g.

The set $X(\mathbf{Q})$ is finite (Faltings).

Theorem

Assume $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ *and* $TS(J_X)$ *finite.*
(a) There exists an embedding $X \hookrightarrow J_X$.
(b) The image of $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$ *in* $\prod_{p \text{ finite}} J_X(\mathbf{Q}_p)$ *lies in the topological closure of* $J_X(\mathbf{Q})$.
(c) (Scharaschkin) If $J_X(\mathbf{Q})$ *is finite, then* $X(\mathbf{Q}) = X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$;
in particular

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

implies $X(\mathbf{Q}) \neq \emptyset$.

Question (Skorobogatov) *Let $X/\mathbf{Q}$ be an arbitrary smooth projective curve of genus $g \geq 2$. If $X(\mathbf{Q}) = \emptyset$, does this imply $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$?*
This question has led to recent research in three different directions.

Study of some Shimura-curves (Skorobogatov, Siksek, Rotger, Yafaev).

Experimental mathematics with hyperelliptic curves of genus 2 with small coefficients (Flynn, 2004).

Theorem (Stoll, 2005) *Let $E/\mathbf{Q}$ be an elliptic curve, X a smooth projective curve and $f : X \to E$ a finite morphism. Assume that $E(\mathbf{Q})$ is finite and that the finite set $X(\mathbf{Q}) \cap f^{-1}(E(\mathbf{Q}))$ is empty.*
(i) Then $X(\mathbf{Q}) = \emptyset$ (trivial).
(ii) If $TS(E)$ is finite, then $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} = \emptyset$.

Surfaces with a pencil of curves of genus zero

Theorem *Let* $a(t), b(t), c(t) \in \mathbf{Q}[t]$, $abc \neq 0$. *Let* $X/\mathbf{Q}$ *be a nonsingular projective surface birational to the affine surface with affine equation*

$$a(t)x^2 + b(t)y^2 + c(t) = 0.$$

If the Schinzel hypothesis holds, then $X(\mathbf{Q})$ *is dense in* $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.
(CT/Sansuc 1978, Serre 1992, CT/Swinnerton-Dyer 1994)

The Schinzel hypothesis

Let $P_1(t), \cdots, P_m(t)$ be irreducible polynomials with integral coefficients and positive leading coefficient. Suppose there is no prime which divides all $\prod_i P_i(n)$, $n \in \mathbf{Z}$. Then there are infinitely many $n \in \mathbf{N}$ such that each $P_i(n)$ is a prime.

The only known case is $m = 1$, $P_1(t) = at + b$ (Dirichlet).
A special case is the twin primes conjecture.
More special cases were put forward by Bouniakowsky and by Dickson.

If the number of $t \in \overline{\mathbf{Q}}$ with $a(t)b(t)c(t) = 0$ is at most 5, then one can give an unconditional proof of the existence of a rational point.

Here is a consequence.
Theorem (CT/Sansuc/Swinnerton-Dyer 1987) *Let $n \geq 8$. If a smooth complete intersection of two quadrics in $\mathbf{P}^n_{\mathbf{Q}}$ has points in the reals, then it has points in $\mathbf{Q}$.*

Earlier results : Mordell ($n \geq 12$); Swinnerton-Dyer ($n \geq 10$).

Surfaces with a pencil of curves of genus 1

We have seen a very special case of a Hasse principle for some curves of genus 1.

Around 1994 Swinnerton-Dyer saw how to use this to predict the existence of rational points on certain surfaces with contain a pencil of curves of genus 1. The technique, put in an invariant setup by CT/Skorobogatov/Swinnerton-Dyer (1998) and then further refined by Wittenberg (2005), is quite elaborate.

I will here only quote some striking results it leads to.

Theorem (Swinnerton-Dyer, 2001) *Let $a_i \in \mathbf{Z}, i = 0, \cdots, 3$ be cubefree integers without common denominator. Let $X \subset \mathbf{P}^3_{\mathbf{Q}}$ be the cubic surface*

$$\sum_{i=0}^{3} a_i x_i^3 = 0.$$

Assume that Tate-Shafarevich groups of elliptic curves are finite. If one of the following conditions is fulfilled : (i) there is a prime $p \neq 3$ which divides a_0 and none of the other a_i's, and there is a prime $q \neq 3$ which divides a_1 and none of the other a_i's, (ii) there is a prime $p \neq 3$ which divides a_0 and none of the other a_i's, and the classes of a_1, a_2, a_3 in $\mathbf{F}_p^*/\mathbf{F}_p^{*3}$ are not all equal, then the Hasse principle holds for X.

Theorem (Swinnerton-Dyer 2001)
Assume Tate-Shafarevich groups of elliptic curves are finite. Then the Hasse principle holds for any diagonal cubic hypersurface

$$\sum_{i=0}^{n} a_i x_i^3 = 0$$

over $\mathbf{Q}$, *as soon as* $n \geq 4$.

Theorem (Wittenberg, 2005)
Let $q_1(x_0, \cdots, x_4)$ *und* $q_2(x_0, \cdots, x_4)$ *be two quadratic forms with coefficients in* $\mathbf{Q}$. *Assume the variety* $X \subset \mathbf{P}^4_{\mathbf{Q}}$ *defined by*

$$q_1(x_0, \cdots, x_4) = 0, q_2(x_0, \cdots, x_4) = 0$$

is a nonsingular surface.
If the Galois group of the equation $det(\lambda q_1 + \mu q_2)$ *is the full symmetric group* S_5, *and we accept the Schinzel hypothesis and the finiteness of Tate-Shafarevich groups of elliptic curves, then the Hasse principle holds for* X.

Theorem (Wittenberg, 2005)
Let $X \subset \mathbf{P}^n_{\mathbf{Q}}$, $n \geq 5$ be a nonsingular complete intersection of two quadrics. If we accept the Schinzel hypothesis and grant the finiteness of Tate-Shafarevich groups of elliptic curves, then the Hasse principle holds for X.

Very special cases had been obtained in earlier papers (CT/Skorobogatov/Swinnerton-Dyer, Swinnerton-Dyer/Bender, CT), which had failed to establish the statements above. Wittenberg's proof involves a systematic rewriting of earlier work in this direction and some quite serious concrete algebraic geometry. It also uses a recent result of Harari (fibration method over a higher dimensional base).