Local-global principle over number fields, a hundred years after Hasse's papers on quadratic forms

CCR Princeton, April 1st 2024

Jean-Louis Colliot-Thélène
CNRS, Université Paris-Saclay
visiting Simons foundation, New York

Diophantine equations (Diophantus of Alexandria, around 260 A.D.)
$f(x_1, \ldots, x_n)$ a polynomial with integral coefficients

First problem : to decide if the equation $f(x_1, \ldots, x_n) = 0$ has at least one solution

(a) with $x_1, \ldots, x_n$ integers, i.e. in the ring $\mathbb{Z}$ (Hilbert's 10th problem) – Matiyasevich (1964) proved that there is no systematic algorithm

(b) with $x_1, \ldots, x_n$ rational numbers, i.e. in the field of rational fractions $\mathbb{Q}$ (weaker problem, unless f homogeneous) – here the existence of a systematic algorithm is an open question

Some other problems (not addressed in this talk) : exhibit solutions ; find all solutions.

Euclid (300 B.C.)
The equation $x^2 = 2y^2$ *has no solution in integers other than* $(0, 0)$.
Proof. If there is another solution, then $x^2 = 2y^2 \neq 0$. A smallest nonzero solution has $x \neq 0$ and $y \neq 0$, not both of them even. But $x^2 = 2y^2$ implies x even, so $x = 2m$, so $x^2 = 4m^2$, then $4m^2 = 2y^2$ hence $2m^2 = y^2$ and then y is even. Contradiction.

One may consider this as an early example of the use of valuations (here the 2-adic valuation) as considered by Hensel (1861-1941).

The equation

$$x^3 + 5y^3 + 25z^3 = 0$$

has no integral solution other than $(0, 0, 0)$.
If there is such a solution, there is one for which 5 does not divide the three integers x, y, z.
Then 5 divides x^3, hence 5 divides x, hence 5^2 divides $5y^3$, hence 5 divides y and x so 5^3 divides $25z^3$ so 5 divides z. Contradiction.

Similarly :
For any prime p :
$x^3 + py^3 + p^2z^3 = 0$
$x^4 + py^4 + p^2z^4 + p^3t^4 = 0$.

Congruences

Let $m > 1$ be an integer. Two natural integers a and b are called congruent modulo m if the division of a and of b by m yields the same rest : $a = Am + r$, $b = Bm + r$, $0 \leq r < m$, in other terms if if m divides $a - b$. The latter definition extends to all integers (a, b).

If a is congruent to a' and b congruent to b' then $a - b$ is congruent to $a' - b'$, and $a.b$ is congruent to $a'.b'$.
The congruence classes thus define a commutative ring $\mathbb{Z}/m$.
The case $m = 9$ was used in primary schools until late in the 20th century. This was referred to as : Casting out nines, preuve par neuf, Neunerprobe mittels der Quersumme.

Let n be an integer. If $m = 2n$ then $m^2 = 4n^2$ is congruent to 0 mod. 4. If $m = 2n + 1$ then $m^2 = (2n + 1)^2 = 4n^2 + 4n + 1$ congruent to 1 mod 4.
Thus a sum of two squares of integers is congruent to $0, 1, 2$ mod.4, it is never congruent to 3 mod. 4. In particular an odd prime p congruent to 3 mod 4 is not a sum of two squares of integers.
A "converse" is harder.
Theorem (.., Fermat, Euler 1750) *If an odd prime number p is congruent to 1 mod. 4, then it is a sum of two squares of integers.*
One may consider this as a first example of a local-global principle. Indeed the hypothesis on p implies thall all possible congruences $p = x^2 + y^2$ modulo a positive integer have a solution.

Let $a, b, c \in \mathbb{Z},\ abc \neq 0$, coprime.
Conics alias quadratic forms in 3 variables

$$ax^2 + by^2 + cz^2 = 0,$$

Legendre (1830) proved :
If there exist $r, s, t \in \mathbb{Z}$ with no common divisor, such that $4abc$ divides $ar^2 + bs^2 + ct^2$, then the given equation has a solution with $x, y, z \in \mathbb{Z}$ not all zero.

In particular the congruence hypothesis implies that a, b, c cannot be all of the same sign.

Fix a prime p. If one lets m run through the powers p^t of p and one considers congruences modulo all p^t, then after Hensel (1861-1941) one defines a ring $\mathbb{Z}_p$ which controls all $\mathbb{Z}/p^t$: a polynomial equation $f(x_1, \ldots, x_n)$ with integral coefficients has a solution in $\mathbb{Z}_p$ if and only if it has a solution modulo all p^t.
The ring $\mathbb{Z}_p$, ring of p-adic integers, is better than all $\mathbb{Z}/p^t$: just like $\mathbb{Z}$ it has no zero divisor, one can thus consider its fraction field $\mathbb{Q}_p$, just like one builds $\mathbb{Q}$ from $\mathbb{Z}$. The field $\mathbb{Q}_p$ is a completion of the field $\mathbb{Q}$, via the p-adic valuation, just like the real field $\mathbb{R}$ is the completion of $\mathbb{Q}$ wrt to the real absolute value.
The ring $\mathbb{Z}$ lies in each ring $\mathbb{Z}_p$. The field $\mathbb{Q}$ lies in each field $\mathbb{Q}_p$.

If a polynomial equation with coefficients in $\mathbb{Z}$ has a solution (with coordinates) in $\mathbb{Z}$, then it has a solution in all $\mathbb{Z}_p$ and in $\mathbb{R}$.
If a polynomial equation with coefficients in $\mathbb{Q}$ has a solution (with coordinates) in $\mathbb{Q}$, then it has a solution in all $\mathbb{Q}_p$ and in $\mathbb{R}$.
In a finite number of steps, one may decide if the local conditions are all satisfied.

For p an odd prime, the equation $pz^2 - x^2 - y^2 = 0$ has solutions in all completions of $\mathbb{Q}$ (including $\mathbb{R}$) except possibly $\mathbb{Q}_p$ and $\mathbb{Q}_2$, and then
either
• no solution in $\mathbb{Q}_p$ and in $\mathbb{Q}_2$ (if p is congruent to 3 mod 4)
or
• also solutions in $\mathbb{Q}_p$ and in $\mathbb{Q}_2$, (if p is congruent to 1 mod 4), and then it has a solution in $\mathbb{Q}$ (Fermat, Euler ; 1747/1755)

One can translate Legendre's theorem (1830) as :
Let $a, b, c \in \mathbb{Q}$ be rational numbers, $abc \neq 0$.
If the equation $ax^2 + by^2 + c = 0$ has solutions in all $\mathbb{Q}_p$ and in $\mathbb{R}$, then also in $\mathbb{Q}$.
Moreover one has the following fundamental theorem, which contains the celebrated quadratic reciprocity law (Gauß 1801, conjectured by Euler) :
The number of completions (p-adic or real) of $\mathbb{Q}$ *over which the equation* $ax^2 + by^2 + c = 0$ *has no solution is an even number.*

A hundred years ago

There were several generalisations of Legendre's theorem (Hilbert, Minkowski, Hasse).
Hasse, Dissertation, Marburg 1921 – he was 22. Four papers on the topic "Quadratische Formen" in Crelles Journal (1923, 1924)
One now says that the Hasse principle, also referred to as local-global principle, holds for a class of diophantine equations over $\mathbb{Q}$ if for any equation in that class there is a solution with rational coordinates as soon as there are "local" solutions in all completions of $\mathbb{Q}$, that is over $\mathbb{R}$ and over the p-adic fields $\mathbb{Q}_p$.
There is a similar definition for number fields k and their completions k_v.

There is an extension of Legendre's theorem, which I only quote over the rational numbers.

For any integer n and any equation $\sum_{i=1}^{n} a_i x_i^2 = 0$ with coefficients in $\mathbb{Q}$, there is a non-zero solution over $\mathbb{Q}$ if and only if there is solution over each $\mathbb{Q}_p$ and $\mathbb{R}$.

One may phrase this in the language of congruences.

In the introduction of the relevant paper in the series, Hasse clearly states that the proof in the case of $n = 4$ variables relies on three arithmetic ingredients :

• the case $n = 3$ (Legendre), which over $\mathbb{Q}$ one may prove by geometry of numbers.

• Dirichlet's theorem (1837/1841) : In an arithmetic progression. $an + b$ with $a > 0$, a and b fixed coprime integers, there are infiinitely many prime numbers.

• The generalisation of Gauss' law of quadratic reciprocity (1801) (Hilbert, Furtwängler).

After 1923, along with the development of class field theory, other local-global principles were obtained.
Extension of Legendre's theorem :
(Hasse's norm principle) *Let K/k be a cylic extension of number fields. If $c \in k$ is a norm of K/k over each completion k_v, then already over k.*
Other results of the kind were obtained by Albert, Brauer-Hasse-Noether (1933), and later Eichler, Kneser, Harder while the arithmetic theory of linear algebraic groups was developed.

It was relatively soon observed that the Hasse principle does not hold for arbitrary classes of equations.

Some classes where the "principle" in general fails

Hasse : There are finite field extensions of number fields for which the norm principle fails, for instance some biquadratic extensions.

Lind (1940) and Reichardt (1942) $x^4 - 17 = 2z^2$
Selmer (1951) $3x^3 + 4y^3 + 5z^3 = 0$.
The latter two special cases of a phenomenon well studied in the theory of curves of genus 1 (Cassels, Tate-Shafarevich group)

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

Fifty years ago

In the face of these and other isolated counterexamples, the question to ask was : is there a common argument or even method behind these counterxamples ?
In his ICM 1970 lecture and his book on Cubic Forms, for most known counterexamples to the Hasse principle Yuri I. Manin showed that a common mould was available.
This combines the reciprocity law for the Brauer group of number fields (Hasse, Brauer, Noether 1930) with the notion of Brauer group $\mathrm{Br}(X)$ of a variety X, as developed and studied by Grothendieck (1968).

Let X be a system of homogeneous equations :

$$f_i(x_0, \ldots, x_n) = 0, \ \ i = 1, \ldots, m).$$

$X(k)$ denotes the set of nonzero solutions of the equation X with coordinates in the number field k.
$X(k_v)$ denotes the set of nonzero solutions of the equation X with coordinates in the local field v.

One can define the Brauer-Manin obstruction to the Hasse principle in a compact formula.
There is a pairing

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

mapping the family $\{m_v\}_v$ of local solutions and $\alpha \in \mathrm{Br}(X)$ to $\sum_v \alpha(m_v)$. Here the k_v's run through all completions of k.
The left kernel of this pairing is denoted $X(\mathbb{A}_k)^{\mathrm{Br}}$ and is called the Brauer-Manin set of X. One has

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$$

Hasse principle would be : RHS not empty implies LHS not empty.
Brauer-Manin obstruction : when middle set is empty.

Since the 80s, classes of diophantine equations have been produced for which the Brauer-Manin obstruction is the only obstruction. For many reasons, in particular because of the Bombieri-Lang conjecture on varieties of general type, no one believed that the Brauer-Manin obstruction would account for all counterexamples to the Hasse principle for arbitrary diophantine equations.

The first unconditional example (Skorobogatov) with $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ but $X(k) = \emptyset$ appeared 30 years after Manin's ICM talk.
There is a series of works analysing the new obstruction and its possible extensions.

There are however many families of equations for which none of these obstructions yield any information. That is the case for hypersurfaces

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

when $n \geq 4$ and $d > n$ (these are "varieties of general type"). Here $\mathrm{Br}(X)$ is reduced to $\mathrm{Br}(k)$.
It thus seems reasonable to concentrate attention on equations whose geometry is closer to that of varieties which one could "parametrize" (cf. quadrics).

A good class of such equations, I shall now say algebraic varieties, or, shorter, varieties, was found by the complex algebraic geometers in the 90s. This happenend in the process of the birational classification of varieties of higher dimension (MMP), in particular in work of Kollár, Miyaoki, Mori, Campana.

It is the class of "rationally connected" varieties. These are the varieties which, over the complex field, have the property that for any two points one may find a curve of genus zero (that is, parametrizable, in old fashion language) lying on the variety and passing through the two points.

Examples of rationally connected varieties

• Hypersurfaces $\sum_{i=0}^{n} a_i x_i^d = 0$ with $n \geq 2$ and $d \leq n$ (Proof : Campana, Kollár-Miyaoka-Mori).

• Geometrically unirational varieties, which over the complex field may be parametrized, not necessarily in a one-to-one way. For example cubic hypersurfaces $\sum_{i=0}^{n} a_i x_i^3 = 0, n \geq 3$.

• Varieties fibred over affine space with fibres quadrics of dimension at least one, for instance those given by an equation

$$a(t_1, \ldots, t_n).x^2 + b(t_1, \ldots, t_n).y^2 + c(t_1, \ldots, t_n) = 0$$

with a, b, c polynomials in $k[t_1, \ldots, t_n]$.

• Homogeneous spaces of connected linear algebraic groups, a generalisation of quadrics.

In 1979, backed by concrete computations and some results, J.-J. Sansuc and I made the following conjecture in the case of surfaces.

Main conjecture (1999). Let X be variety over a number field $k \subset \mathbb{C}$. If the variety considered over $\mathbb{C}$ is rationally connectred, then the Brauer-Manin obstruction is the only obstruction to the Hasse principle for X over k.

That is, for such varieties, one hopes :

$$[\prod_v X(k_v)]^{\mathrm{Br}} \neq \emptyset \Longrightarrow X(k) \neq \emptyset.$$

Some classes of rationally connected varieties for which the conjecture has been proved.

Homogeneous spaces of connected linear algebraic groups
These are generalisations of quadrics. The situation is understood when the geometric stabilizers are connected (Sansuc 1981, Borovoi 1996).
Methods : Class field theory, Galois cohomology (Serre, Tate), earlier results of Albert, Brauer-Hasse-Noether (1933). Eichler, Kneser, Harder.
For finite geometric stabilizers, the questions in this area are difficult, they are related to the inverse Galois problem (recent works building upon the fibrations and descent techniques : Harpaz and Wittenberg).

The circle method (Hardy and Littlewood, Davenport, Birch, Hooley, Heath-Brown)

Theorem (Birch, 1961/1962) *Let $F(x_0, \ldots, x_n) = 0$ be a nonsingular hypersurface of degree d with coefficients in $\mathbb{Q}$. For $n \geq (d-1)2^d$, the Hasse principle holds.*

For $n \geq 4$, the "main conjecture" predicts the Hasse principle as soon as $n \geq d$.

For $d = 3$:
Birch gives the result for $n \geq 16$. This was lowered to $n \geq 9$ (Heath-Brown 1983) and then $n = 8$ (Hooley 1988). The "main conjecture" predicts the result for $n \geq 4$.

Fibration and descent

In the years 1980-1987 (CT, Sansuc, Coray, Swinnerton-Dyer) the main conjecture was proved for classes of varieties to which methods already mentioned did not apply (not enough variables, no homogeneous structure).

For Châtelet equations

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

with $a \in \mathbb{Q}$ *and* $P(t)$ *a polynomial with coefficients in* $\mathbb{Q}$ *of degree* 4 *the main conjecture holds. If* $P(t)$ *is irreducible this gives the Hasse principle.*

(The main conjecture predicts this last result for $P(t)$ irreducible of arbitrary degree.)

For example one can decide when a rational number may be written as $a^2 + b^2 + c^4$.

Methods

Fibrations

By intersection with hyperplanes one tries to reduce to varieties of smaller dimension for which one already knows the conjecture. The simplest case is Hasse's proof of his principle for quadratic forms in at least 5 variables starting from the result in 4 variables.
One tricky point is to find hyperplane sections which like the given variety still have points in all completions.

Descente. This is a generalisation of the method which had long be used to study cubic curves.
For Châtelet surfaces, the descent varieties are 5-dimensional intersections of two quadrics

$$f(x_0, \ldots, x_7) = 0, \ g(x_0, \ldots, x_7) = 0$$

with f and g homogeneous of degree 2, with some extra feature. By fibrations, the search for solutions of the latter system is reduced to the study of a lower dimensional variety which is somehow easier to handle (ultimately to del Pezzo surfaces of degree 6).

Regarding general intersections ot two quadrics, we have

For "reasonable" intersections of two quadrics in at least 8 homogeneous variables, the Hasse principle holds.
(CT-Sansuc-Swinnerton-Dyer 1987, Heath-Brown 2018, CT 2022, Molyakov 2023)
The main conjecture predicts that this holds for at least 7 variables and, in the smooth case, even for 6 variables.

Around Schinzel's hypothesis

Schinzel's hypothesis (1958) is a daring generalisation of Dirichlet's theorem on primes in an arithmetic progression. This theorem says that a linear polynomial $P(x) = ax + b$ with integral coefficients represents infinitely many primes (and gives a density) if a and b are coprime. Schinzel's hypothesis predicts a similar result for arbitrary irreducible polynomials in $\mathbb{Z}[x]$ and even for a simultaneous set $P_i(x), i = 1, \ldots, N$ of irreducible polynomials. The hypothesis goes back to Bouniakowsky (1857) and to works of Hardy and Littlewood (early 20th century). An explicit density was proposed by Bateman and Horn.

Remark (CT/Sansuc 1979, ... 1994) *Under Schinzel's hypothesis, for equations*

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

with $a(t), b(t), c(t) \in \mathbb{Q}[t]$, *the Brauer-Manin obstruction is the only obstruction to the Hasse principle.*

In the simplest cases, one directly mimicks Hasse's proof for quadratic forms in 4 variables (the reciprocity laws of class field theory also play their part in the proof).

"Arithmetic statistics"

Green, Tao, Ziegler (2010-2012) proved :
For a reasonable finite system of linear polynomials in $\mathbb{Z}[x, y]$ *in two variables* $a_i x + b_i y + c_i$ $(i = 1, \ldots, N)$ *there exist pairs of integers* (n, m) *such that all* $a_i n + b_i m + c$ $(i = 1, \ldots, N)$ *are prime numbers.*
The motto "Schinzel implies Hasse" can then be unconditionally developed for whole families of equations.

For equations $a(t)x^2 + b(t)y^2 + c(t) = 0$ *with coefficients in* $\mathbb{Q}$*, if the polynomal* $a(t)b(t)c(t)$ *has all its roots in* $\mathbb{Q}$*, then the strong form of the main conjecture holds, namely* $X(\mathbb{Q})$ *is dense in the Brauer-Manin set* $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$*.*

(Browning, Harpaz, Mathiesen, Skorobogatov, Wittenberg, 2014-2016)

Until then, for most equations of this type, e.g. surfaces $y^2 + z^2 = \prod_{i=1}^{n}(t - e_i)$ for $n > 8$, one did know whether rational points were not located on a finite union of curves.

"Schinzel on average"
One considers the set of all integral irreducible polynomials $P(t)$ of a given degree d with an obvious extra condition.

Theorem (Skorobogatov and Sofos, 2022) *If one orders the polynomials of a given degree by the maximum value H of the absolute values of the coefficients, when H grows, for 100 % of these polynomials $P(t)$ there exists at least one integer n such that $P(n)$ is prime.*
(One does not require that a polynomial represent infinitely many primes.)
This is enough to prove
For fixed $a \in \mathbb{Z}$, and fixed d, for a positive proportion of the polynomials $P(t) \in \mathbb{Z}[t]$ ordered by the maximum of the coefficients, the equation $y^2 - az^2 = P(t)$ has a solution in rational numbers (y, z, t).

Geometry of numbers (à la Minkowski)

The Hasse principle for random Fano hypersurfaces
Browning, Le Boudec, Sawin (2023)

Fix $n \geq 4$ and $d \leq n$. The Hasse principle holds for almost all hypersurfaces in $\mathbb{P}^n$ of degree d.
(One does not know which ones.)

Almost all : the hypersurfaces are ordered by the maximal absolute value H of the coefficients of a primitive equation in $\mathbb{Z}[x_0, \ldots, x_n]$ and one counts the number of equations for which the result holds, as H grows.

Similar result for cubic surfaces ($d = 3, n = 3$). This corresponds to the fact, taught to us by experience, that although Brauer-Manin obstruction to the Hasse principle may occur for such surfaces, they very rarely happen.

But the following question remains open.

Can one decide if a given equation

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

with integral coefficients (a, b, c, d) *has a nonzero solution in integers* (x, y, z, t) *?*
There is a result in this direction by Swinnerton-Dyer (2001) conditional on the finiteness of Tate-Shafarevich groups of elliptic curves.

One knows (1987) : If the coefficients (a, b, c, d) have no common divisor and are cubefree, Brauer-Manin obstruction for such a cubic surface can occur only if each prime number which divides $abcd$ occurs in two coefficients.
Cassels-Guy $(5, 9, 10, 12)$