Raymond and Beverly Sackler
Distinguished Lectures in Mathematics

Tel Aviv University

November 13, 2003

Rational points on surfaces fibred into curves of genus one

J.-L. Colliot-Thélène

C. N. R. S. et Université Paris-Sud
(France)

In the previous lecture, I mentioned the fibration method for studying the question whether the set of rational points $X(k)$ is dense in the Brauer-Manin subset $X(\mathbb{A}_k)^{\mathrm{Br}}$ of the adèles of a nonsingular, projective variety X over a number field k.

The theorems quoted in the first lecture led to actual results for the total space of one-parameter families of conics, and there is scope for applying them to the total space of one-parameter families of varieties, when the generic member of the family is birational to a homogeneous space of a connected linear algebraic group.

What if one considers one-parameter families of homogeneous spaces of abelian varities, for instance one-paramer families of curves of genus one ?

This is a very natural question. For instance, if one wishes to study the Hasse principle for a cubic surface in $\mathbf{P}^3$, the natural thing to do is to fix a line in $\mathbf{P}^3$, to consider the pencil of planes through this line: they cut out on the surface a pencil of curves of genus one. Can one use the conjectural results for each curve of genus one in the pencil (built upon finiteness of the Tate-Shafarevich group) to gather a global information on the rational points of the surface ?

In 1994, Swinnerton-Dyer took the first serious step in this direction, and in 1998 CT/Skorobogatov/Swinnerton-Dyer produced a suitable general format for the method. Since then Swinnerton-Dyer and various collaborators have produced a series of results – most of them, but not all, conditional on Schinzel's hypothesis and on the finiteness of Tate-Shafarevich groups.

It is not clear at this point what the final format for the (rather involved) method will be. In this lecture I will describe some of the key steps.

Before I do this, let me list a series of concrete results obtained.

Two simultaneously diagonal quadratic forms

Theorem
Let k be a number field and $a_i, b_i \in k^*, i = 0, \dots, 4$. Let $X \subset \mathbf{P}^4_k$ be defined by

$$\sum_{i=0}^{4} a_i x_i^2 = 0, \qquad \sum_{i=0}^{4} b_i x_i^2 = 0.$$

Assume:
(i) Tate-Shafarevich groups are finite;
(ii) Schinzel's hypothesis holds.
If the a_i, b_i are general enough, then the Hasse principle holds for X.

(Swinnerton-Dyer 1995, CT/Skorobogatov/Swinnerton-Dyer 1998)

General enough: independence of various products $a_i b_j - a_j b_i$ in k^*/k^{*2}. The hypothesis implies $X(\mathbb{A}_k)^{\mathrm{Br}} = X(\mathbb{A}_k)$.

Should be enough to imply Hasse principle for $\sum_{i=0}^{n} a_i x_i^2 = 0, \ \sum_{i=0}^{n} b_i x_i^2 = 0$ as soon as $n = 5$.

Previous results: unconditional Hasse principle for $\sum_{i=0}^{n} a_i x_i^2 = 0, \ \sum_{i=0}^{n} b_i x_i^2 = 0$ for $n \geq 7$ (method as in CT/Sansuc/Swinnerton-Dyer 1987)

Special diagonal quartic surfaces

Theorem *Let k be a number field and $X \subset \mathbf{P}^3_k$ be a quartic surface defined by a diagonal equation*

$$\sum_{i=0}^{3} a_i x_i^4 = 0.$$

Assume

(i) Tate-Shafarevich groups are finite.

(ii) Schinzel's hypothesis holds.

(iii) The product $a_0a_1a_2a_3$ is a square in k, but is not a fourth power, and none of the $\pm a_ia_j$ $(i \neq j)$ is a square.

(iv) $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$.

Then $X(k) \neq \emptyset$.

(Swinnerton-Dyer 2000)

General diagonal cubic surfaces over the rationals

Theorem

Let $X \subset \mathbf{P}^3_{\mathbf{Q}}$ *be a cubic surface defined by a diagonal equation*

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

where one may assume all a_i *in* $\mathbf{Z}$ *and cubefree. Assume*

(i) Tate-Shafarevich groups of elliptic curves are finite.

(ii) There exists a prime $p \neq 3$ *such that* $3 \mid v_p(a_0)$ *and* $p \nmid a_i, i \neq 0$, *and there exists a prime* $q \neq 3$ *such that* $3 \mid v_q(a_1)$ *and* $q \nmid a_i, i \neq 1$.

or

(ii') There exists a prime $p \neq 3$ *such that* $3 \mid v_p(a_0)$ *and* $p \nmid a_i, i \neq 0$, *and the classes of* $a_1, a_2, a_3 \in \mathbf{F}_p^*/\mathbf{F}_p^{*3}$ *are not all equal.*

(iii) $X(\mathbb{A}_{\mathbf{Q}}) \neq \emptyset$.

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

(Swinnerton-Dyer 2000)

The proof extends to any number field k which does not contain all cubic roots of 1.

In the proof one uses finiteness of Tate-Shafarevich groups of elliptic curves over arbitrary quadratic extensions of the ground field.

Comment. Each of the hypotheses (ii) or (ii') implies $X(\mathbb{A}_{\mathbf{Q}})^{\mathrm{Br}} \neq \emptyset$ (CT/Kanevsky/Sansuc 1987).

Basic comment on this theorem : *it does not refer to Schinzel's hypothesis.* The proof uses it, but in the only known case, namely it uses Dirichlet's theorem on primes in an arithmetic progression.

An easy application of the fibration method (in the spirit of Hasse's proof for quadratic forms in 5 variables once the 4 variables case is known) then yields:

Theorem

Assume that Tate-Shafarevich groups are finite. Then the Hasse principle holds for diagonal cubic hypersurfaces in $\mathbf{P}^n_{\mathbf{Q}}$, $n \geq 4$.

(Swinnerton-Dyer 2000)

For $n \geq 6$, this is a known result, proved unconditionnally by means of the circle method (R. C. Baker 1989; Davenport 1959 for $n \geq 8$).

In the well-known analogy between number fields and function fields in one variable over a finite field, the finiteness of Tate-Shafarevich groups of elliptic curves over a number field translates as the finiteness of the Brauer group of certain surfaces over a finite field. This finiteness is known in some cases (Tate). Mimicking Swinnerton-Dyer's argument, I obtained the unconditional result:

Theorem

Let $k = \mathbf{F}_q(C)$ be a function field in one variable over the finite field $\mathbf{F}_q$. Assume q odd, $q \equiv 2$ mod. 3. The Hasse principle holds for diagonal cubic hypersurfaces in $\mathbf{P}^n_k$, $n \geq 4$.

A first idea of the method

Let X be a nonsingular, projective, absolutely irreducible surface over a number field k. Assume it is equipped with a dominant k-morphism $p : X \to \mathbf{P}^1_k$ whose generic fibre is absolutely irreducible.

Under suitable hypotheses on the fibres (in particular, one should assume that *each* of them contains a component of multiplicity one), and upon application of Schinzel's hypothesis, from the hypothesis

$$X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$$

one manages to conclude that there exist infinitely many points $M \in \mathbf{P}^1(k)$ whose fibre X_M satisfies

$$X_M(\mathbb{A}_k) \neq \emptyset.$$

If the fibre X_M satisfies the Hasse principle, this is enough to conclude $X_M(k) \neq \emptyset$, hence $X(k) \neq \emptyset$. Such is the case if the generic fibre is a conic. But if it is a curve of genus one, which I now assume, then we face the problem: the Hasse principle generally does not hold for curves of genus one over a number field. There even exist one parameter families of such counterexamples !

One could dream of using the method of Harari's theorem described in the previous lecture to produce a fibre X_M such that $X_M(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$. Not only is the "abelian difficulty" in the way, but for families of curves of genus one there is no hope to produce rational points $M \in \mathbf{P}^1(k)$ such that the (reduced) Brauer group of X_M is covered by the specialization of the (reduced) Brauer group of the generic fibre – which is what Harari proveswhen the generic fibre is a rationally connected variety.

What has been successful could probably be best described as going though a rat's hole.

Let me first recall the *Selmer calculus* in the simplest set-up. Let k be a field, char.$k = 0$,

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

an elliptic curve with $e_i \in k$, so that all 2-torsion of E is rational. We have the exact sequence

$$0 \to E[2] \to E \stackrel{x \mapsto 2x}{\longrightarrow} E \to 0$$

where $E[2] \cong (\mathbf{Z}/2)^2$. The long exact sequence in Galois cohomology gives

$$0 \to E(k)/2E(k) \to H^1(k, E[2]) \to H^1(k, E)[2] \to 0$$

where $H^1(k, E[2]) \cong (k^*/k^{*2})^2$ classifies 2-*covers*: that is, given $(\alpha_1, \alpha_2) \in (k^*/k^{*2})^2$, we have the 2-cover of E defined by the set of affine equations:

$$x - e_1 = \alpha_1 u_1^2,\ x - e_2 = \alpha_2 u_2^2,\ x - e_3 = (\alpha_1 \alpha_2)^{-1} u_3^2.$$

The group $H^1(k, E)$ classifies curves of genus one whose jacobian is E : these are the principal homogeneous spaces under E.

Let now k be a number field.

The 2-Selmer group $\mathrm{Sel}(E,2)$ of E is the subgroup of $H^1(k,E[2])$ consisting of classes whose associated 2-cover contains points in all completions k_v of k.

The Tate-Shafarevich group $Ш(E)$ is the kernel of the diagonal map $H^1(k,E) \to \prod_{v\in\Omega} H^1(k_v,E)$. It classifies principal homogeneous spaces under E which have points in all k_v's.

The previous sequence induces a basic exact sequence

$$0 \to E(k)/2 \to \mathrm{Sel}(E,2) \to Ш(E)[2] \to 0.$$

Cassels defined an alternate pairing on the group $Ш(E)$, with values in $\mathbf{Q}/\mathbf{Z}$. He proved that if $Ш(E)$ is finite, then this pairing is nondegenerate. The abelian group $Ш(E)$ must then be a sum of groups of the shape $(\mathbf{Z}/n)^2$. In particular its order must be a square, and so must be the order of e.g. $Ш(E)[2]$.

We thus get a Hasse principle for some very special curves of genus 1.

Proposition

Suppose that $E(k)[2] = (\mathbf{Z}/2)^2$ *and injects into* $E(k)/2$*, and suppose that the order of* $\mathrm{Sel}(E, 2)$ *is 8. If the Tate-Shafarevich group of* E *is finite, then* $Ш(E)[2] = 0$*, the Hasse principle holds for 2-covers of* E*, and the rank of* $E(k)$ *is 1.*

Let now $X \to \mathbf{P}^1_k$ be a family of curves of genus one. Assume that the generic fibre X_η is a 2-cover of its jacobian E_η. Assume that the 2-torsion of E_η is entirely rational over $K = k(\mathbf{P}^1)$. (This is not a simplifying assumption: at present, for the method to work, we need some nontrivial "constant" torsion in $E_\eta(K)$.)

Assume $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$.

Suppose one can find a point $M \in \mathbf{P}^1(k)$ such that

(i) the fibre X_M/k satisfies $X_M(\mathbb{A}_k) \neq \emptyset$

(ii) the order of $\mathrm{Sel}(E_M, 2)$ is 8.

If the Tate-Shafarevich group of E_M is finite, the above proposition implies $X_M(k) \neq \emptyset$, hence X_M isomorphic to E_M, and $E_M(k)$ infinite, hence $X_M(k)$ infinite.

As already mentioned, under reasonable (algebraic) assumptions on the reducible fibres, (i) may be ensured by a suitable application of the fibration method (use of Harari's formal lemma, together with Schinzel's hypothesis).

I now have to explain how (ii) can be – simultaneously – achieved.

For the present method to work, we have to restrict attention to families $X \to \mathbf{P}^1_k$ such that a certain algebraico-geometric group associated to the generic fibre is of order 8 (a more precise condition to be given below).

In a very vague fashion, the result is reminiscent of a Hilbert irreducibility theorem : because a kind of algebraic Selmer group is small, one is able to find a specialized arithmetic Selmer group which is just as small.

Given an elliptic curve E_η over the field $K = k(t)$, one defines the algebraico-geometric Tate-Shafarevich group $H^1_{nr}(K, E_\eta)$ as the subgroup of $H^1(K, E)$ consisting of elements whose image in $H^1(\overline{k}(t), E)$ vanishes when further restricted to all completions of $\overline{k}(t)$, namely $\overline{k}((t-a))$ for $a \in \overline{k}$ and $\overline{k}((1/t))$.

One may then define an algebraico-geometric 2-Selmer group $\mathfrak{S}(E_\eta, 2)$ which fits into an exact sequence

$$0 \to E_\eta(K)/2E_\eta(K) \to \mathfrak{S}(E_\eta, 2) \to H^1_{nr}(K, E_\eta)[2] \to 0$$

which is one analogue of the Selmer sequence.

There is a well-known theory (Kodaira, Néron) of minimal models of elliptic curves over discrete valuation rings.

Let $\mathcal{E}/\mathbf{P}^1_k$ the Néron minimal model of $E_\eta/k(\mathbf{P}^1)$. It is a smooth group scheme over $\mathbf{P}^1_k$. There is a short exact sequence of group schemes

$$0 \to \mathcal{E}^* \to \mathcal{E} \to \oplus_Q i_{Q*} F_Q \to 0,$$

where $\mathcal{E}^*/\mathbf{P}^1_k$ has all its fibres connected, Q runs through the finitely many closed points of $\mathbf{P}^1_k$ where E_η has bad reduction, and F_Q is a finite group scheme over the residue field k_Q.

One shows that $H^1_{nr}(K, E_\eta) = H^1_{\text{ét}}(\mathbf{P}^1_k, \mathcal{E})$.

We thus have induced maps

$$\delta_Q : H^1_{nr}(K, E_\eta) \to H^1(k_Q, F_Q).$$

We now restrict attention to the case where the bad reduction of E_η is multiplicative and of type I_2. In that case, each $F_Q = \mathbf{Z}/2$. We have induced maps

$$\partial_Q : \text{Ш}(E_\eta, 2) \to H^1(k_Q, \mathbf{Z}/2).$$

Let us come back to a family $X \to \mathbf{P}^1_k$ of curves of genus one.

Let X_η be the generic fibre and E_η its jacobian. We assume that E_η has all the previous properties.

We assume that X_η is a 2-cover of its jacobian E_η, and that it defines a nontrivial class $m_X \in \text{Ш}(E_\eta, 2)$, hence that the class $[X_\eta] \in H^1(K, E_\eta)$ belongs to $H^1_{nr}(K, E_\eta)[2]$ (this amounts to restrictions on the possibilities for the singular fibres of $X/\mathbf{P}^1_k$).

We now make the **crucial assumption** that the kernel of the composite map Δ :

$$\text{Ш}(E_\eta, 2) \to \oplus_Q H^1(k_Q, \mathbf{Z}/2) \to \oplus_Q \frac{H^1(k_Q, \mathbf{Z}/2)}{\partial_Q(m_X)}$$

is of order 8, spanned by m_X and the image of $E_\eta(K)[2]$.

Theorem
Let $X/\mathbf{P}^1_k$ satisfy the above assumptions. Assume
(i) Tate-Shafarevich groups are finite.
(ii) Schinzel's hypothesis holds.
(iii) $X(\mathbb{A}_k)^{\text{Br}} \neq \emptyset$.
Then $X(k)$ is Zariski dense in X.

(CT/Skorobogatov/Swinnerton-Dyer 1998)

Comment on the crucial assumption

The "crucial assumption" implies that the 2-primary torsion part of the Brauer group of X is "vertical", i.e. its image in the Brauer group of the generic fibre X_η comes from the Brauer group of $k(\mathbf{P}^1)$.

As a matter of fact, in the proof, the only part of assumption (iii) which is used is the fact that there exists an adèle orthogonal to the vertical part of the Brauer group.

One could dream that the theorem above holds as it stands even if one does not make the "crucial assumption" on the kernel of Δ. But I have no idea how to proceed.

The rôle of the nonvertical part of the Brauer group is rather mysterious.

For the time being, all we have at our disposal is an example, due to O. Wittenberg, of an elliptic surface for which the nonvertical, hence "transcendental" part of the Brauer group leads to a lack of weak approximation.

Further indications on the proof of the Theorem

Under the assumption $m_X \in \mathfrak{S}(E_\eta, 2)$, the singular fibres X_Q occur over the same set T of closed points Q where E_η has bad reduction, and there exists a trivial or quadratic extension l_Q/k_Q such that the fibre X_Q consist of two nonsingular conics, each defined over l_Q, meeting transversally in 2 (geometric) points.

We may assume $\infty \notin T$. Each closed point Q is then defined by a monic irreducible polynomials $r_Q(t) \in k[t]$. For simplicity, let me assume here that all r_Q have even degree.

Let $r(t) := \prod_Q r_Q(t)$.

Associated to the whole situation $X \to \mathbf{P}^1_k$ there is a natural finite set of bad places S_0 of k, containing the archimedean and dyadic places, and such that the class group of the ring O_{S_0} of S_0-integers is trivial.

Using the hypothesis $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$, one produces elements $\lambda_v \in k_v$ for $v \in S_0$ such that if $\lambda \in k$ is close enough to each λ_v fro $v \in S_0$ and if each $r_Q(\lambda)$ is a unit at all places away from the union of S_0 and a unique place v_Q, then the fibre X_λ/k is nonsingular and has points in all completions. That is, it defines an element of the 2-Selmer group $\mathrm{Sel}(E_\lambda, 2)$ of its jacobian E_λ.

That such λ exist is guaranteed by Schinzel's hypothesis. The v_Q's will be referred to as the "Schinzel primes".

There is here some flexibility: one may impose distinct additional finite sets S_Q $(Q \in T)$ of places v away from S_0 such that $v(r_Q(\lambda)) = 1$ for $v \in S_Q$, provided each such place v (of degree one over k) splits in the extension l_Q/k_Q. This flexibility is crucial for the argument to follow.

We let $S(\lambda) = S_0 \cup (\cup_Q S_Q) \cup (\cup_Q \{v_Q\})$.

For any commutative normal ring A, let

$$\mathcal{H}(A) = (A^*/A^{*2})^2 \subset H^1(A, (\mathbf{Z}/2)^2).$$

This is an isomorphism if the class group of A is trivial.

For such λ as above, evaluation at λ yields an isomorphism between a group of algebraic nature and a group of arithmetic nature:

$$\theta_\lambda : \mathcal{H}(O_S[t][1/r(t)]) \simeq \mathcal{H}(O_{S(\lambda)}),$$

where S is the union of S_0 and the S_Q for all $Q \in T$, $S(\lambda)$ as above is the union of S and the v_Q's and for any finite set S of places, O_S is the ring of S-integers.

We have :

$\mathrm{Sel}(E_\lambda, 2) \subset \mathcal{H}(O_{S(\lambda)})$.

$\mathcal{H}(O_S[t][1/r(t)]) \subset \mathcal{H}(k[t][1/r(t)])$.

$\mathfrak{S}(E_\eta, 2) \subset \mathcal{H}(k[t][1/r(t)])$.

Under the isomorphism θ_λ^{-1}, the group $\mathrm{Sel}(E_\lambda, 2)$ is mapped into $\mathfrak{S}(E_\eta, 2)$.

$E_\lambda[2] + \mathbf{Z}/2.[X_\lambda] \simeq (\mathbf{Z}/2)^3 \subset \mathrm{Sel}(E_\lambda, 2)$ is mapped isomorphically to $E_K[2] + \mathbf{Z}/2.m_X \subset \mathcal{H}(k[t][1/r(t)])$.

One wants to use the "crucial hypothesis" to exhibit a λ as above such that

$$E_\lambda[2] + \mathbf{Z}/2.[X_\lambda] = \mathrm{Sel}(E_\lambda, 2).$$

For any element in $H^1(k[t][1/r(t)], (\mathbf{Z}/2)^2)$ not in the kernel of Δ, there is one of two types of maps over a closed point of $\mathbf{A}^1_k$ which detects this. And one wants to use this to choose auxiliary sets S_Q in such a way that any element of $\mathcal{H}(O_{S(\lambda)})$ except for the obvious 8 elements is ruled out as an element of $\mathrm{Sel}(E_\lambda, 2)$.

To rule out an element $\xi \in \mathcal{H}(O_{S(\lambda)})$ means to find a place v and an element of $E_\lambda(k_v)$ such that in the pairing

$$H^1(k_v, E_\lambda[2]) \times H^1(k_v, E_\lambda[2]) \to \mathbf{Z}/2$$

induced by the Weil pairing $E_\lambda[2] \times E_\lambda[2] \to \mu_2$, the class of ξ is not orthogonal to the image of $E_\lambda(k_v)/2 \subset H^1(k_v, E_\lambda[2])$ (here one uses a theorem of Tate). The only obvious elements of $E_\lambda(k_v)/2$ which we have at our disposal are the classes of the four 2-torsion elements.

Roughly speaking, if one starts with a given λ and the 2-Selmer group is too big, the "crucial assumption" enables us to produce a $\lambda_1 \in k$ very close to the original λ at the places of $S(\lambda) \subset S(\lambda_1)$, in such a way that the bad classes in $\mathrm{Sel}(E_\lambda, 2) \subset \mathcal{H}(O_{S(\lambda)}) \subset \mathcal{H}(O_{S(\lambda_1)})$ do not belong to $\mathrm{Sel}(E_{\lambda_1}, 2)$.

This does not seem to lead anywhere, because in the process new classes have appeared in $\mathcal{H}(O_{S(\lambda_1)})$ which one now has to rule out.

The process turns out to work all the same.

A key ingredient is a *symmetrized Selmer calculus.*

Symmetrization of the Selmer calculus

Let E be an elliptic curve over a local field k_v.

Let $V_v = H^1(k_v, E[2])$ and $W_v = E(k_v)/2$.

Cassels and Tate proved that the Kummer map $E(k_v)/2 \hookrightarrow H^1(k_v, E[2])$ makes W_v into a maximal isotropic subgroup of V_v equipped with the non-degenerate alternate pairing induced by the Weil pairing.

Let now E be an elliptic curve over a number field. Suppose it has good reduction outside a finite set S of places of k, where S includes the archimedean primes, the dyadic primes and suppose the class group of O_S is trivial. Suppose $E[2] = (\mathbf{Z}/2)^2$.

Let $V_S := \oplus_{v \in S} V_v$ and $W_S := \oplus_{v \in S} W_v$.

The pairings $V_v \times V_v \to \mathbf{Z}/2$ add up to a non-degenerate, alternate pairing

$$V_S \times V_S \to \mathbf{Z}/2.$$

Under our assumptions on S, class field theory implies that the diagonal map $\mathcal{H}(O_S) \to \prod_{v\in S} \mathcal{H}(k_v)$ is an embedding which makes $\mathcal{H}(O_S)$ into a maximal isotropic group of $V_S = \oplus_{v\in S} V_v$.

The Kummer embeddings $W_v \hookrightarrow V_v$ add up to create another maximal isotropic subgroup $W_S \subset V_S$.

The 2-Selmer group may now be identified with the left kernel of the induced pairing

$$\mathcal{H}(O_S) \times \ \oplus_{v\in S} E(k_v)/2 \to \mathbf{Z}/2.$$

Both sides have the same $\mathbf{F}_2$-dimension.

By linear algebra, one shows that there exist maximal isotropic subspaces $K_v \subset V_v$ such that the space $K_S := \oplus_{v\in S} K_v$ is a supplementary space of $\mathcal{H}(O_S)$ in V_S. For v outside a fixed set independent of E, one may take $K_v = \mathcal{H}(O_v)$.

Under projection of V_S onto $\mathcal{H}(O_S)$ along K_S, the above pairing induces a pairing between

$$\mathcal{I}_S := \mathcal{H}(O_S) \cap (W_S + K_S)$$

and

$$\mathcal{W}_S := W_S/(W_S \cap K_S) = \oplus_{v\in S} W_v/(W_v \cap K_v).$$

Proposition

(i) Projection $V_S \to \mathcal{H}(O_S)$ *induces an isomorphism* $\tau : \mathcal{W}_S \simeq \mathcal{I}_S$.

(ii) Both the left and right kernel of the pairing $\mathcal{I}_S \times \mathcal{W}_S \to \mathbf{Z}/2$ *are isomorphic to the* 2*-Selmer group of* E.

(iii) Under the isomorphism τ*, this pairing defines a* **symmetrical** *bilinear form on* $\mathcal{W}_S$*, hence also on* $\mathcal{I}_S$.

In the situation under study, namely bad reduction is of type I_2, for v not in S_0, each group

$$W_v(E_\lambda)/(W_v(E_\lambda) \cap K_v)$$

is either 0 (case of good reduction for E_λ at v) or $\mathbf{Z}/2$ (whereas $W_v(E_\lambda) \simeq (\mathbf{Z}/2)^2$.)

End of the proof (sketch)

Recall the isomorphism

$$\theta_\lambda : \mathcal{H}(O_S[t][1/r(t)]) \simeq \mathcal{H}(O_{S(\lambda)}).$$

One now shows that, for any λ as above, the group $\mathcal{W}_S(E_\lambda)$ is isomorphic to the direct sum $B_0 \oplus B_1 \oplus B_2$ of three vector spaces over $\mathbf{F}_2$, where

$$B_0 = E_\lambda[2] + \mathbf{Z}/2.[X_\lambda] \simeq (\mathbf{Z}/2)^3,$$

B_1 corresponds to a fixed part (independent of λ) having to do with the bad reduction of X and with the Schinzel primes v_Q's,

B_2 is a vector space with a basis indexed by the elements of $\cup_Q S_Q$.

This decomposition can be arranged in such a way that the symmetric pairing on $\mathcal{W}_S(E_\lambda)$ induces a pairing on $B_0 \oplus B_1$ which is independent of the choice of λ.

This is quite subtle, since the Schinzel primes, which depend on λ, which itself depends on the choice of the S_Q's, contribute to B_1. In the proof of this fact, the reciprocity law of class field theory is systematically used.

Let $B_1' \subset B_1$ be the left kernel of the induced pairing $B_1 \times B_1 \to \mathbf{Z}/2$, and let B_1'' be a supplementary space of B_1' in B_1.

On then uses the "crucial assumption" along with the isomorphism θ_λ to produce, for each nontrivial class in B_1'', a suitable Q and a prime v of degree one split in the extension l_Q/k_Q such that the pairing of the group $W_v/(W_v \cap K_v) = \mathbf{Z}/2$ with this class is nontrivial. By linear algebra, taking a subset of all these v's, one finds that the symmetric pairing given by the refined Selmer calculus is given by a matrix of the following type:

B_0	B_1'	B_1''	B_2
0	0	0	0
0	0	0	n.s.
		n.s.	
0	n.s.		

(n.s = nonsingular)

Symmetry gives the n.s. in the right hand side upper corner. Thus the corank of the matrix is 3, which completes the proof.

Concrete applications of the method

Special intersections of two quadrics in $\mathbf{P}^4$

(Swinnerton-Dyer, CT/Skorobogatov/Swinnerton-Dyer)

Let $X \subset \mathbf{P}^4_k$ be given by the simultaneously diagonal quadratic equations:

$$\sum_{i=0}^{4} a_i x_i^2 = 0, \qquad \sum_{i=0}^{4} b_i x_i^2 = 0.$$

If one cuts out X by $x_4 = tx_3$, then one gets the pencil of curves of genus one defined by

$$\sum_{i=0}^{2} a_i x_i^2 + (a_3 + t^2 a_4) x_3^2 = 0,$$

$$\sum_{i=0}^{2} b_i x_i^2 + (b_3 + t^2 b_4) x_3^2 = 0.$$

On checks that the jacobian E_η of the curve X_η (over $k(t)$) has all its 2-torsion rational, that any bad reduction is of type I_2, that X_η is a 2-cover of E_η and that its class belongs to the group $Ш(E_\eta, 2)$.

In a paper with Bender, Swinnerton-Dyer considers a system of two quadratic forms which are only partially simultaneously diagonal, namely

$$a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + q_1(x_3, x_4) = 0,$$

$$b_0x_0^2 + b_1x_1^2 + b_2x_2^2 + q_2(x_3, x_4) = 0.$$

One transforms this surface into a fibration over $\mathbf{P}^1_k$ by setting $x_4 = tx_3$. In this more general case, the jacobian of the generic fibre has only one nontrivial rational point of order 2.

Using isogenies of degree 2 rather than multiplication by 2, one also manages to prove a theorem like the main theorem.

Further work might ultimately lead to a proof (assuming the Schinzel hypothesis and finiteness of Ш) of the well-known

Conjecture

For any nonsingular complete intersection of two quadrics in $\mathbf{P}^n_k$, $n \geq 5$, *the Hasse principle holds.*

Special diagonal quartic surfaces
(Swinnerton-Dyer)

A diagonal quartic surface $X \subset \mathbf{P}^3_k$

$$\sum_{i=0}^{3} a_i x_i^4 = 0$$

has a natural projection onto the quadric $Y \subset \mathbf{P}^3_k$ given by

$$\sum_{i=0}^{3} a_i y_i^2 = 0.$$

Assume $a_0 a_1 a_2 a_3$ is a square in k.

If X has points in all completions of the number field k, then the quadric Y is isomorphic to $\mathbf{P}^1_k \times_k \mathbf{P}^1_k$. This gives two fibrations of X over $\mathbf{P}^1_k$ into curves of genus 1, and one checks that each of them has its bad fibres of type I_4 (four projective lines L_i, $i \in \mathbf{Z}/4$, with L_i and L_{i+1} meeting transversally in one point). One again checks that the jacobian of the generic fibre has all its 2-torsion rational.

Diagonal cubic surfaces over $\mathbf{Q}$
(Swinnerton-Dyer, no use of Schinzel's hypothesis)

The starting point (already used by Heath-Brown in a special case) is to consider the equation

$$a_1x_1^3 + a_2x_2^3 = t = a_3x_3^3 + a_4x_4^3.$$

That is, one looks at the affine cone over the original cubic surface. Because the surface is diagonal, one may rewrite this cone (birationally) as the fibre product over $\mathbf{P}^1_k$ of two families of curves of genus one over $\mathbf{P}^1_k$, with bad reduction only at 0 and ∞. The generic fibre is the product of two curves of genus one.

The jacobian of each of these curves contains a *constant* torsion subgroup, namely μ_3. One then uses 3-isogenies, but simultaneously for each of the two curves of genus one.

Finding a $\lambda \in k^*$ such that the equation

$$a_1x_1^3 + a_2x_2^3 = \lambda = a_3x_3^3 + a_4x_4^3$$

has solutions in all k_v is easy. The hard work consists in finding such a λ for which the part of the (two) relevant Tate-Shafarevich groups killed by the 3-isogenies is too small to be nonzero. It is in this process that one has to impose that the ground field contain no nontrivial cube root of 1.