On cubic surfaces violating the Hasse principle

Jörg Jahnel

University of Siegen

University of Sydney, February/March, 2014

joint work with
Andreas-Stephan Elsenhans (University of Sydney)

Diophantine equations

Problem (Diophantine equation)

Given $f \in \mathbb{Z}[X_0, \ldots, X_n]$, describe the set

$$L(f) := \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid f(x_0, \ldots, x_n) = 0\}$$

explicitly.

Geometric Interpretation

- Integral points on an n-dimensional hypersurface in $\mathbf{A}^{n+1}$.
- If f is homogeneous: Rational points on an $(n-1)$-dimensional hypersurface V_f in $\mathbf{P}^n$.

Seemingly easier problem: Decide whether $L(f)$ is non-empty.

A statistical heuristics

Given a concrete (homogeneous) f, how many solutions do we expect?

Put $Q(B) := \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid |x_i| \leq B\}$. Then

$$\#Q(B) = (2B+1)^{n+1} \sim C_1 \cdot B^{n+1}.$$

On the other hand,

$$\max_{(x_0,\ldots,x_n)\in Q(B)} |f(x_0, \ldots, x_n)| \sim C_2 \cdot B^{\deg f}.$$

Heuristics

Assuming equidistribution of the values of f on $Q(B)$, we are therefore led to expect the asymptotics

$$\#\{(x_0, \ldots, x_n) \in V_f(\mathbb{Q}) \mid |x_0|, \ldots, |x_n| \leq B\} \sim C \cdot B^{n+1-\deg f}$$

for the number of solutions.

Statistical heuristics–Examples

The statistical heuristics explains the following well-known examples.

Examples

- $n + 1 - \deg f < 0$: Very few solutions.
  Example: $x^k + y^k = z^k$ for $k \geq 4$.
- $n + 1 - \deg f = 0$: A few solutions.
  Example: $y^2 z = x^3 + 8xz^2$.
  Elliptic curves.

  Another example: $x^4 + 2y^4 = z^4 + 4w^4$.
  $K3$ surfaces.
- $n + 1 - \deg f > 0$: Many solutions.
  Example: $x^2 + y^2 = z^2$.
  Conics.

  Another example: $x^3 + y^3 + z^3 + w^3 = 0$.
  Cubic surfaces.

Statistical heuristics–Geometric interpretation

If V_f is smooth then $\mathscr{O}(n+1-\deg f)|_{V_f}$ is exactly the anticanonical invertible sheaf on V_f. Thus, the three cases correspond to the three cases of the Kodaira classification.

Heuristics (Geometric interpretation)

- Kodaira-Dimension $\dim V_f$, Varieties of general type:
  Very few solutions.
- Kodaira-Dimension 0, Varieties of intermediate type:
  A few solutions.
- Kodaira-Dimension $-\infty$, Fano varieties:
  Many solutions.

Two types of complications

- Unsolvability
  - Unsolvability in reals,
    $x^2 + y^2 + z^2 = 0$.
  - p-adic unsolvability,
    $u^3 + 2v^3 + 7w^3 + 14x^3 + 49y^3 + 98z^3 = 0$.
- "Accumulating" subvarieties:

  $x^3 + y^3 = z^3 + w^3$ defines a cubic surface V in $\mathbf{P}^3$.

$$\#\{(x_0, \dots, x_n) \in V(\mathbb{Q}) \mid |x_0|, \dots, |x_n| \leq B\} \sim C \cdot B$$

is predicted.

However, V contains the line given by $x = z$, $y = w$, on which there is quadratic growth, already.

The Hasse principle

The picture is incomplete. More complications are possible.

Hasse principle (named after Helmut Hasse)

If $V_f(\mathbb{Q}_p) \neq \emptyset$ and $V_f(\mathbb{R}) \neq \emptyset$, then $V_f(\mathbb{Q}) \neq \emptyset$.

It may happen that the Hasse principle is violated. I.e., that $V_f(\mathbb{Q}_p) \neq \emptyset$ and $V_f(\mathbb{R}) \neq \emptyset$, but nevertheless $V_f(\mathbb{Q}) = \emptyset$.

- For varieties of general type, $V_f(\mathbb{Q}) = \emptyset$ is what one expects. Thus, one does not expect the Hasse principle.
- Concerning varieties of intermediate type, genus-1-curves that are counterexamples to the Hasse principle have been constructed by C.-E. Lind (1940, $2w^2 = x_0^4 - 17x_1^4$) and E. S. Selmer (1951, $3x_0^3 + 4x_1^3 + 5x_2^3 = 0$).
- But given a Fano variety, one might tend to expect the Hasse principle to be true.

The Hasse principle II

Theorem (Hasse-Minkowski)

Suppose f to be homogeneous of degree two. Then the Hasse principle holds for V_f.

Theorem (Hardy-Littlewood)

Let $d \geq 3$ be any integer. Then there exists a constant $N(d)$ such that $V_f(\mathbb{Q}) \neq \emptyset$ for every homogeneous form of degree d in at least $N(d)$ variables. The Hasse principle holds trivially.

Let now f be a homogeneous cubic in four variables. Then $C := V_f \subset \mathbf{P}^3$ is a cubic surface.

Theorem (Skolem 1955)

Let $C \subset \mathbf{P}^3$ be a singular *cubic surface. Then the Hasse principle holds for C.*

The geometry of smooth cubic surfaces

Let $C \subset \mathbf{P}^3$ be a smooth cubic surface over an algebraically closed field.

Classical algebraic geometry gives us a lot of information about such surfaces. For instance,

- C is isomorphic to $\mathbf{P}^2$, blown up in six points. These are in general position.
- C contains precisely 27 lines.
- The configuration of the 27 lines is highly symmetric. The group of all permutations respecting the intersection pairing is isomorphic to the Weyl group $W(E_6)$ of order 51 840.
- There is a pentahedron associated with general C (Sylvester).
- There are (at least) two kinds of moduli spaces, coming out of the classical invariant theory.
    - The coarse moduli space of smooth cubic surfaces (Salmon, Clebsch).
    - The fine moduli space of *marked cubic surfaces* (Cayley, Coble).

The 27 lines

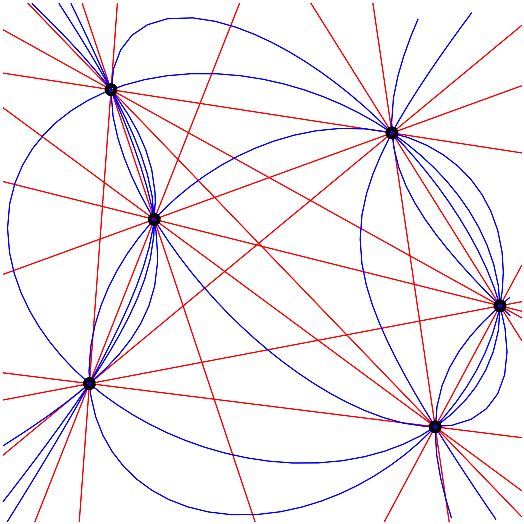

Figure: The 27 lines in the blown-up model

Classical counterexamples

Theorem (Swinnerton-Dyer 1962)

Let $K/\mathbb{Q}$ be the unique cubic field extension contained in the cyclotomic extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. Put $\theta := \mathrm{Tr}_{\mathbb{Q}(\zeta_7)/K}(\zeta_7 - 1)$ and let C be the cubic surface, given by

$$\begin{aligned} x_3(x_0 + x_3)(x_0 + 2x_3) &= \mathrm{N}_{K/\mathbb{Q}}(x_0 + \theta x_1 + \theta^2 x_2) \\ &= x_0^3 - 7x_0^2 x_1 + 21x_0^2 x_2 + 14x_0 x_1^2 - 77x_0 x_1 x_2 \\ &\qquad + 98x_0 x_2^2 - 7x_1^3 + 49x_1^2 x_2 - 98x_1 x_2^2 + 49x_2^3 \,. \end{aligned}$$

Then C violates the Hasse principle.

Remark

Swinnerton-Dyer's example was soon generalized by L. J. Mordell. He gave two families of counterexamples, one using norm forms from the cubic subfield of $\mathbb{Q}(\zeta_7)$, the other from the cubic subfield of $\mathbb{Q}(\zeta_{13})$.

The three linear forms on the left hand side were always linearly dependent.

Classical counterexamples II

Theorem (Cassels/Guy 1966)

Let C be the cubic surface given by

$$5x_0^3 + 12x_1^3 + 9x_2^3 + 10x_3^3 = 0\,.$$

Then C violates the Hasse principle.

Remark

This is the historically first example of a diagonal cubic surface violating the Hasse principle.

The arithmetic of diagonal cubic surfaces was systematically investigated by J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc in 1985. More counterexamples to the Hasse principle were found, but also evidence that a general diagonal cubic surface fulfills the Hasse principle (but not weak approximation).

A further generalization of Mordell's counterexamples

Theorem (J. 2007)

Let $p \equiv 1 \pmod 3$ *be any prime,* K *the cubic subfield of* $\mathbb{Q}(\zeta_p)$*, and* $\theta := \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p - 1)$*. For* a_1, a_2, d_1, d_2 *integers, consider the cubic surface* $X \subset \mathbf{P}^3_{\mathbb{Q}}$*, given by*

$$x_3(a_1x_0 + d_1x_3)(a_2x_0 + d_2x_3) = \mathrm{N}_{K/\mathbb{Q}}\big(x_0 + \theta x_1 + \theta^2 x_2\big)\,.$$

1. *Assume* $p \nmid d_1d_2$*, that* $\gcd(a_1, d_1)$ *and* $\gcd(a_2, d_2)$ *contain only prime factors that decompose in* K*, and that among the zeroes* z_1*,* z_2*,* z_3 *of* $T(a_1 + d_1T)(a_2 + d_2T) - 1 = 0$*, at least one is simple and in* $\mathbb{F}_p$*. Then,* $X(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$*.*
2. *Suppose* $p \nmid d_1d_2$ *and* $\gcd(d_1, d_2) = 1$*. Then, for every point* $(t_0 : t_1 : t_2 : t_3) \in X(\mathbb{Q})$*,* $s := (t_3/t_0 \mod p)$ *admits the property that* $\frac{a_1+d_1s}{s}$ *is a cube in* $\mathbb{F}_p^*$*.*
   In particular, if $\frac{a_1+d_1s_i}{s_i} \in \mathbb{F}_p^*$ *is a non-cube for every* i *such that* $s_i \in \mathbb{F}_p$ *then* $X(\mathbb{Q}) = \emptyset$*.*

The method of the proof

- Write the equation of C as $l_1 l_2 l_3 = \mathrm{N}_{L/K}(l)$ for linear forms l, l_1, l_2, l_3 and L/K a cubic Galois extension. (K is an extension of $\mathbb{Q}$ in the diagonal case).
- Ensure that no K-rational point is contained in the three planes $l_i = 0$. ($l_i = 0$ implies $l^{\sigma_1} = l^{\sigma_2} = l^{\sigma_3} = 0$. I.e., check that the four linear forms are linearly independent.)
- Prove that, for every prime $\mathfrak{p}$ of K, the norm residue symbol

$$s_{\mathfrak{p}} := \left(\tfrac{l_1(x)}{l_2(x)}, L_{\mathfrak{p}}/K_{\mathfrak{p}}\right) \in \tfrac{1}{3}\mathbb{Z}/\mathbb{Z}$$

  is independent of the choice of $x \in C(K_{\mathfrak{p}})$.
- Observe that

$$\textstyle\sum_{\mathfrak{p}} s_{\mathfrak{p}} \neq 0 \in \tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\,,$$

  in contradiction with global class field theory.

Manin's interpretation

Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. Then the cyclic $K(C)$-algebra

$$\mathscr{A} = (L(C), \sigma, \tfrac{l_1}{l_2}) := L1 \oplus Lu \oplus Lu^2,$$

for u a formal symbol and the relations $u^3 = \frac{l_1}{l_2}$ as well as $ux = \sigma(x)u$ for all $x \in L(C)$, is an Azumaya algebra over $K(C)$.

Observation

The Azumaya algebra $\mathscr{A}$ extends to an Azumaya algebra over the whole scheme C.

The reason is that $\div(\frac{l_1}{l_2})$ is the norm of a (non-principal) divisor. Observe that $(L(C), \sigma, \frac{l_1}{l_2})$ and $(L(C), \sigma, \frac{l_1}{l_2} \cdot \mathrm{N}_{L(C)/K(C)}(\varphi))$ are isomorphic algebras.

The Brauer group

Definition

Let S be any scheme. Then the (cohomological) *Brauer group* of S is defined by $\mathrm{Br}(S) := H^2_{\text{ét}}(S, \mathbb{G}_m)$.

Remarks

1. This definition is not very explicit. In general, Brauer groups are not easily computable.
2. One has $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and
$$\mathrm{Br}(\mathbb{Q}) = \ker(\mathrm{sum}\colon \bigoplus_{p \in \{2,3,5,\dots\}} \mathrm{Br}(\mathbb{Q}_p) \oplus \bigoplus_{\nu\colon K \to \mathbb{R}} \mathrm{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}).$$
3. Let $\alpha \in \mathrm{Br}(S)$ be any Brauer class. Then, for every K-rational point $p \in S(K)$, there is $\alpha|_p \in \mathrm{Br}(\operatorname{Spec} K)$.

   Hence, an adelic point *not* fulfilling the condition that the sum zero cannot be approximated by $\mathbb{Q}$-rational points.

   This is called the *Brauer-Manin obstruction* to weak approximation.

The Brauer group II

The cohomological Brauer group of a variety S over a field k is equipped with a canonical filtration, defined by the Hochschild-Serre spectral sequence.

1. $\mathrm{Br}_0(S) \subseteq \mathrm{Br}(S)$ is the image of $\mathrm{Br}(k)$ under the natural map. At least when S has a k-rational point, $\mathrm{Br}_0(S) \cong \mathrm{Br}(k)$. $\mathrm{Br}_0(S)$ does not contribute to the Brauer-Manin obstruction.
2. One has

   $$\mathrm{Br}_1(S)/\,\mathrm{Br}_0(S) \cong H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), \mathrm{Pic}(S_{k^{\mathrm{sep}}}))\,.$$

   This subquotient is called the algebraic part of the Brauer group. For k a number field, it is responsible for the so-called *algebraic* Brauer-Manin obstruction.
3. Finally, $\mathrm{Br}(S)/\,\mathrm{Br}_1(S)$ injects into $\mathrm{Br}(S_{k^{\mathrm{sep}}})$. This quotient is called the transcendental part of the Brauer group. For k a number field, the corresponding obstruction is called a *transcendental* Brauer-Manin obstruction.

The Brauer group of a smooth cubic surface

Lemma

Let C be a smooth cubic surface over an algebraically closed field. Then $\mathrm{Br}(C) = 0$.

Idea of proof. One has $\mathrm{Br}(\mathbf{P}^2) = 0$ and a blow-up does not change the Brauer group.

Corollary

Let C be a smooth cubic surface over a field k of characteristic zero.

- *Then the transcendental part $\mathrm{Br}(C)/\mathrm{Br}_1(C)$ of the Brauer group vanishes.*
- *The canonical map*

$$\delta\colon H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Pic}(C_{\overline{k}})) \longrightarrow \mathrm{Br}(C)/\mathrm{Br}(k)$$

  is an isomorphism.

The Brauer group of a smooth cubic surface II

Theorem (Manin 1969)

Let C be a smooth cubic surface over a field k. Then

$$H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Pic}(C_{\overline{k}})) \cong \mathrm{Hom}((NF \cap F_0)/NF_0, \mathbb{Q}/\mathbb{Z})$$

Here, $F \subset \mathrm{Div}(C)$ is the subgroup generated by the 27 lines on C. $F_0 \subset F$ is the subgroup of all principal divisors in F.

Thus, the $\mathrm{Gal}(\overline{k}/k)$-module structure on $F \cong \mathbb{Z}^{27}$, i.e. the Galois operation on the 27 lines, determines the Brauer group $\mathrm{Br}(C)/\mathrm{Br}(k)$ completely.

Remark

$\mathrm{Gal}(\overline{k}/k)$ permutes the 27 lines in such a way that the intersection matrix is respected. Thus, every smooth cubic surface over k defines a homomorphism $\varrho\colon \mathrm{Gal}(\overline{k}/k) \to W(E_6) \subseteq S_{27}$. The subgroup $\mathrm{im}\,\varrho$ determines the Brauer group.

Systematic computation

There are 350 conjugacy classes of subgroups in $W(E_6)$.

It turns out that $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Pic}(C_{\overline{k}}))$ is isomorphic to

0	for 257 classes,
$\mathbb{Z}/2\mathbb{Z}$	for 65 classes,
$\mathbb{Z}/3\mathbb{Z}$	for 16 classes,
$(\mathbb{Z}/2\mathbb{Z})^2$	for 11 classes,
$(\mathbb{Z}/3\mathbb{Z})^2$	for one class.

Today, this is a very simple computation using `gap` or `magma`.

The result that only these five groups occur was proven by Sir Peter Swinnerton-Dyer in 1993.

Colliot-Thélène's conjecture

Conjecture (Colliot-Thélène 1985)

The Brauer-Manin obstruction is the only obstruction to the Hasse principle for smooth cubic surfaces over a number field k.

For $k = \mathbb{Q}$, this means that if $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(C)} \neq \emptyset$ then we expect $C(\mathbb{Q}) \neq \emptyset$.

Corollary (from Colliot-Thélène's conjecture)

Only the cases that

$$\mathrm{Br}(C)/\,\mathrm{Br}(k) \cong \mathbb{Z}/3\mathbb{Z} \quad \textit{or} \quad \mathrm{Br}(C)/\,\mathrm{Br}(k) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

have the potential to violate the Hasse principle.

Proof. In the other cases, all Brauer classes split after a suitable quadratic or biquadratic extension l of k. As one may suppose $C(\mathbb{A}_k) \neq \emptyset$, the conjecture shows $C(l) \neq \emptyset$. But, for cubic surfaces, $C(k(\sqrt{d})) \neq \emptyset \Longrightarrow C(k) \neq \emptyset$. $\square$

Steiner trihedra

Definition

Let C be smooth cubic surface.

1. Three tritangent planes such that no two of them have one of the 27 lines in common are said to be a *trihedron*.

   If there exists another trihedron defining the same nine lines then one speaks of a *Steiner trihedron*.

2. A *triplet* (T_1, T_2, T_3) is a decomposition of the 27 lines into three subsets T_1, T_2, T_3 of nine lines each such that every T_i is defined by a Steiner trihedron.

Remarks

1. There are 72 Steiner trihedra on each smooth cubic surface, forming 36 pairs.
2. Every pair of Steiner trihedra corresponds to a way of writing C in the *Cayley-Salmon form*

$$l_1 l_2 l_3 = l_4 l_5 l_6 \, .$$

Steiner trihedra II

Proposition (E.+J. 2009)

Let C be a smooth cubic surface over a field k such that $\mathrm{Br}(C)/\mathrm{Br}(k)$ *has an element of order three.*

Then C has a triplet (T_1, T_2, T_3) consisting of Galois invariant sets.

Idea of proof. Among the subgroup classes of $W(E_6)$ such that $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Pic}(C_{\overline{k}}))$ has an element of order three, there is unique maximal one. That stabilizes a triplet. □

Consequence

After a suitable extension of the base field, every cubic surface such that $\mathrm{Br}(C)/\mathrm{Br}(k)$ *is of exponent three has the form*

$$l_1 l_2 l_3 = \mathrm{N}(l).$$

Eckardt points

The geometry of the 27 lines on a smooth cubic surface is very rigid.

There are 45 tritangent planes. The intersection matrix is the same for all smooth cubic surfaces.

But there are two ways a tritangent plane may look like.

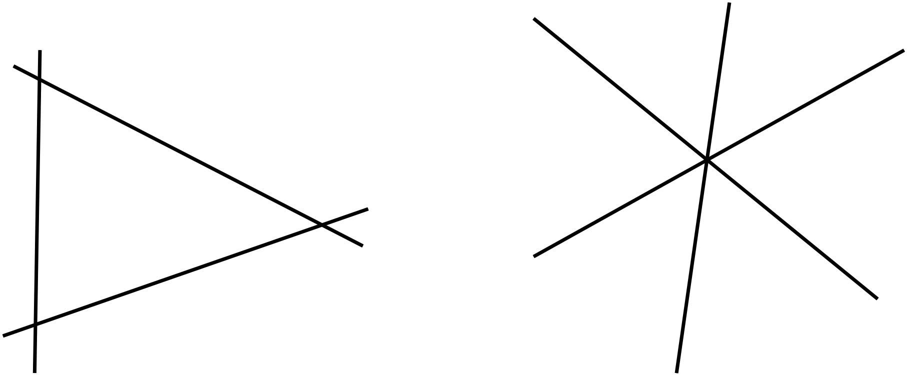

Figure: An ordinary tritangent plane (left) and one with an Eckardt point (right)

Eckardt points II

Facts (well-known in the 19th century)

- *A smooth cubic surface may have no, 1, 2, 3, 4, 6, 9, 10, or 18 Eckardt points.*
  - *A generic cubic surface has no Eckardt point.*
  - *To have an Eckardt point is a codimension one condition in moduli space.*
  - *To have at least two Eckardt points is a codimension two condition in moduli space.*
- *The existence of an Eckardt point is equivalent to the cubic surface having a non-trivial automorphism.*

Eckardt points III

Fact

1. *The Swinnerton-Dyer-Mordell type surfaces are contained in a two-dimensional closed subscheme of the moduli space.*
2. *Diagonal cubic surfaces correspond to a single moduli point.*

Idea of 1. They have three Eckardt points.

The equations are of the form

$$x_3(a_1x_0 + d_1x_3)(a_2x_0 + d_2x_3) = \mathrm{N}_{K/\mathbb{Q}}(x_0 + \theta x_1 + \theta^2 x_2)\,.$$

The three tritangent planes $V(x_3)$, $V(a_1x_0 + d_1x_3)$, and $V(a_2x_0 + d_2x_3)$ have a line in common. Thus, on each of the three tritangent planes $V(x_0 + \theta^{\sigma_i}x_1 + (\theta^{\sigma_i})^2x_2)$, the corresponding three lines meet at a single point. $\square$

Remark

Diagonal cubic surfaces have 18 Eckardt points.

Our family

The family

We consider the cubic surface C over $\mathbb{Q}$, given by the equation

$$x_0x_1x_2 = \mathrm{N}_{K/\mathbb{Q}}(ax_0 + bx_1 + cx_2 + dx_3)\,, \tag{1}$$

for $K/\mathbb{Q}$ a cyclic cubic field extension and $a, b, c, d \in K$.

There is only one change in comparison with the Swinnerton-Dyer-Mordell type surfaces. The three linear forms on the left hand side are now linearly independent.

Inert primes

Proposition (Inert primes)

Let l be a prime that is inert in $K/\mathbb{Q}$. Denote by w the unique prime of K lying above l and assume that

- $a, b, c \in \mathscr{O}_{K_w}$, $d \in \mathscr{O}_{K_w}^*$,
- $(a/d \bmod l), (b/d \bmod l), (c/d \bmod l) \in \mathbb{F}_{l^3}$ *are not contained in* $\mathbb{F}_l$.

Finally, let C denote the surface (1).

For any $(t_0 : t_1 : t_2 : t_3) \in C(\mathbb{Q}_l)$ such that $t_0 t_1 \neq 0$, the quotient $t_1/t_0 \in \mathbb{Q}_l$ is in the image of the norm map $N\colon K_w \to \mathbb{Q}_l$.

Idea of proof. Normalize coordinates such that $t_0, \ldots, t_3 \in \mathbb{Z}_l$ and at least one of them is a unit. Have to show that $\nu_l(t_1/t_0)$ is divisible by three.

Assume the contrary. Then, as the equation of the surface ensures that $3|\nu_l(t_0 t_1 t_2)$, the values $\nu_l(t_i)$, for $i = 0, 1, 2$, must be mutually non-congruent modulo 3.

Inert primes II

First case: There is no unit among t_0, t_1, t_2.
Then t_3 is a unit. As d is a unit, we have that $at_0 + bt_1 + ct_2 + dt_3 \in \mathscr{O}_{K_w}^*$. Hence, $\mathrm{N}_{K_w/\mathbb{Q}_l}(at_0 + bt_1 + ct_2 + dt_3) \in \mathbb{Z}_l^*$, which, in view of $t_0 t_1 t_2$ not being a unit, contradicts the equation of the surface.

Second case: There is exactly one unit among t_0, t_1, t_2.
Without restriction, assume that t_0 is the unit. Again, $t_0 t_1 t_2$ is not a unit. The equation of the surface requires that $\mathrm{N}_{K_w/\mathbb{Q}_l}(at_0 + bt_1 + ct_2 + dt_3)$ must be a non-unit.

To ensure this, we need $at_0 + bt_1 + ct_2 + dt_3 \notin \mathscr{O}_{K_w}^*$, which means nothing but

$$at_0 + dt_3 \equiv 0 \pmod{l}.$$

But then $a/d \equiv -t_3/t_0 \pmod{l}$, a contradiction as the right hand side modulo l is in $\mathbb{F}_l$, but the left hand side is not. □

Ramification

Lemma

Let $l \neq 3$ be a prime number and consider the nodal cubic curve E over $\mathbb{F}_l$, defined by

$$27x_0x_1x_2 = (x_0 + x_1 + x_2)^3 \,.$$

Then, for every $\mathbb{F}_l$-rational point $(t_0 : t_1 : t_2)$ on E, at least one of the expressions t_1/t_0, t_2/t_1, and t_0/t_2 is properly defined and non-zero in $\mathbb{F}_l$. Further, these quotients evaluate solely to cubes in $\mathbb{F}_l^*$.

Idea of proof. The first assertion simply says that $(1:0:0)$, $(0:1:0)$, $(0:0:1) \notin E$. Further, in $\mathbb{Z}[T_0, T_1, T_2]$, the polynomial expression

$$(T_0^2 + 2T_0T_1 + T_1^2 + 5T_0T_2 - 4T_1T_2 - 5T_2^2)^3 + 729T_0(T_1 - T_2)^3T_2^2$$

splits into two factors, one of which is $27T_0T_1T_2 - (T_0 + T_1 + T_2)^3$.

For $(t_0 : t_1 : t_2) \in E(\mathbb{F}_l)$ with $t_2 \neq 0$, we see that t_0/t_2 is a cube, except possibly for the case when $t_1 = t_2$. But then the equation of the curve shows that $t_0/t_2 = (\frac{t_0+2t_2}{3t_2})^3$. □

Ramification II

Proposition

Let $l \neq 3$ be prime that is ramified in $K/\mathbb{Q}$. Denote by $\mathfrak{p}$ the unique prime of K lying above l and assume that

- $a \in \mathscr{O}_{K_\mathfrak{p}}, (a \bmod \mathfrak{p}) = \frac{\alpha}{3}$,
- $b \in \mathscr{O}_{K_\mathfrak{p}}, (b \bmod \mathfrak{p}) = \frac{1}{3}$,
- $c \in \mathscr{O}_{K_\mathfrak{p}}, (c \bmod \mathfrak{p}) = \frac{1}{3\alpha}$,
- $d \in \mathfrak{p} \backslash \mathfrak{p}^3$.

for some non-cube $\alpha \in \mathbb{F}_l^*$. Finally, let C denote the surface (1).

Let $(t_0 : t_1 : t_2 : t_3) \in C(\mathbb{Q}_l)$ be any point. If, for $0 \leq i < j \leq 2$, one has $t_i t_j \neq 0$ then the quotient $t_j/t_i \in \mathbb{Q}_l$ is not *in the image of the norm map* $\mathrm{N}\colon K_\mathfrak{p} \to \mathbb{Q}_l$.

Idea of proof. The reduction of C is non-trivial twist of the nodal cubic curve considered in the lemma. No l-adic point reduces to the cusp $(0 : 0 : 0 : 1)$. $\square$

New counterexamples to the Hasse principle

Theorem (E.+J. 2013)

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ and $z = \zeta_7 + \zeta_7^{-1} - 2$. Write $\mathfrak{p}$ for the unique prime lying above (7). Suppose that $a, b, c, d \in \mathscr{O}_K$ satisfy the following conditions.

1. *d splits as $(d) = \mathfrak{p}\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$, where $\mathrm{N}(\mathfrak{p}_i)$ are prime numbers $\neq (7)$. I.e., (d) does not contain any inert prime and contains $\mathfrak{p}$ exactly once.*
2. *$a/d = \frac{1}{7}(a_0 + a_1 z + a_2 z^2)$ for $a_i \in \mathbb{Z}$ and $\gcd(a_1, a_2)$ is a product of only split primes.*
   - *$b/d = \frac{1}{7}(b_0 + b_1 z + b_2 z^2)$ for $b_i \in \mathbb{Z}$ and $\gcd(b_1, b_2)$ is a product of only split primes.*
   - *$c/d = \frac{1}{7}(c_0 + c_1 z + c_2 z^2)$ for $c_i \in \mathbb{Z}$ and $\gcd(c_1, c_2)$ is a product of only split primes.*
3. *$a \equiv b \pmod 6$.*
4. *$a \equiv -1 \pmod{\mathfrak{p}}$, $b \equiv -2 \pmod{\mathfrak{p}}$, and $c \equiv -4 \pmod{\mathfrak{p}}$.*

Finally, let C denote the surface (1). Then $C(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ but $C(\mathbb{Q}) = \emptyset$.

Idea of proof. Step 1: Existence of l-adic points for every l.

This is clear for split primes and $l = \infty$, as we have the form $x_0x_1x_2 = l_1l_2l_3$.

For the other primes, use Hensel's lemma. It suffices to show that C_l has a non-singular $\mathbb{F}_l$-rational point. For this, we show that $(C_l)_{\text{sing}}$ is of dimension zero. Thus, $\#(C_l)_{\text{reg}}(\mathbb{F}_l) \geq l^2 - 3l - 3 > 0$ for $l \geq 5$.

The assumption $a \equiv b \pmod 6$ ensures that $(1 : (-1) : 0 : 0) \in C_l(\mathbb{F}_l)$ is a non-singular point for $l = 2, 3$.

Step 2: Non-existence of $\mathbb{Q}$-rational points.

Use the sum relation form from class field theory. Apply Propositions above.

Assumptions: $\frac{1}{3} \equiv -2 \pmod 7$, $\alpha := \frac{1}{2} \equiv 4 \pmod 7$ is a non-cube.

l inert $\Longrightarrow$ $a/d = \frac{1}{7}(a_0 + a_1z + a_2z^2)$ for a_0, a_1 not both divisible by l. Hence, $(a/d \bmod l) \in \mathbb{F}_{l^3} \backslash \mathbb{F}_l$. $\square$

An example

Example

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $z := \zeta_7 + \zeta_7^{-1} - 2$, and let C be the cubic surface over $\mathbb{Q}$, given by the equation $x_0x_1x_2 = \mathrm{N}_{K/\mathbb{Q}}(ax_0 + bx_1 + cx_2 + dx_3)$, for

$$a := -1, \quad b := 5 + 6z^2, \quad c := 3 + z^2, \quad d := z\,.$$

Then C violates the Hasse principle.

Indeed,

1. $d = z$ for $(z) = \mathfrak{p}$, (no further factors).
2. $a/d = \frac{1}{7}(14 + 7z + z^2)$,
   $b/d = \frac{1}{7}(-70 + 7z - 5z^2)$,
   $c/d = \frac{1}{7}(-42 - 14z - 3z^2)$,
   $\gcd(7,1) = \gcd(7,-5) = \gcd(-14,-3) = 1$.
3. $a \equiv b \pmod 6$.
4. $a \equiv -1 \pmod z$, $b \equiv -2 \pmod z$, $c \equiv -4 \pmod z$. $\square$

An example II

The equation of C is, in explicit form,

$$x_0^3 - 141x_0^2x_1 - 30x_0^2x_2 + 7x_0^2x_3 + 4863x_0x_1^2 + 2233x_0x_1x_2 - 532x_0x_1x_3 + 251x_0x_2^2 - 119x_0x_2x_3 + 14x_0x_3^2 - 31499x_1^3 - 26286x_1^2x_2 + 6013x_1^2x_3 - 6799x_1x_2^2 + 3157x_1x_2x_3 - 364x_1x_3^2 - 559x_2^3 + 392x_2^2x_3 - 91x_2x_3^2 + 7x_3^3 = 0\,.$$

C has bad reduction at 2, 3, 7, 3739, and 7589.

$S_{\mathbb{F}_2}$: binode;
$S_{\mathbb{F}_7}$: cone over a nodal cubic;
other three: conical

A minimization algorithm yields a reembedding of C as the surface, given by the equation

$$-x_0^3 + 2x_0^2x_1 - x_0^2x_2 - 5x_0^2x_3 + x_0x_1^2 - x_0x_1x_2 + 7x_0x_1x_3 + 2x_0x_2^2 - 15x_0x_2x_3 - 11x_0x_3^2 - x_1^3 - 2x_1^2x_2 + 9x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^3 + x_2^2x_3 + 8x_2x_3^2 - x_3^3 = 0\,.$$

Congruence conditions

Corollary

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$*,* $l \equiv \pm 1 \pmod 7$ *be a prime number, and* $\widetilde{a}, \widetilde{b}, \widetilde{c}, \widetilde{d}$ *be four residue classes in* $[\mathscr{O}_K/(l)]^* \cong (\mathbb{F}_l^*)^3$*.*

Then there exists a cubic surface C *that is a counterexample to the Hasse principle, of the form*

$$x_0 x_1 x_2 = \mathrm{N}_{K/\mathbb{Q}}(a x_0 + b x_1 + c x_2 + d x_3)\,,$$

for $a, b, c, d \in \mathscr{O}_K$ *such that* $(a \bmod (l)) = \widetilde{a}$*, ...,* $(d \bmod (l)) = \widetilde{d}$*.*

Congruence conditions II

Idea of proof. This looks like infinitely many congruences ...

- d: Choose solution $d' \in \mathscr{O}_K$ of

$$(d' \bmod (l)) = \widetilde{d}, \quad d' \equiv z \pmod{(7)}.$$

  Partial factorization $(d') = \mathfrak{p}\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \cdot (m')$, the $\mathfrak{p}_i$ being factors in K of split primes and $m' > 0$ a product of inert primes.

  Choose prime $m \equiv m' \pmod{l}$, $m \equiv \pm 1 \pmod{7}$, and put $d := m \cdot \frac{d'}{m'}$.

- c: $c \equiv -4 \pmod{\mathfrak{p}}$ is equivalent to $7c/d \equiv \gamma z^2 \pmod{(7)}$ for some $\gamma \in \{1, \ldots, 6\}$. Thus choose solution $c' = c_0' + c_1' z + c_2' z^2 \in \mathscr{O}_K$ of

$$(c' \bmod (l)) = 7\widetilde{c}\widetilde{d}^{-1}, \quad c' \equiv \gamma z^2 \pmod{(7)}$$

  and put $c := \frac{c'}{7} \cdot d$.

  Assure $\gcd(c_1', c_2') = 1$ by choosing c_2 as a prime number.

- b and a: Analogous to c. $\square$

Zariski density

Theorem (E.+J. 2013)

The cubic surfaces over $\mathbb{Q}$ that are counterexamples to the Hasse principle define a Zariski dense subset of the moduli scheme of smooth cubic surfaces.

Idea of proof. Over an algebraically closed field, every smooth cubic surface may be brought into Cayley-Salmon form $l_1 l_1 l_3 = l_4 l_5 l_6$. Hence, the morphism

$$p\colon \mathbf{A}^{12} \longrightarrow \mathscr{M}$$

$$(a_{10}, \ldots, a_{33}) \;\mapsto\; [C_a\colon x_0 x_1 x_2 = (a_{10}x_0 + \ldots + a_{13}x_3)(a_{20}x_0 + \ldots + a_{23}x_3)(a_{30}x_0 + \ldots + a_{33}x_3)]$$

to the moduli scheme is dominant.

Suppose the counterexamples to the Hasse principle were contained in a proper, Zariski closed subset $H \subset \mathscr{M}$. Then all the counterexamples, we constructed, must be contained in $p^{-1}(H) \subset \mathbf{A}^{12}$, which is a proper, Zariski closed subset. I.e., in a hypersurface $V \subset \mathbf{A}^{12}$ of a certain degree d.

Then $V(\mathbb{F}_l) \leq dl^{11}$ for every prime l. But the counterexamples constructed

Thanks

Thank you!!