Rational and integral points on higher dimensional varieties

The American Institute of Mathematics

This is a hard–copy version of a web page available through http://www.aimath.org
Input on this material is welcomed and can be sent to `workshops@aimath.org`
Version: Mon Nov 22 11:41:01 2004

This document is an outcome of the ARCC workshop "Rational and Integral Points on Higher Dimensional Varieties," held at AIM in Palo Alto, December 11-20, 2002.

The lecture notes and problem list were primarily provided by John Voight and William McCallum. The glossary, photographs, and the overall arrangement of material was provided by William Stein.

Table of Contents

Notes of selected lectures, by John Voight.

A.1 Colliot-Thelene 1: Rational points on surfaces with a pencil of curves of genus one

Symmetrizing the Computation of the Selmer Group

Let k be a field, $\operatorname{char} k = 0$, $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ an elliptic curve with $e_i \in k$ so that all 2-torsion of E is rational. We have the exact sequence

$$0 \to E[2] \to E \xrightarrow{2} E \to 0$$

where $E[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. 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-*coverings*: that is, given $(\alpha_1, \alpha_2) \in (k^*/k^{*2})^2$, we have the 2-cover defined by the 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 principal homogeneous spaces.

Now let k be a number field, Ω the set of places of k. We have the diagram

$$\begin{tikzcd}
 & & \mathrm{Sel}(E,2) \arrow[r] \arrow[d] & Ш^2(k,E)[2] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(k)/2E(k) \arrow[r] \arrow[urr] \arrow[d] & H^1(k,E[2]) \arrow[r] \arrow[d] & H^1(k,E)[2] \arrow[r] \arrow[d] & 0 \\
 & \prod_{v\in\Omega} E(k_v)/2E(k_v) \arrow[r] & \prod_v H^1(k_v,E[2]) \arrow[r] & \prod_v H^1(k_v,E)[2] \arrow[r] & 0
\end{tikzcd}$$

so $\mathrm{Sel}(E, 2)$ gives 2-covers with points everywhere locally, and $Ш^2(k, E)$ measures the difference.

Over a local field, we have a pairing

$$H^1(k_v, E[2]) \times H^1(k_v, E[2]) \to H^2(k_v, \mu_2)$$

induced by the Weil pairing, which is nondegenerate and alternating, so that $(x, x) = 0$.

Fact (Tate). $E(k_v)/2E(k_v) \hookrightarrow H^1(k_v, E[2])$ is maximal isotropic for the above pairing.

If E/k has good reduction at k_v, then $E(k_v)/2E(k_v) = E(\mathcal{O}_v)/2E(\mathcal{O}_v) \simeq H^1(\mathcal{O}_v, E[2])$, which is $(\mathcal{O}_v^*/\mathcal{O}_v^{*2})^2 \subset (k_v^*/k_v^{*2})^2$, the maximal isotropic subgroup.

Suppose $S \subset \Omega$ is a finite set of places, and suppose S contains the primes above $\infty, 2$, and the primes of bad reduction. Then

$$\begin{tikzcd}
\bigoplus_{v\in S} E(k_v)/2E(k_v) \arrow[d] & \times & H^1(\mathcal{O}_S, E[2]) \arrow[d, "i"] \arrow[drr, "e"] & & \\
\bigoplus_{v\in S} H^1(k_v, E[2]) & \times & \bigoplus_{v\in S} H^1(k_v, E[2]) \arrow[rr, "\sum e_v"] & & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

Then $\mathrm{Sel}(E, 2)$ is the right kernel of e.

Fact. If $\mathrm{Cl}(\mathcal{O}_S) = 0$, then i is injective.

This follows from class field theory. So we choose S_0 such that $\mathrm{Cl}(\mathcal{O}_{S_0}) = 0$, and take $S \supset S_0$. If $\mathrm{Cl}(\mathcal{O}_S) = 0$, i is an injection, and the image of i is a maximal isotropic subgroup of $V_S = \bigoplus_{v \in S} V_v$, $V_v = H^1(k_v, E[2])$.

What we have achieved: the Selmer group $\mathrm{Sel}(E, 2)$ is now a kernel of 'a square matrix', since $\bigoplus_{v \in S} E(k_v)/2E(k_v)$ and $H^1(\mathcal{O}_S, E[2])$ have the same dimension over $\mathbb{F}_2$. Letting $\mathfrak{h}(A) = (A^*/A^{*2})^2$, we have

$$W_S \times \mathfrak{h}(\mathcal{O}_S) \to \mathbb{Z}/2\mathbb{Z}$$

where

$$W_S = \bigoplus_{v \in S} W_v,\ W_v = E(k_v)/2E(k_v).$$

Proposition. *Assume $S \supset S_0$ (containing primes above $\infty, 2$ and those of bad reduction and such that $\mathrm{Cl}(\mathcal{O}_{S_0}) = 0$) is a finite set of places. Suppose that $\mathfrak{h}(\mathcal{O}_S) \subset V_S$ is a maximal isotropic subgroup. Then there exist $K_v \subset V_v$ for $v \in S$ maximal isotropic such that $K_v = \mathfrak{h}(\mathcal{O}_v)$ for $v \in S \setminus S_0$, and*

$$\mathfrak{h}(\mathcal{O}_S) \oplus \bigoplus_{v \in S} K_v = V_S.$$

This is purely a result in linear algebra.

Recall we have $W_S \times \mathfrak{h}(\mathcal{O}_S) \to \mathbb{Z}/2\mathbb{Z}$ from $W_S \subset V_S$ and $\mathfrak{h}(\mathcal{O}_S) \subset V_S$.

Definition. We let $\mathrm{Sel}(E, 2) \subset \mathcal{I}^S \subset \mathfrak{h}(\mathcal{O}_S)$, where

$$\mathcal{I}^S = \{\xi \in \mathfrak{h}(\mathcal{O}_S) : \text{for all } v \in S,\ \xi \in K_v + W_v\}.$$

We let

$$\mathcal{W}_S = \bigoplus_{v \in S} W_v/(W_v \cap K_v).$$

We then have a pairing

$$\mathcal{W}_S \times \mathcal{I}^S \xrightarrow{e_S} \mathbb{Z}/2\mathbb{Z}.$$

Proposition. *The Selmer group is the kernel of e_S. The map $\tau : \mathcal{I}^S \simeq \mathcal{W}_S$ is an isomorphism. For $\mu \in \mathcal{I}^S$, we define a map*

$$\mu = \textstyle\sum_{v \in S} \alpha_v + \beta_v \mapsto \sum_{v \in S} \alpha_v;$$

via τ, the new pairing $\mathcal{W}_S \times \mathcal{I}^S \to \mathbb{Z}/2\mathbb{Z}$ is symmetric.

Example. For $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$, $e_i \in \mathcal{O}_v$, $v(\prod(e_i - e_j)) = 1$ (reduction is of type I_2). Then

$$\begin{tikzcd} E(k_v)/2E(k_v) \arrow[r] \arrow[dr] & (k_v^*/k_v^{*2})^2 \arrow[d] \\ E(k_v)[2] \arrow[u] \arrow[r, two heads] & \mathbb{Z}/2\mathbb{Z} \subset (\mathbb{Z}/2\mathbb{Z})^2 \end{tikzcd}$$

Here $W_v/(W_v \cap K_v) = \mathbb{Z}/2\mathbb{Z}$, $W_v \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Algebraico-Geometric version of Selmer group

Let k be a field, $\mathrm{char}\, k = 0$, $E : y^2 = (x - c_1(t))(x - c_2(t))(x - c_3(t))$, so E is defined over $F = k(t)$. To simplify, we assume that all $p_i = c_i - c_j$ are of the same even degree. We also assume that $r(t) = \prod(c_i - c_j)$ is separable, $r(t) = \rho \prod_{M \in \mathcal{M}} r_M(t)$ where $\rho \in k^*$, r_M monic irreducible, so E has reduction type I_2.

Now assume k is a totally imaginary number field. The Neron model $\mathcal{E}/\mathbb{P}^1$ has

$$0 \to \mathcal{E}^* \to \mathcal{E} \to \bigoplus_{M\in\mathcal{M}} i_{M*}\mathbb{Z}/2\mathbb{Z} \to 0.$$

Let $V \subset \mathbb{A}^1 = \operatorname{Spec} k(t)$ be $V = \mathbb{A}^1 \setminus \{r = 0\}$.

Let $\mathcal{S} \subset \mathfrak{h}(k(V))$ consist of triples (m_1, m_2, m_3), $m_i \in k(t)$ squarefree, $(\prod_{i=1}^3 m_i)$ is a square which divides $r(t)^2$, and $\gcd(m_i, p_i) = 1$.

Put another way, we have

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{E}(F)/2\mathcal{E}(F) \arrow[r] & \mathcal{S} \arrow[r] \arrow[d] & H^1_{\text{ét}}(\mathbb{P}^1, \mathcal{E}) \arrow[r] \arrow[d] & 0 \\
& & (F^*/F^{*2})^2 \arrow[r] & H^1(F, E)[2] \arrow[r] & 0
\end{tikzcd}$$

Corresponding to $m = (m_1, m_2, m_3)$, we have the surface X_m defined by the equations $x - e_i(t) = m_i(t)u_i^2$, $i = 1, 2, 3$. Then $X_m/\mathbb{P}^1$ has a minimal model if and only if $X_m/\mathbb{P}^1$ is locally isomorphic for the étale topology with $\mathcal{E}/\mathbb{P}^1$.

We have a map

$$\mathcal{S} \xrightarrow{\delta} \bigoplus_{M\in\mathcal{M}} (k_M^*/k_M^{*2})$$

where $k_M = k[t]/r_M(t)$. We see that $E(F)/2E(F) \subset \ker\delta$.

Theorem (Theorem A)**.** *Suppose that* $\ker\delta$ *is the image of* $E(F)[2]$*. (In particular, the generic rank is zero.) Assume Schinzel's hypothesis. Then there exist infinitely many* $x \in \mathbb{P}^1(k)$ *such that* $\operatorname{rk} E_x(k) = 0$.

Theorem (Theorem B)**.** *Let* $m \in \mathcal{S}$*, and assume that*

$$\ker\left(\mathcal{S} \to \bigoplus_M k_M^*/(k_M^{*2}, \delta_M(m))\right) = E(F)[2] \oplus \mathbb{Z}/2\mathbb{Z}.$$

Assume Schinzel's hypothesis. Assume $X_m(\mathbf{A}_k)^{\mathrm{Br}_1(X)} \neq \emptyset$*. Then there exist infinitely many* $x \in \mathbb{P}^1(k)$ *such that* $E_x(k)$ *is of rank one and* $X_{m,x}(k) \neq \emptyset$.

A.2 Colliot-Thelene 2: Rational points on surfaces with a pencil of curves of genus one

We had $y^2 = (x - c_1(t))(x - c_2(t))(x - c_3(t))$, $E/F = k(t)$, and

$$r(t) = \prod_{i<j}(c_i - c_j) = \rho \prod_{M\in\mathcal{M}} r_M(t)$$

separable, all r_M irreducible, even degree, $\mathcal{S} \subset \mathfrak{h}(F) = (F^*/F^{*2})^2$, $m = (m_1, m_2, m_3)$, $m_3 = m_1m_2$ up to F^{*2}. $\mathcal{X}_m/\mathbb{P}^1$, $x - c_i(t) = m_i(t)u_i^2$, $i = 1, 2, 3$.

$$\delta : \mathcal{S} \to \bigoplus_{M\in\mathcal{M}} k_M^*/k_M^{*2}$$

and δ' is the composition with the map

$$\bigoplus_{M\in\mathcal{M}} k_M^*/k_M^{*2} \to \bigoplus_{M\in\mathcal{M}} k_M^*/(k_M^{*2}, \delta_M(m)).$$

where $k_M = k[t]/r_M$.

Fact. $E(F)/2E(F) \subset \ker\delta$.

Theorem (Theorem B)**.** *Assume Schinzel's hypothesis, and the finiteness of* Ш*. Let $m \in \mathcal{S}$, $m \notin E(F)[2]$. Let $X = \mathcal{X}_m/\mathbb{P}^1$. Assume:* $\ker\delta' = E(F)[2] \oplus \mathbb{Z}/2\mathbb{Z}(m)$*, and* $X(\mathbf{A}_k)^{\mathrm{Br}_{vert}(X)} \neq \emptyset$.

Then $R = \{x \in \mathbb{P}^1(k) : \#X_x(k) = \infty\}$ is infinite, and $X(k)$ is Zariski dense.

Here,

$$\mathrm{Br}_{\mathrm{vert}}(X) = \{\xi \in \mathrm{Br}(X) : \xi_\eta|_{X_\eta} \text{ comes from } \mathrm{Br}(F)\} \subset \mathrm{Br}_1(X).$$

Schinzel's hypothesis: Let $P_i(x) \in \mathbb{Z}[x]$ for $i = 1, \dots, r$ be distinct irreducible polynomials with leading coefficient positive (plus technical condition, to exclude polynomials like $X^2 + X + 2$); then there exist infinitely many values $n \in \mathbb{N}$ such that each $P_i(x)$ is a prime.

Remark. The assumption that $\ker\delta' = E(F)[2] \oplus \mathbb{Z}/2\mathbb{Z}(m)$ is satisfied for general c_i. For the assumption that $X(\mathbf{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)} \neq \emptyset$, in general we have $\mathrm{Br}_{\mathrm{vert}}(X) = \mathrm{Br}\,k$ so this reduces to $X(\mathbf{A}_k) \neq \emptyset$.

The proof of this theorem will take up the rest of these notes.

We shall define a finite set $S \subset \Omega$ of 'bad places'. For each $v \in S$, we have some $x_v \in k_v$, and we look for $x \in \mathcal{O}_S$, with x very close to x_v for $v \in S$, and find one x such that:

- $X_x(\mathbf{A}_k) \neq \emptyset$;
- $\dim_{\mathbb{F}_2}(\mathrm{Sel}(E_x, 2)) = 3$, spanned by $E_x[2]$ and $m(x)$.

We have $S \supset S_0$, containing 2-adic places and those over ∞ (note we are being sloppy for real places), and places of bad reduction of $\mathcal{E}/k$, of $\mathcal{X}_m = X/k$, and such that $\mathrm{Cl}(\mathcal{O}_{S_0}) = 0$. If $v \notin S$, then $r_M(t) \in \mathcal{O}_S[t]$ is separable (finite étale cover).

We look at $r_M(x)$ and look at its prime decomposition; it will have some part in S and another part T_M^x of primes of multiplicity 1, and one prime v_M, the 'Schinzel prime'. We realize $(T_M \cup v_M) \cap (T_N \cup v_N) = \emptyset$ for $M \neq N$. Then $\mathcal{E}_x/k$ has bad reduction in $S \cup (\bigcup_M T_M) \cup (\bigcup v_M)$.

First we find x such that $X_x(\mathbf{A}_k) \neq \emptyset$. For $M \in \mathcal{M}$, we introduce the algebra $A_M(t) = \mathrm{cores}_{k_M/k}(K_M/k_M, t - \theta_M)$, where K_M/k_M is the quadratic extension connected to m. Then $r_M(t) = N_{k_M/k}(t - \theta_M)$. A priori, $A_M(t) \in \mathrm{Br}\,k(t) \to \mathrm{Br}\,X_\eta$. Since r_M is even, $A_M \in \mathrm{Br}(X)$.

Let $(P_v) \in X(\mathbf{A}_k)^{\mathrm{Br}_{\mathrm{vert}}(X)}$, with projection $(x_v) \in \mathbb{A}^1(k_v)$. We know that $\sum_{v\in\Omega} A_M(x_v) = 0$. For almost all places of k, $X(k_v) \xrightarrow{A_M} \mathrm{Br}(k_v)$ is trivial.

Fix S as before plus places where some A_M is not trivial on $X(k_v)$. Now $\sum_{v\in S} A_M(x_v) = 0$. Fix $x_v \in k_v$ for $v \in S$ with this property. Note $X_{x_v}(k_v) \neq \emptyset$. Suppose $x \in \mathcal{O}_S$ is very close to x_v for $v \in S$ and the decomposition of $r_M(x)$ has all primes in T_M split in K_M/k_M.

Claim. For such x, $X_x(\mathbf{A}_k) \neq \emptyset$.

Proof. The only places where it will fail to have a point are those of bad reduction. For $v \in S$, $X_x(k_v) \neq \emptyset$, as x is close to x_v. For $v \in T_M$, $X_x(k_v) \neq \emptyset$ since the two rational curves are defined. For $v = v_M$, write

$$0 = \sum_{v\in\Omega} A_M(x)_v = \sum_{v\in S} A_M(x)_v + \sum_{v\in T_M} A_M(x)_v + A_M(x)_{v_M} = 0 + 0 + A_M(x)|_{v_M}$$

the second because v splits in K_M; therefore the prime that is left over forces the prime v_M to split in K_M/k_M, we again have points locally. □

For the second part, we now need to control the Selmer groups uniformly in the family $\mathcal{E}_x$, for x satisfying $(*)$, namely, x is very close to x_v for $v \in S$, $r_M(x)$ decomposes into primes in S, T_M primes splitting in K_M/k_M, and the Schinzel prime v_M.

Let $T = T_x = S \cup \bigcup_{M\in\mathcal{M}} T_m$, and $\widetilde{T} = \widetilde{T_x} = S \cup \bigcup T_M \cup \bigcup v_M$. We have

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{h}(\mathcal{O}_T) \arrow[r] \arrow[d] & \mathfrak{h}(\mathcal{O}_T[u]) \arrow[r, "\mathrm{ord}_M"] \arrow[d, "\mathrm{ev}_x"] & \bigoplus_{M\in\mathcal{M}} (\mathbb{Z}/2\mathbb{Z})^2 \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathfrak{h}(\mathcal{O}_T) \arrow[r] & \mathfrak{h}(\mathcal{O}_{\widetilde{T}}) \arrow[r, "\mathrm{ord}_M"] & \bigoplus_{M\in\mathcal{M}} (\mathbb{Z}/2\mathbb{Z})^2 \arrow[r] & 0 \end{tikzcd}$$

Here

$$\mathrm{Sel}(E_x) \subset \mathcal{I}^{\widetilde{T}} \subset \mathfrak{h}(\mathscr{O}_{\widetilde{T}}),$$

and N_x the Cartesian square from $\mathfrak{h}(\mathcal{O}_T[u]) \xrightarrow{\mathrm{ev}_x} \mathfrak{h}(\mathcal{O}_{\widetilde{T}})$. Then $\mathrm{Sel}(E_x)$ is the kernel of a symmetric pairing on N_x.

We find two 'constant' subgroups N_x. First, we find $N_0 = \mathfrak{h}(\mathcal{O}_S) \cap \mathcal{I}^{\widetilde{T_x}}$, fixed because x very close to x_v for $v \in S$. For the second pair:

Proposition. *For each $M \in \mathcal{M}$, there exists a unique $(a_M, b_M) \in \mathfrak{h}(\mathcal{O}_S)$ such that for any x with $(*)$, $(a_M r_M(x)^{f_M}, b_M r_M(x)^{g_M}) \in \mathcal{I}^{\widetilde{T_x}}$, and for each $v \in S$, its component in V_v belongs to K_v.*

We define the subgroup

$$A = \bigoplus_{M\in\mathcal{M}} \mathbb{Z}/2(a_M r_M(t)^{f_M}, b_M r_M(t)^{g_M}).$$

Note $(f_M, g_M) \in \{(0,1), (1,0), (1,1)\}$.

Proposition.

$$N_x = N_0 \oplus A \oplus \phi_x^{-1}\left(\bigoplus_{v\in T\setminus S} (W_v/W_v \cap K_v)\right).$$

Proposition. *On $N_0 \oplus A \subset N_x$, the restriction of the pairing e_x is independent of x.*

To prove this, use various reciprocity laws.

To conclude, write $N_0 \oplus A = B_0 \oplus B_1 \oplus B_2 \subset \mathfrak{h}(k(t))$, where $B_0 = E(F)[2] \oplus \mathbb{Z}/2\mathbb{Z}(m)$, $B_0 \oplus B_1 = \ker e_x|_{N_0 \oplus A}$, and B_2 is the supplement. Use the assumption that $\ker \delta' = (\mathbb{Z}/2\mathbb{Z})^3$ to get rid of B_1...

Now use finiteness of Ш and Cassels-Tate pairing, $\dim(\text{Ш}(E_x)[2]) \leq 1$ implies $\text{Ш}(E_x)[2] = 0$, so the rank is 1.

A.3 de Jong: Rationally Connected Varieties

Deformation theory

Let X be a nonsingular projective variety over $\mathbb{C}$, and let $C \hookrightarrow X$ be a one-dimensional closed subscheme. We have $\mathscr{O}_X \supset \mathscr{I}_C$, the ideal sheaf of C, and we assume that C is a local complete intersection, or what is equivalent, $\mathscr{I}_C/\mathscr{I}_C^2$ is a locally free sheaf of $\mathscr{O}_C$-modules of rank $\dim X - 1$. For example, this holds if X is a nodal curve.

Definition. The *normal bundle of the curve C in X* is
$$\mathscr{N}_C X = \mathscr{H}om_{\mathscr{O}_C}(\mathscr{I}_C/\mathscr{I}_C^2, \mathscr{O}_C).$$

We have that
$$\widetilde{\mathscr{O}}_{\mathrm{Hilb}_X,[C]} = \mathbb{C}[[t_1, \ldots, t_d]]/(f_1, \ldots, f_r),$$
where $d = h^0(C, \mathscr{N}_C X)$, and $r \leq h^1(C, \mathscr{N}_C(X))$. We say that H^0 is the deformation space, and H^1 are the obstructions to deformation. In particular, the dimension the Zariski tangent space of the Hilbert scheme at $[C]$ has $\mathscr{T}_{[C]} \operatorname{Hilb}_X = H^0(C, \mathscr{N}_C X)$, and it has dimension at least $\chi(\mathscr{N}_C X)$, the Euler characteristic.

Example. In the case where $[f : C \to \mathbb{P}^1] \in \overline{\mathcal{M}_g}(\mathbb{P}^1, d)$, with C is a smooth genus g curve, and f having at worst simple branchings, then there are no obstructions to deformation and
$$\mathscr{T}_{[f]}\overline{\mathcal{M}_g}(\mathbb{P}^1, d) = \bigoplus_{P \in \mathrm{Ram}(f)} \mathscr{T}_{\mathbb{P}^1}|_{f(P)}.$$
This is a canonical way of understanding how to move branch points on maps to $\mathbb{P}^1$.

A map of moduli spaces

Let $f : X \to \mathbb{P}^1$ be a nonconstant morphism with X a nonsingular projective variety over $\mathbb{C}$, and let $C \subset X$ be a closed subscheme which is a smooth curve of genus g, such that the ramification of $f|_C$ is simple. In a (formal) neighborhood of $[C \subset X]$, the spaces $\overline{\mathcal{M}_g}(X, [C])$ and the Hilb_X are the same. The map
$$\overline{\mathcal{M}_g}(X, [C]) \to \overline{\mathcal{M}_g}(\mathbb{P}^1, d)$$
where d is the degree of f on C, induces on tangent spaces
$$H^0(C, \mathscr{N}_C X) \to \textstyle\bigoplus_{P \in \mathrm{Ram}(f|_C)} \mathscr{T}_{\mathbb{P}^1}|_{f(P)}$$
induced by the right vertical arrow in the diagram
$$\begin{tikzcd}
0 \arrow[r] & \mathscr{T}_C \arrow[r] \arrow[d, equal] & \mathscr{T}_X|_C \arrow[r] \arrow[d] & \mathscr{N}_C X \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathscr{T}_C \arrow[r] & f^*\mathscr{T}_{\mathbb{P}^1}|_C \arrow[r] & (f^*\mathscr{T}_{\mathbb{P}^1}|C)/\mathscr{T}_C \arrow[r] & 0
\end{tikzcd}$$
If C is contained in the smooth locus of f, then the middle vertical map $\mathscr{T}_X|_C \to f^*\mathscr{T}_{\mathbb{P}^1}|_C$ is surjective, hence also the right vertical map $\mathscr{N}_C X \to (f^*\mathscr{T}_{\mathbb{P}^1}|C)/\mathscr{T}_C$ is also surjective as maps of sheaves. This will not give a surjection on global sections, however one has:

Corollary. *If C is contained in the smooth locus of f, and $\mathscr{N}_C X$ is "sufficiently positive", then the morphism*
$$\overline{\mathcal{M}_g}(X, [C]) \to \overline{\mathcal{M}_g}(\mathbb{P}^1, d)$$
analytically locally around $[C \subset X]$ is a projection $\mathbb{C}^{a+b} \to \mathbb{C}^b$.

One argues that the Hilbert scheme is smooth at the point $[C \subset X]$ since one can twist by a small number of points and keep that the H^1 vanishes. In particular, the corollary implies that the morphism is surjective.

We are now ready to prove:

Theorem (G, Harris, Starr)**.** *If $k = \overline{k}$,* $\operatorname{char} k = 0$*, then any rationally connected variety over $k(C)$ for C a curve has a rational point.*

Proof. Assume that $(*)$: all fibres of $X \to \mathbb{P}^1$ are reduced.

Step 1. Take a general complete intersection $C \subset X$; it will be smooth, irreducible, of say genus g and degree d. The condition $(*)$ implies that C is in the smooth locus and $C \to \mathbb{P}^1$ (by Bertini) has at worst simple branching.

Step 2. Choose a large integer N and choose general points $c_1, \dots, c_N \in C$, and rational curves $C_i \subset X$ such that:

(i) $C \cap C_i = \{c_i\}$;
(ii) $C_i \subset f^{-1}(f(C_i))$;
(iii) $\mathscr{N}_{C_i} X_{f(c_i)}$ is very ample;
(iv) $\mathscr{T}_{c_i} C_i \subset \mathscr{T}_{c_i} X_{f(c_i)}$ is in general position.

Now let $C^{\text{new}} = C \cup C_1 \cup \dots \cup C_N$. The basic property is that $\mathscr{N}_{C^{\text{new}}} X|_{C_i} \supset \mathscr{N}_{C_i} X$. Moreover, $\mathscr{N}_{C^{\text{new}}} X|_C \supset \mathscr{N}_C X$ with colength N and assumption (iv) gives that this is "general". This gives that the sheaf $\mathscr{N}_{C^{\text{new}}} X$ on C^{new} is sufficiently positive.

Now deform this curve to a simply branched curve, and this gives the result; conclude by the corollary. □

Multiple fibres

We must deal with the case when $(*)$ fails. Suppose we have a family of varieties $X \to \mathbb{P}^1$ with fibres at $t_1, \dots, t_r$ irreducible of multiplicity $m_1, \dots, m_r$. Since the curve must intersect these fibres transversally, this must be preserved in any deformation, meaning that the ramification index at t_i will be divisible by m_i.

In this case, the problem is: $\overline{\mathcal{M}_g}(X, \beta) \to \overline{\mathcal{M}_g}(\mathbb{P}^1, d)$ cannot dominate. Instead, we consider consider the subset $Z_{g,d}^{(t_i,m_i)} \subset \overline{\mathcal{M}_g}(\mathbb{P}^1, d)$ consisting of stable maps $f : C \to \mathbb{P}^1$, C of genus g, f of degree d, such that all ramification indices above t_i are equal to m_i.

Now we have the additional problems: Which reducible curves are in $Z_{g,d}^{(t_i,m_i)}$? And perhaps $\dim Z$ is too small? To resolve both problems, enlarge the genus g (but not d) by adding loops to C: join two points with a good rational curve. This allows you to break off a component even in this case.

Conclusion

This is work with Jason Starr. What will guarantee the existence of a rational point on a variety over a function field in two variables? Is there a geometric condition which would be like rational connectedness in this case? This is too much to hope for, there are many surfaces S with a nontrivial Brauer-Severi variety $X \to S$. Maybe there are geometric restrictions on the fibres $X \to S$ such that one obtains a rational section.

A good guess for this condition: demand that certain moduli spaces of rational curves on the fibers are themselves rationally connected. For example, Starr and Harris proved that for hypersurfaces X of degree d in $\mathbb{P}^n$ with $d^2 + d + 2 \le n$, the moduli spaces of rational curves of fixed degree on X are themselves rationally connected.

A.4 Graber: Rationally Connected Varieties

Introduction

Definition. A field K is *quasi-algebraically closed* (C_1) if any polynomial $F \in K[x_0, \dots, x_n]$ with $\deg F \le n$ has a root in K.

Any finite field is quasi-algebraically closed, as is any function field $\overline{k}(C)$ of a curve over an algebrically closed field. This implies that any Laurent series ring $\overline{k}[[t]]$ is C_1.

These generalize to the following three possible definitions:

Definition. A projective variety X is *rationally connected* (RC) if any two general points $p, q \in X$ can be joined by a rational curve $f : \mathbb{P}^1 \to X$.

Definition. X is *rationally chain connected* (RCC) if any two general points $p, q \in X$ can be joined by a chain of rational curves.

Definition. X is *separably rationally connected* (SRC) if X is normal and there exists a rational curve $f : \mathbb{P}^1 \to X_{\mathrm{sm}}$ such that f^*TX is ample, i.e. $f^*TX = \bigoplus \mathscr{O}(d_i)$, $d_i > 0$.

Theorem. *If X is smooth projective over $\mathbb{C}$, then X is rationally connected (RC) if and only if X is rationally chain connected (RCC) if and only if X is separably rationally connected (SRC).*

In characteristic zero, X a smooth hypersurface of degree d in $\mathbb{P}^n$ is rationally connected if and only if $d \leq n$.

The main result we will consider is the following:

Theorem (G, Harris, Starr)**.** *If $k = \overline{k}$, $\operatorname{char} k = 0$, then any rationally connected variety over $k(C)$ for C a curve has a rational point.*

Remark. In characteristic p, the same is true for SRC. (de Jong, Starr)

Theorem. *Over $\overline{k}((t))$, any rationally connected variety has a rational point.*

This follows from the function field case. Geometrically, you can find a nonsingular integral model over $k[[t]]$; to find a section, it is equivalent to find a reduced component of the central fiber.

Theorem (Ernault)**.** *If $X/\mathbb{F}_q$ is smooth, projective, and geometrically rationally chain connected, then X has a rational point.*

Proof, a Beginning

We now prove the theorem that an RC variety over $k(C)$ has a rational point.

Choose an integral model $f : X \to B$. First, we reduce to the case $B \cong \mathbb{P}^1$. By restriction of scalars, have a map $X \to B \to \mathbb{P}^1$; the fibres of $X \to \mathbb{P}^1$ are products of fibres of f, and the product of rationally connected varieties is rationally connected.

Next, choose a curve $C \subset X$ which dominates $\mathbb{P}^1$. Deform C and specialize until it breaks off a section. We have a map of moduli spaces

$$\{\text{curves in } X\} \xrightarrow{\pi_f} \{\text{coverings of } \mathbb{P}^1\}.$$

The latter is built out the data of the branch points plus monodromy; fixing the genus of the curve and the degree of the cover, we know that this moduli space is irreducible. It is possible to degenerate any branched cover of $\mathbb{P}^1$ to a reducible cover with a section as one component. It is enough to show that this map π_f on moduli spaces is surjective. Now it is just a matter of tracing the monodromy as the branch points move around (at least in characteristic zero). In characteristic p, it can also be done (look, for example, at $\mathbb{P}^1 \to \mathbb{P}^1$).

To make all of this more precise, we look at stable maps. Given X a smooth projective variety over $\mathbb{C}$, and given $g \in \mathbb{N}$ and $\beta \in H_2(X, \mathbb{Z})$, we construct a space $\overline{\mathcal{M}_g}(X, \beta)$ consisting of maps $f : C \to X$ such that C is a connected nodal curve of arithmetic genus g, f is a morphism, and $f_*(C) = \beta$, together with a stability criterion.

This space $\overline{\mathcal{M}_g}(X, \beta)$ is projective, and given any morphism $f : X \to Y$, one has an induced map $M_f : \overline{\mathcal{M}_g}(X, \beta) \to \overline{\mathcal{M}_g}(Y, f_*\beta)$ from $C \to X \to Y$. If $Y = \mathbb{P}^1$, then $\overline{\mathcal{M}_g}(\mathbb{P}^1, d)$ is a compactification of the space of branched covers. We want to show that M_f is surjective. (We only need the coarse moduli space; in fact, at least in characteristic zero we have a Deligne-Mumford stack.)

When K is C_1, the bound $d \leq n$ is sharp. If K is not algebraically closed, then pick a finite extension $K \subset L$, and consider $N_L : L \to K$; this has a polynomial of degree $[L : K]$ with no nontrivial zeros; therefore it is impossible to get a larger class of hypersurfaces.

Is the notion of rational connectivity sharp? In the case of finite fields, we also get: if $X/\mathbb{F}_q$ smooth projective, and either $H^i(X, \mathscr{O}_X) = 0$ for $i > 0$ or $H^0(X, \bigwedge^i \Omega_X) = 0$ for $i > 0$, then X has a rational point. (These two are equivalent in characteristic zero.) The analog over function fields is false. In particular, there exists a family X of Enriques surfaces over $k(C)$ (C is a curve over $\mathbb{C}$) which has no section.

The general statement: Let $\pi : X \to M$ be a proper morphism of varieties over $\mathbb{C}$. Suppose that for all maps $f : C \to M$, there exists a pullback $\widetilde{f} : C \to X$. It would suffice for there to exist $Z \subset X$ dominating M such that the general fibre of $\pi|_Z$ is rationally connected. It is a theorem that this is necessary and sufficient (G, Harris, Mazur, Starr).

A.5 Harari 1: Weak approximation on algebraic varieties (introduction)

Let k be a number field, and let k_v be the completion of k at v. Let Ω_k be the set of all places of k.

Basic Facts

Theorem (Weak Approximation). *Let $\Sigma \subset \Omega_k$ be a finite set of places of k. Let $\alpha_v \in k_v$ for $v \in \Sigma$. Then there is an $\alpha \in k$ which is arbitrarily close to α_v for $v \in \Sigma$.*

This is a refinement of the Chinese remainder theorem. One reformulation of it is as follows: the diagonal embedding $k \hookrightarrow \prod_{v \in \Omega_k} k_v$ is dense, the product equipped with the product of the v-adic topologies.

We have the slight refinement: $\mathbb{P}^1(k)$ is dense in $\prod_v \mathbb{P}^1(k_v)$.

Definition. Let X/k be a geometrically integral algebraic variety. Then X satisfies *weak approximation* if given $\Sigma \subset \Omega_k$ a finite set of places and $M_v \in X(k_v)$ for $v \in \Sigma$, there exists a k-rational point $M \in X(k)$ which is arbitrarily close to M_v for $v \in \Sigma$.

Care must be taken if $\prod_{v \in \Omega_k} k_v$ is empty; by convention, we will say that in this case X satisfies weak approximation even if $X(k)$ is empty.

We see weak approximation is equivalent to the statement that $X(k)$ is dense in $\prod_v X(k_v)$.

Remark. If X is projective, $X(\mathbf{A}_k) = \prod_v X(k_v)$ and weak approximation is equivalent to strong approximation, namely, $X(k)$ is dense in $X(\mathbf{A}_k)$ for the adelic topology. (Here, $X(k_v) = \mathscr{X}(\mathcal{O}_v)$, $\mathscr{X} \to \operatorname{Spec} \mathcal{O}_k$ a flat and proper model of X.)

Let X, X' be smooth. Assume that X is k-birational to X'. Then X satisfies weak approximation if and only if X' satisfies weak approximation (a consequence of the implicit function theorem for k_v).

We can speak about weak approximation for a function field $k(X)$: this means that weak approximation holds for any smooth (projective) model of X.

Example. The spaces $\mathbb{A}^1_k, \mathbb{P}^1_k$, and more generally, $\mathbb{A}^n_k, \mathbb{P}^n_k$, satisfy weak approximation, as does any k-rational variety, e.g. a smooth quadric with a k-point.

More Examples

Theorem. *Let $Q \subset \mathbb{P}^n_k$ a (smooth) projective quadric. Then Q satisfies weak approximation.*

Here, we do not assume that there is a k-rational point. This is the difficult part, the Hasse-Minkowski theorem: if $Q(k_v) \neq \emptyset$ for all v, then $Q(k) \neq \emptyset$.

There are several results for complete intersections:

A. A smooth intersection of 2 quadrics $X \subset \mathbb{P}^n_k$ (Colliot-Thélène, Sansuc, Swinnerton-Dyer 1987) satisfies weak approximation if $n \geq 8$ or if $n \geq 4$ and there exists a pair of skew-conjugate lines on X.
B. Châtelet surfaces: $y^2 - az^2 = P(x)$, where $\deg P = 4$, $a \in k^* - k^{*2}$. If P is irreducible, then X (a smooth projective model) satisfies weak approximation. (Uses descent method.)
C. The circle method: $X \subset \mathbb{P}^n_k$ a smooth cubic hypersurface, then weak approximation holds for $n \geq 16$ (Skinner 1997).

There are also results for linear algebraic groups:

A. If T is a k-torus, and $\dim T \leq 2$, then T satisfies weak approximation beacuse T is k-rational (Voskreseskii).
B. If G is a semi-simple, simply connected linear k-group, then G satisfies weak approximation (Kneser-Platonov, around 1969).

Conjecture. *A smooth intersection of 2 quadrics in $\mathbb{P}^n$ for $n \geq 5$ satisfies weak approximation.*

A smooth cubic hypersurface (of dimension at least 3) satisfies weak approximation.

The Fibration Method

Theorem. *Let $p : X \to B$ be a projective, flat surjective morphism (with X smooth, to simplify). Assume that*

(i) *B is projective and satisfies weak approximation;*
(ii) *Almost all k-fibers of p satisfy weak approximation; and*
(iii) *All fibers of p are geometrically integral.*

Then X satisfies weak approximation.

(Here almost all means on a Zariski-dense open subset).

There are refinements when B is the projective space : you can accept degenerate fibers on one hyperplane (using the strong approximation theorem for the affine space).

Applications: (i) Hasse-Minkowski theorem, from four variables to five; (ii) intersection of 2 quadrics in $\mathbb{P}^n$ for $n \geq 8$ (here one uses a fibration in Châtelet surfaces) and $n \geq 5$ with a pair of skew conjugate lines (to go from $n = 4$ to $n \geq 5$ by induction); (iii) cubic hypersurfaces of dimension ≥ 4 with 3 conjugate singular points (Colliot-Thélène, Salberger).

Proof. Start with M_v a smooth k_v-point for any v on X. Project $p(M_v) = P_v \in B(k_v)$. Use weak approximation on B, so can approximate P_v by $P \in B(k)$ for $v \in S$. Consider the fiber $p^{-1}(P) = X_P \subset X$; X_P has a k_v-point M'_v close to M_v for $v \in \Sigma$ by the implicit function theorem. To apply weak approximation on X_P, we check that $X_P(k_v) \neq \emptyset$ for $v \notin \Sigma$; this is OK if Σ is sufficiently large by the Weil estimates : here we use that all k-fibers are geometrically irreducible, which implies that the reduction mod. v of X_P also is for a sufficiently large v (independent of P). □

Some Counterexamples

Cubic surfaces: the surface $5x^3 + 9y^3 + 10z^3 + 12w^3 = 0$ fails the Hasse Principle (Cassels, Guy).

Certain intersections of two quadrics in $\mathbb{P}^4_k$ (see above).

Looking (over the rationals) at $y^2 + z^2 = f(x)g(x)$, $\deg(f) = \deg(g) = 2$, $\gcd(f, g) = 1$, it is possible to construct counterexamples to weak approximation. The idea: $K = \mathbb{Q}(i)$, $K_v = K \otimes_{\mathbb{Q}} \mathbb{Q}_v$; there exists a finite set Σ_0 such that if $v \notin \Sigma_0$ and $M_v \in X(\mathbb{Q}_v)$, then $f(M_v)$ is a norm of $K_v/\mathbb{Q}_v$ (use a computation with valuations). If you find $\Sigma \supset \Sigma_0$ and $v_0 \in \Sigma$ such that there exists M_{v_0} such that $f(M_{v_0})$ is not a local norm and $v \neq v_0$ there exists M_v such that $f(M_v)$ is a local norm, then there is no weak approximation. (Think: global reciprocity of class field theory.)

For tori, let K/k be a biquadratic extension, then there are counterexamples like $T : N_{K/k}(x_1w_1 + \cdots + x_4w_4) = 1$, where $w_1, \ldots, w_4$ is a basis of K/k; this holds e.g. for $k = \mathbb{Q}$, $K = \mathbb{Q}(i, \sqrt{5})$.

Theorem (Minchev)**.** *Let X be a projective, smooth k-variety, assume that $\pi_1(\overline{X}) \neq 0$, where $\overline{X} = X \otimes \overline{k}$, $\overline{k}$ an algebraic closure. Assume $X(k) \neq \emptyset$, then X does not satisfy weak approximation.*

Sketch of proof. Enlarge the situation over $\operatorname{Spec} \mathscr{O}_{k,\Sigma_0}$ where Σ_0 is a finite set of places. By assumption, there is a nontrivial geometrically connected covering $Y \to X$, which for models gives $\mathscr{Y} \to \mathscr{X}$. Take an arbitrary $M \in X(k)$, the fibre $Y_M = \operatorname{Spec} L$ where L is an étale algebra $L = k_1 \times \cdots \times k_r$; each k_i is unramified outside Σ_0. Only finitely many k_i are possible (by Hermite's Theorem). Find $v \notin \Sigma_0$ such that v is totally split for each k_i (by Cebotarev's Theorem); find M_v such that the fiber of Y at X for M_v is not (this is possible because Y is geometrically connected, via a "geometric" Cebotarev-like Theorem). Then M_v cannot be approximated by a rational point M. □

A.6 Harari 2: Weak approximation on algebraic varieties (cohomology)

Let X be a smooth, geometrically integral variety over k (a number field), and suppose that X is projective. We denote by $\overline{X(k)}$ the closure of $X(k)$ in $\prod_{v \in \Omega_k} X(k_v) = X(\mathbf{A}_k)$.

Here our aim is to: (i) explain the counterexamples to weak approximation; (ii) find 'intermediate' sets E between $\overline{X(k)}$ and $X(\mathbf{A}_k)$; (iii) in some cases, prove that $E = \overline{X(k)}$.

General setting

Let G/k be an algebraic group (usually linear, but not necessarily connected, e.g. G finite). If G is commutative: define $H^i(X,G)$ the étale cohomology groups ($i = 1,2$; the cohomological dimension of a number field forgetting real places makes the higher cohomology groups uninteresting). In general, we have only the pointed set $H^1(X,G)$ (defined by Cech cocycles for the étale topology). If $X = \operatorname{Spec} k$, $H^1(X,G) = H^1(\Gamma, G(\overline{k}))$, where $\Gamma = \operatorname{Gal}(\overline{k}/k)$. If G is linear, $H^1(X,G)$ corresponds to G-torsors over X up to isomorphism.

Take $f \in H^i(X,G)$, define

$$X(\mathbf{A}_k)^f = \left\{(M_v) \in X(\mathbf{A}_k) : (f(M_v)) \in \operatorname{img}(H^i(k,G) \to \textstyle\prod_v H^i(k_v,G))\right\}.$$

Obviously $X(k) \subset X(\mathbf{A}_k)^f$. We will see that in many cases $\overline{X(k)} \subset X(\mathbf{A}_k)^f$

Example.

(a) $\operatorname{Br} X = H^2(X, \mathbb{G}_m)$;

$$\overline{X(k)} \subset X(\mathbf{A}_k)^{\operatorname{Br}} = \bigcap_{f \in \operatorname{Br} X} X(\mathbf{A}_k)^f.$$

(Indeed the Brauer group of the ring of integers of k_v is zero). $X(\mathbf{A}_k)^{\operatorname{Br}}$ is the *Brauer-Manin* set of X. Manin showed in 1970 that for a genus one curve with finite Tate-Shafarevich group, the condition $X(\mathbf{A}_k)^{\operatorname{Br}} \neq \emptyset$ implies the existence of a rational point.

(b) Let $f : Y \to X$ be a Galois, geometrically connected, nontrivial étale covering with group G. Then $f \in H^1(X,G)$, where G is considered as a constant group scheme. Then $\overline{X(k)} \subset X(\mathbf{A}_k)^f$ (via Hermite's Theorem). It is possible to find $(M_v) \notin X(\mathbf{A}_k)^f$, which implies Minchev's result that X does not satisfy weak approximation.

Remark. If X is rational, then $\operatorname{Br} X/\operatorname{Br} k = H^1(k, \operatorname{Pic} \overline{X})$ is finite, where $\overline{X} = X \times_k \overline{k}$. Then $X(\mathbf{A}_k)^{\operatorname{Br}}$ is 'computable'.

Theorem (H, Skorobogatov)**.** *If G is linear and $f \in H^1(X,G)$, then $\overline{X(k)} \subset X(\mathbf{A}_k)^f$ (and $X(\mathbf{A}_k)^f$ is "computable").*

Abelian descent theory

This was developed by Colliot-Thélène and Sansuc, and recently completed by Skorobogatov.

Theorem. *Define*

$$X(\mathbf{A}_k)^{\operatorname{Br}_1} = \bigcap_{f \in \operatorname{Br}_1 X} X(\mathbf{A}_k)^f$$

where $\operatorname{Br}_1 X = \ker(\operatorname{Br} X \to \operatorname{Br} \overline{X})$*. Assume that* $X(\mathbf{A}_k)^{\operatorname{Br}_1} \neq \emptyset$*. Then:*

(a) *We have*

$$X(\mathbf{A}_k)^{\operatorname{Br}_1} = \bigcap_{\substack{f \in H^1(X,S) \\ S \text{ of multiplicative type}}} X(\mathbf{A}_k)^f.$$

(b) *Assume further that* $\operatorname{Pic}\overline{X}$ *is of finite type, set* S_0 *such that* $\widehat{S_0} = \operatorname{Pic}\overline{X}$*; then there exists a torsor* $f_0 : Y \to X$ *under* S_0 *(a* universal torsor*, i.e. "as nontrivial as possible") such that*

$$X(\mathbf{A}_k)^{\mathrm{Br}_1} = X(\mathbf{A}_k)^{f_0}.$$

This Theorem is difficult, see Skorobogatov's book for a complete account on the subject. One of the ideas is to recover the Brauer group of X (mod. $\operatorname{Br} k$) making cup-products $[Y] \cup a$, where $a \in H^1(k, \widehat{S_0})$ and $[Y]$ is the class of Y in $H^1(X, S_0)$.

Now assume that X is a rational variety, so $X(\mathbf{A}_k)^{\mathrm{Br}} = X(\mathbf{A}_k)^{\mathrm{Br}_1}$ (since $\operatorname{Br}\overline{X} = 0$). Assume $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$. Consider a universal torsor $f : Y \xrightarrow{S_0} X$. If $\sigma \in H^1(k, S_0)$, can define $f^\sigma : Y^\sigma \to X$ where

$$[Y^\sigma] = [Y] - \sigma \in H^1(X, S_0).$$

Then

$$X(\mathbf{A}_k)^f = \bigcup_{\sigma \in H^1(k,S_0)} f^\sigma(Y^\sigma(\mathbf{A}_k)).$$

If you can prove that the torsors Y^σ satisfy weak approximation, then $\overline{X(k)} = X(\mathbf{A}_k)^f = X(\mathbf{A}_k)^{\mathrm{Br}}$, so the Brauer-Manin obstruction is the only one.

Example. There are many examples of this:

(a) Châtelet surface: $y^2 - az^2 = P(x)$, $a \in k^*/k^{*2}$, $\deg P = 4$. Colliot-Thélène, Sansuc, Swinnerton-Dyer showed that $\overline{X(k)} = X(\mathbf{A}_k)^{\mathrm{Br}}$, so the Brauer-Manin obstruction is the only one. If P is irreducible, then $\operatorname{Br} X/\operatorname{Br} k = 0$, so X satisfies weak approximation.
If P is reducible, we can have a counterexample to weak approximation, e.g. $y^2 - az^2 = f_1(x)f_2(x)$, where $\deg f_1 = \deg f_2 = 2$, $\gcd(f_1, f_2) = 1$, in some cases there is an obstruction given by the Hilbert symbol $f = (a, f_1)$.

(b) Conic bundles over $\mathbb{P}^1$ with at most 5 degenerate fibres. Results of Colliot-Thélène, Salberger, Skorobogatov covered at most 4. In the case of 5, the existence of a global rational point is easy to show, so the only problem is weak approximation, and which is due to Salberger, Skorobogatov 1993 (using descent and K-theory).

Theorem (Sansuc 1981)**.** *Let G be a linear connected algebraic group over k, X a smooth compactification of G, then the Brauer-Manin obstruction is the only one:*

$$\overline{X(k)} = X(\mathbf{A}_k)^{\mathrm{Br}}.$$

Back to fibration methods

If $p : X \to B$ is a fibration, we saw that if the base and the fibres satisfy weak approximation, under certain circumstances then X satisfies weak approximation.

Here we consider $p : X \to \mathbb{P}^1$, a projective, surjective morphism (and the generic fibre X_η is smooth). Assume also that all fibres are geometrically integral (can do with all but one because of strong approximation on the affine line).

Question. If $\overline{X_P(k)} = X_P(\mathbf{A}_k)^{\mathrm{Br}}$ for almost all fibres X_P, $P \in \mathbb{P}^1(k)$, can you prove that $\overline{X(k)} = X(\mathbf{A}_k)^{\mathrm{Br}}$?

Theorem (H 1993, 1996)**.** *Yes,* $\overline{X(k)} = X(\mathbf{A}_k)^{\mathrm{Br}}$ *if you assume that:*

(i) $\operatorname{Pic}\overline{X_\eta}$ *is torsion-free, where* $\overline{X_\eta} = X_\eta \times_K \overline{K}$, $K = k(\eta)$*; e.g.* X_η *rational, or smooth complete intersection of dimension at least three.*

(ii) $\operatorname{Br}\overline{X_\eta}$ *is finite.*

Two ideas:

(a) $\operatorname{Br}X_\eta/\operatorname{Br}K \to \operatorname{Br}X_P/\operatorname{Br}k$ is an isomorphism for many k-fibres X_P ('many' in the sense of Hilbert's irreducibility theorem).

(b) If $\alpha_1,\dots,\alpha_r$ are elements of $\operatorname{Br}X_\eta$, assume $\alpha_i \in \operatorname{Br}U$, $U \subset X$ an open subset. Use the 'formal lemma': Take $(M_v) \in X(\mathbf{A}_k)^{\mathrm{Br}}$, $M_v \in U$, Σ_0 a finite set of places; then there exists $(P_v) \in X(\mathbf{A}_k)$, $P_v \in U$, $\Sigma \supset \Sigma_0$ finite such that:

1. $P_v = M_v$ for $v \in \Sigma_0$;
2. $\sum_{v\in\Sigma} j_v(\alpha_i(P_v)) = 0$ for $1 \le i \le r$, where $j_v : \operatorname{Br}k_v \to \mathbb{Q}/\mathbb{Z}$ is the local invariant.

Applications: (i) Recover Sansuc's result just knowing the case of a torus; (ii) If you know that $\overline{X(k)} = X(\mathbf{A}_k)^{\mathrm{Br}}$ for X a smooth cubic surface, then by induction the same holds for hypersurfaces, so if $\dim X \ge 3$, then X satisfies weak approximation.

Nonabelian descent

If G/k is a finite but not commutative k-group, it is possible that for $f \in H^1(X,G)$, $X(\mathbf{A}_k)^f \not\supset X(\mathbf{A}_k)^{\mathrm{Br}}$.

Theorem (Skorobogatov 1997)**.** *There exists $X/\mathbb{Q}$ a bi-elliptic surface such that $X(\mathbb{Q}) = \emptyset$, $X(\mathbf{A}_\mathbb{Q})^{\mathrm{Br}} \neq \emptyset$.*

Actually: $X(\mathbf{A}_\mathbb{Q})^f = \emptyset$ for some $f \in H^1(X,G)$, $G(\overline{\mathbb{Q}}) = (\mathbb{Z}/4\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

There are similar statements for weak approximation (H 1998), e.g. take X/k any bi-elliptic surface, $X(k) \neq \emptyset$, then $\overline{X(k)} \subsetneq X(\mathbf{A}_k)^{\mathrm{Br}}$.

Nevertheless the Brauer-Manin condition is quite strong, as shows the following result :

Theorem (H 2001)**.** *We have:*

(a) *If G/k is a linear connected k-group, $f \in H^1(X,G)$, then*
$$X(\mathbf{A}_k)^{\mathrm{Br}} \subset X(\mathbf{A}_k)^f.$$

(b) *If G is any commutative k-group, $f \in H^2(X,G)$, then*
$$X(\mathbf{A}_k)^{\mathrm{Br}} \subset X(\mathbf{A}_k)^f.$$

Open question : is the first part of this theorem still true for a G which is an extension of a finite *abelian* group by a connected linear group ? My guess is "no".

A.7 Hassett 1: Equations of Universal Torsors

Cox Rings

This follows an exposition due to Hu and Keel (Yi Hu and Seán Keel, *Mori dream spaces and GIT*, Michigan Math. J., **48** (2000), 331-348). Let $K = \mathbb{C}$, and X a projective smooth variety over K. Let $L_1,\dots,L_r$ be line bundles on X. If $\nu = (n_1,\dots,n_r) \in \mathbb{N}^r$, then $L^\nu = L_1^{\otimes n_1} \otimes \cdots \otimes L_r^{\otimes n_r}$.

We have a multiplication map $\Gamma(X,L^{\nu_1}) \otimes \Gamma(X,L^{\nu_2}) \to \Gamma(X,L^{\nu_1+\nu_2})$. We have a ring $R(X,L_1,\dots,L_r) = \bigoplus_{\nu\in\mathbb{N}^r} \Gamma(X,L^\nu)$, which is often not finitely generated.

If $L_1,\dots,L_r$ are (semi)ample (a *semiample* bundle is a pullback of an ample bundle), then $R(X,L_1,\dots,L_r)$ is finitely generated.

Definition. Let X be smooth and projective, and assume $\mathrm{Pic}(X) \cong \mathbb{Z}^r$ (e.g. a Fano variety). The *Cox ring* $\mathrm{Cox}(X)$ is $\mathrm{Cox}(X) = R(X, L_1, \ldots, L_r)$ where:

(i) $L_1, \ldots, L_r$ is a basis for $\mathrm{Pic}(X)$;
(ii) Every effective divisor D can be written $D = n_1[L_1] + \cdots + n_r[L_r]$ for $n_j \geq 0$.

Remark.

A. $\mathrm{Cox}(X)$ is (multi)graded by $\mathrm{Pic}(X)$; for $\nu \in \mathrm{Pic}(X)$, there is a ν-graded piece $\mathrm{Cox}(X)_\nu$. This gives a natural action by T_{NS}, the Neron-Severi torus, $t(\xi) = \chi_v(t)\xi$, $t \in T$, $\chi_v \in X^*(T_{NS})$ corresponding to $v \in \mathrm{Pic}(X)$.
B. Graded pieces which are nonzero are in one-to-one correspondence with effective divisor classes of X.
C. Definition does not depend on choice of $\{L_j\}$; $R(X, L_1, \ldots, L_\nu) \simeq R(X, M_1, \ldots, M_v)$ is natural up to the action of the Neron-Severi torus.

The Hilbert function $h(\nu) = \dim \mathrm{Cox}(X)_\nu = \chi(\mathscr{O}_X(v))$ if ν has no higher cohomology, so is a 'polynomial in ν'. For example, if $\nu \in K_X + (\text{ample cone})$, Kodaira vanishing implies that $h(\nu) = \chi(\mathscr{O}_X(\nu))$.

If $-K_X$ is nef (D is *nef* if $D \cdot C \geq 0$ for every curve C) and big (D is *big* if D is in the interior of the effective cone), for example if X is Fano, then $h(\nu) = \chi(\mathscr{O}(\nu))$ for all ν nef and big. Our basic strategy: use knowledge of the Hilbert function to read off the structure of $\mathrm{Cox}(X)$. There is hope that the ring will be finitely generated from this polynomial expression.

Finite Generation

What are necessary conditions for $\mathrm{Cox}(X)$ to be finitely generated? (Part of a theorem of Hu, Keel which give necessary and sufficient conditions.) We must have:

A. The effective cone of X should be finitely generated. (It is an open problem if the effective cone of a Fano variety is finitely generated, either in the sense that the closed cone is rational polyhedral or the associated monoid is finitely generated.)
B. The nef cone is finitely generated.

There are also sufficient conditions:

A. $\mathrm{Cox}(X) \cong k[x_\sigma]$ for $\sigma \in \Sigma(1)$ if X is a toric variety.
B. If X is (log) Fano of dimension ≤ 3. Then $\mathrm{Cox}(X)$ is finitely generated (Shokurov).

Conjecture (Hu, Keel)**.** *If X is (log) Fano, then* $\mathrm{Cox}(X)$ *is finitely generated.*

Remark. The universal torsor $T \subset \mathrm{Spec}\,\mathrm{Cox}(X)$ as an explicitly defined open subset, if $\mathrm{Cox}(X)$ is finitely generated.

E_6 *Cubic Surface*

This is joint work with Tschinkel. The E_6 cubic surface S is defined by the equation $xy^2 + yw^2 + z^3 = 0$ embedded in $\mathbb{P}^3$; it contains a unique line $\ell : y = z = 0$, and a unique singularity $P : x = y = z = 0$.

Analysis of the singularity: In affine coordinates, we have $Y^2 + YW^2 + Z^3 = 0$. We rewrite this as $(Y + W^2/2)^2 - (1/4)W^4 + Z^3 = 0$, and up to analytic equivalence, this is $Y'^2 + W'^4 + Z^3 = 0$, which is the normal form of an E_6 singularity.

The resolution $\beta : \widetilde{S} \to S$ has six -2 exceptional curves in an E_6-diagram, and $\mathrm{Pic}(\widetilde{S})$ has intersection form

F_1	F_2	F_3	ℓ	F_4	F_5	F_6
-2	0	1	0	0	0	0
0	-2	0	0	0	0	1
1	0	-2	0	0	0	1
0	0	0	-1	1	0	0
0	0	0	1	-2	1	0
0	0	0	0	1	-2	1
0	1	1	0	0	1	-2

with numbering as

$$\begin{tikzcd}
 & & 2 \arrow[d, dash] & & & \\
1 \arrow[r, dash] & 3 \arrow[r, dash] & 6 \arrow[r, dash] & 5 \arrow[r, dash] & 4 \arrow[r, dash] & \ell.
\end{tikzcd}$$

The inverse of this matrix is given by

A_1	A_2	A_3	L	A_4	A_5	A_6
0	1	1	2	2	2	2
1	1	2	3	3	3	3
1	2	2	4	4	4	4
2	3	4	3	4	5	6
2	3	4	4	4	5	6
2	3	4	5	5	5	6
2	3	4	6	6	6	6

The inverse proves that:

Proposition. *The effective cone of X is generated by $\{F_j, \ell\}$; the nef cone is generated by $\{A_j, L\}$.*

We have

$$\mathrm{Cox}(\widetilde{S}) = \bigoplus_{n_1,\dots,n_6} \Gamma(\mathscr{O}_{\widetilde{S}}(n_1F_1 + \cdots + n_6F_6 + n_\ell \ell));$$

we choose ξ_j generating $\Gamma(\mathscr{O}_{\widetilde{S}}(F_j))$. (Descent to k involves rescaling these ξ_j such that the relations are defined over k.)

We have $k[\xi_1, \dots, \xi_6, \xi_\ell] \hookrightarrow \mathrm{Cox}(X)$, but this is not surjective. We need additional generators. We let $\xi^{\alpha(j)} \in \Gamma(\mathscr{O}(A_j))$; since A_1 is semiample, we have $\dim \Gamma(\mathscr{O}(A_j)) = 2$ by Riemann-Roch, and $\widetilde{S} \to \mathbb{P}^1$ is a conic bundle. Then

$$\Gamma(\mathscr{O}(A_1)) = \langle \xi^{\alpha(1)}, \tau_1 \rangle.$$

Similarly, $\dim \Gamma(\mathscr{O}(A_2)) = 3$, so we have an additional generator

$$\Gamma(\mathscr{O}(A_2)) = \langle \xi^{\alpha(2)}, \xi^{\alpha(2)-\alpha(1)}\tau_1, \tau_2 \rangle.$$

Since $\dim \Gamma(\mathscr{O}(A_\ell)) = 4$, we have a fourth generator

$$\Gamma(\mathscr{O}(A_\ell)) = \langle \xi^{\alpha(\ell)}, \xi^{\alpha(\ell)-\alpha(1)}\tau_1, \xi^{\alpha(\ell)-\alpha(2)}\tau_2, \tau_\ell \rangle.$$

Fact. We have a surjection $\mathbb{C}[\xi_1, \dots, \xi_\ell, \tau_1, \tau_2, \tau_\ell] \to \mathrm{Cox}(X)$.

Now we look for relations among these generators. By the Hilbert function, we know that $\dim \Gamma(\mathscr{O}(A_6)) = 7$, but we have 8 elements of degree $\alpha(\mathscr{O})$ in the polynomial ring:

$$\{\xi^{\alpha(6)}, \xi^{\alpha(6)-\alpha(1)}\tau_1, \dots, \xi^{\alpha(6)-\alpha(\ell)}\tau_\ell\}.$$

Since $\mathscr{O}(A_\ell) = \mathscr{O}_S(+1)$, $Y = \xi^{\alpha(\ell)}$, $Z = \xi^{\alpha(\ell)-\alpha(1)}\tau_1$, $W = \xi^{\alpha(\gamma)-\alpha(2)}\tau_2$ after renormalization, so the original equation $Y^2 + YW^2 + Z^3 = 0$ gives the relation

$$F : \tau_\ell \xi_\ell^3 \xi_4^2 \xi_5 + \tau_2^2 \xi_2 + \tau_1^3 \xi_1^2 \xi_3 = 0.$$

With this,

$$\mathrm{Cox}(\widetilde{S}) = \mathbb{C}[\xi_1, \dots, \xi_\ell, \tau_1, \tau_2, \tau_\ell]/\langle F \rangle;$$

by a computation of the Hilbert function of the quotient, there are no more relations.

This method should also work for other very singular cubic surfaces.

A.8 Hassett 2: Weak approximation for function fields

Weak Approxmation

We start with the diagram:

$$\begin{tikzcd} X \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec} F \arrow[r] & \operatorname{Spec} \mathcal{O}_F \end{tikzcd}$$

where $X(F) = \mathcal{X}(\mathcal{O}_F)$, X smooth projective over a number field, and $\mathcal{X}$ an integral model of X.

Definition. The F-rational points of X satisfy *weak approximation* if for each $\{v_j\}$ a finite set of places, with completions F_{v_j}, and open sets $U_j \subset X(F_{v_j})$, there exists an $x \in X(F)$ with $x \in U_j$ for each j.

Note that for nonarchimedean places, $\mathfrak{p}_j \in \operatorname{Spec} \mathcal{O}_F$, $\mathbb{F}_{\mathfrak{p}_j} = \mathcal{O}_F/\mathfrak{p}_j$, then we have reduction maps

$$X(F_{v_j}) = X(\widehat{\mathcal{O}_{F,v_j}}) \xrightarrow{\rho_{j,n}} X(\mathcal{O}_F/\mathfrak{p}_j^{n+1}) \ni s_j.$$

The basic open subsets $\rho_{j,n}^{-1}(s_j)$ have 'fixed reduction modulo $\mathfrak{p}_j^{n+1}$'.

Remarks. By Hensel's lemma, $x_j \in X(\mathbb{F}_{\mathfrak{p}_j})$ gives a point in $X(F_{v_j})$ if x_j is smooth.

If $\mathcal{X}$ is regular, then if $x_j \in X(\mathbb{F}_{\mathfrak{p}_j})$ comes from a point in $X(F_{v_j})$, then x_j is regular.

Function field analog

Now consider the diagram

$$\begin{tikzcd} X \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\ \operatorname{Spec} F \arrow[r] & B \end{tikzcd}$$

where B is a smooth projective curve over $\mathbb{C}$, $F = \mathbb{C}(B)$, and X a smooth projective variety over F with a regular projective model $\mathcal{X} \to B$. Fix a finite set $\{b_j\} \subset B$, $x_j \in \mathcal{X}_{b_j}$ smooth points, and local Taylor series data at these points, $s_j \in \mathcal{X}(\mathcal{O}_{B,b_j}/\mathfrak{m}_{b_j}^{n_j+1})$, $s_j(b_j) = x_j$.

Definition. $\mathcal{X}$ satisfies *weak approximation* if for any such set of data there exists $s : B \to X$ so that $s = s_j \pmod{\mathfrak{m}_{b_j}^{n_j+1}}$.

Remarks.

A. $\mathcal{X}$ satisfies weak approximation if and only if for each regular model $\mathcal{X}_1 \to \mathcal{X}$, and points $\{b_j\} \subset B$ and smooth points $x'_j \in (\mathcal{X}_1)_{b_j}$, there exists a section $s : B \to \mathcal{X}_1$ with $s(b_j) = x'_j$.

B. If $\mathcal{X}_1, \mathcal{X}_2$ are models of X, then $\mathcal{X}_1$ satisfies weak approximation if and only if $\mathcal{X}_2$ does, so it makes sense to say X *satisfies weak approximation.*

C. F-rational varieties satisfies weak approximation.

Rationally connected case

Let $X \to F = \mathbb{C}(B)$ be rationally connected, with model $\mathcal{X} \to B$. Here we have the theorem:

Theorem (Graber, Harris, Starr; Kollár)**.** *There exists a section $s : B \to \mathcal{X}$. Choose points $\{b_j\} \subset B$ such that the fibres $\mathcal{X}_{b_j}$ are smooth, and choose points $x_j \in \mathcal{X}_{b_j}$; then there exists a section $s : B \to X$ with $s(b_j) = x_j$.*

This will not give Taylor series data, because once one blows up to get the second-order Taylor series, the fibres are no longer irreducible.

All the fibers of $\mathcal{X} \to B$ are rationally *chain* connected, except for the degenerate fibers (e.g., reducible fibers), which might have to go through singular points. Also, for example, the cone over an elliptic curve $x^3 + y^3 + z^3 = 0$ is rationally chain connected but is not itself rationally connected.

Problem. *Let X/F be a smooth projective variety, $F = \mathbb{C}(B)$, B a curve. If X is rationally connected, show that X satisfies weak approximation.*

Effectivity

Problem. *Given $b_j \in B$, $D_{jk} \in \mathcal{X}_{b_j}$ of multiplicity one, does there exist an effective curve class $[M]$ such that $[M] \cdot \mathcal{X}_b = m$, and $[M] \cdot D_{ij} = m$.*

Let Y be a projective smooth variety over $\mathbb{C}$. We have $NS(Y) \subset H^2(Y, \mathbb{Z})$, the Néron-Severi group, and $N_1(Y) \subset H_2(Y, \mathbb{Z})$, the 1-cycles. We have the cone $\overline{NE}^1(Y) \subset NS(Y)_{\mathbb{R}}$, the cone of effective divisors; we also have the cone of moving curves $\overline{\mathrm{Mov}}_1(Y) \subset N_1(Y)_{\mathbb{R}}$, consisting of cycle classes $[M]$ such that M is irreducible and passes through the generic point of Y.

Given an effective divisor D and a moving class M, then $D \cdot M \geq 0$.

Note that $\overline{NE}^1(Y) \subset \overline{\mathrm{Mov}}_1(Y)^*$, the dual cone.

Theorem (Demailly, Peternell)**.** *Equality holds, $\overline{NE}^1(Y) = \overline{\mathrm{Mov}}_1(Y)^*$.*

As an application, this allows us to find $[M] \in \overline{\mathrm{Mov}}^1(\mathcal{X})$ with the desired intersection properties.

A.9 Heath-Brown: Rational Points and Analytic Number Theory

Analytic number theory is often quite useful in questions on rational points on varieties. For example, using the circle method, weak approximation gives formulas of the type

$$N(B) \sim CB^k (\log B)^j$$

where

$$C = \sigma_\infty \prod_p \sigma_p.$$

What kind of asymptotic formulae can we expect when weak approximation fails? Look at

$$L_1(x_1,x_2)L_2(x_1,x_2) = x_3^2 + x_4^2$$
$$L_3(x_1,x_2)L_4(x_1,x_2) = x_5^2 + x_6^2$$

where $L_i(x_1, x_2)$ are linear forms over $\mathbb{Z}$. This is the intersection of two quadrics in $\mathbb{P}^5$. In this case, the Hasse principle may fail, and weak approximation may fail. We take

$$H(x_1,\dots,x_6) = \max(|x_1|,|x_2|).$$

We have the following "theorem": There is a modification of the Hardy-Littlewood formula in which

$$C = \kappa\sigma_\infty \prod_p \sigma_p$$

where $\kappa \in [0,2]$, κ vanishes precisely when the Hasse principle fails, κ is built from information at a finite number of 'bad' places, and $\kappa \in \mathbb{Q}$ is easily calculable. To do this, use a "descent" process followed by variation of the circle method.

Theorem (H-B, Moroz)**.** *Let $a, b \in \mathbb{N}$ be coprime, with $a \equiv \pm 2, \pm 3 \pmod 9$. Then the surface*

$$x_1^3 + 2x_2^3 + ax_3^3 + bx_4^3 = 0$$

has a nontrivial rational point.

To prove this, there are two ingredients. First, a result of Satgé: $x_1^3 + 2x_2^3 = p$ has a rational point if p is prime, $p \equiv 2 \pmod 9$ (proved by Heegner point construction). Second, $ax_3^3 + bx_4^3$ takes infinitely many prime values $2 \pmod 9$.

In the other direction, analytic number theorists are often interested in rational points on varieties. We take the counting function

$$N(F;B) = \#\{F(x_1,\dots,x_n) = 0 : \max|x_i| \le B,\ x \in \mathbb{Z}^n\}.$$

For instance, take $F(x) = a_1x_1^3 + \cdots + a_nx_n^3$; there exists an asymptotic formula $n \ge 8$ (Vaughan). In the case $n = 7$, analytic methods establish a local-global principle, but not an asymptotic formula. To handle this case, we would want:

Conjecture. *We have*

$$N(F_0;B) \ll B^\theta$$

for some constant $\theta < 7/2$, where

$$F_0(x) = x_1^3 + x_2^3 + x_3^3 - x_4^3 - x_5^3 - x_6^3.$$

This is known for any $\theta > 7/2$, and conjectured to be true for any $\theta > 3$, so it is reasonable to expect.

What about $N(F_0, B)$ for $F_0 = x_1^d + x_2^d + x_3^d - x_4^d - x_5^d - x_6^d$? We can show $\theta < 7/2$ for $d \ge 24$. This variety has lines in trivial planes of the type $x_1 = x_4, x_2 = x_5, x_3 = x_6$, and no other lines if $d \ge 5$; what other quadric or low degree curves can be found?

Proposition (Green 1975)**.** *Any curve of genus* 0 *or* 1 *in* $F_0 = 0$ *has* x_i/x_j *constant for some* i, j, *as soon as* $d \geq 25$.

(Here $25 = (6-1)^2$.) This involves meromorphic functions and Nevanlinna theory.

Question. To what extant can one reduce the number 25 for quadratic curves?

Proposition (Davenport 1963)**.** *Any cubic form* $F(x) \in \mathbb{Z}[x]$ *in* $n \geq 16$ *variables has a nontrivial integer zero.*

This applies to an arbitrary cubic form; there is a better result for smooth forms with $n \geq 9$. Define a matrix $J(X)$ with entries

$$J(X)_{ij} = \frac{\partial^2 F}{\partial x_i \partial x_j}$$

and $V_m = \{x : \operatorname{rk} J(x) \leq m\} \subset \mathbb{P}^{m-1}$. Assume that $F(x) = 0$ has no nontrivial rational point; then any component C of V_m which has a rational point has $\dim C \leq m - 1$.

Question. What about components C without a rational point?

Vinogradov's mean value theorem refers to the counting function of the variety defined by the equations

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j$$

for $1 \leq j \leq k$, $V(k,s) \subset \mathbb{P}^{2s-1}$, count $0 < x_i, y_i \leq B$. This is a cone with vertex $(1 : \cdots : 1; 1 : \cdots : 1)$.

One can easily show $N(B) \gg B^s, B^{2s-k(k+1)/2}$ for all s, k; if $k \geq s$ then x is a permutation of y, $N(B) \sim s! B^s$. In fact, $N(B) \sim cB^s$ for $s = k+1$ (Vaughan, Wooley).

For $s \geq s_0(k) \sim k^2 \log k$, we have $N(B) \sim cB^{2s-k(k+1)/2}$.

Question. Can we find how $N(B)$ behaves for 'in-between' values?

Applications: Exponential sums, zero-free region for $\zeta(s)$ and the error term in the prime number theorem. So this question has several far-reaching implications!

Question. Can one prove $N(B) \sim cB^s$ for $k = 4$, $s = 6$? If L is a linear space of projective dimension ℓ, and $C \subset V(4,6) \cap L$, such that C is not contained in the subset of points where x is a permutation of y, is $\dim C \leq (2\ell - 1)/3$?

A.10 Mazur: Families of rationally connected subvarieties

Introduction

This is joint work with Graber, Harris, and Starr.

Throughout, we let k be any finite field and K a field of transcendence degree 1 over $\mathbb{C}$. We have two classical results, due to Chevalley-Warning and Tsen, for k and K, respectively: a hypersurface of low degree has a rational point; a *hypersurface of low degree* X is one with $\deg X \leq \dim X + 1$.

Inspired by these theorems, one (i.e. Artin) defines a field F to be *quasi-algebraically closed* if every hypersurface of low degree over F has a F-rational point. In view of resent results due to Kollár, Kollár-Miyaoka-Mori, and Graber-Harris-Starr, we ask similar questions not for hypersurfaces but for certain other classes of varieties.

We generalize the notion of hypersurfaces of low degree to rationally connected varieties over $\mathbb{C}$ which are projective and smooth: a variety X is *rationally connected* if for any two points $p, q \in X$, there exists a rational curve $C \subset X$ with $p, q \in C$. Rationally connected varieties are closed under birational transformation, products, domination (if $X \to Y$ is dominant, and X is rationally connected, then Y is rationally connected), and specialization. This is a much better class of varieties than, say, rational varieties (consider the difficulty in determining which cubic 4-folds are rational).

There is another candidate for a generalization of hypersurfaces of low degree: a variety X over F is *$\mathscr{O}$-acyclic* if

$$h^i(X, \mathscr{O}_X) = \begin{cases} 1, & i = 0 \\ 0, & i > 0. \end{cases}$$

Rationally connected varieties are $\mathscr{O}$-acyclic.

The only rationally connected curves are rational curves; the only rationally connected surfaces are rational surfaces. However, there are $\mathscr{O}$-acyclic surfaces which are not rational, e.g. Enriques surfaces.

Theorem. *If X is a smooth hypersurface over $\mathbb{C}$, then it is equivalent for X to be of low degree, rationally connected, and $\mathscr{O}$-acyclic.*

Theorem (Generalized Chevalley-Warning; Katz)**.** *Any $\mathscr{O}$-acyclic variety over k has a k-rational point.*

Over $\mathbb{C}$, and given an endomorphism $f : X \to X$, one defines the Lefschetz number $L(f) = \sum(-1)^i \operatorname{tr}(F|H^i)$; this complex number measures the fixed point locus of f. Over a finite field, the Lefschetz number counts the number of fixed points, at least modulo p; one computes that the Lefschetz number is 1 mod p.

For the generalization to rationally connected varieties over K, a variety X over K can be thought of as a family of rationally connected varieties over a curve $X \to C$. By *family* we always mean that although the base C might not be proper or smooth, the morphism is proper and generically smooth.

Theorem (Generalized Tsen; Graber, Harris, Starr)**.** *Any rationally connected variety over K has a K-rational point.*

A converse

Given a family $X \to B$, a section is a triangle

$$\begin{tikzcd} B \arrow[r] \arrow[dr, ""'{name=D}] & X \arrow[d] \\ & B. \end{tikzcd}$$

We define a *pseudo-section* to be a triangle

$$\begin{tikzcd} S \arrow[r] \arrow[dr] & X \arrow[d] \\ & B; \end{tikzcd}$$

where $S \to B$ is a family of rationally connected varieties. Since a point is rationally connected, a section gives a pseudo-section.

We can rephrase the GHS theorem in this language as follows: If $f : X \to B$ is a family with a pseudo-section, then its restriction $f_C : X_C \to C$ to every smooth curve $C \hookrightarrow B$ has a section.

Theorem (Weak converse to GHB)**.** *If $f : X \to B$ is a family such that every restriction $f_C : X_C \to C$ for every smooth curve $C \hookrightarrow B$ has a section, then $f : X \to B$ has a pseudo-section.*

This theorem is related to Lefschetz's theorem about π_1 as can be seen by restricting attention to finite étale covers.

Applications

This theorem has application to finding varieties X/K with no rational point; in particular:

Corollary. *There exists an Enriques surface over some K with no K-rational point.*

This is completely ineffective; an open question is to find the genus of the curve given by this counterexample.

Question. Is there an Enriques surface over $\mathbb{Q}(t)$ with no rational point over $\mathbb{C}(t)$?

Every Enriques surfaces over k has a point over k; this is not the case over K, so we have distinguished finite fields from function fields of transcendence degree 1 over $\mathbb{C}$. We ask: in the Artin-Lang philosophy, what kinds of varieties are cut out by $\mathscr{O}$-acyclic varieties?

We have another corollary:

Corollary. *A family of curves of genus* 1 *over a base B has a section if and only if it has a section over every curve $C \subset B$.*

The corollary is clear: a family of curves of genus 1 has no room for a pseudo-section.

Number Theoretic Applications

Now we consider $\pi : X \to B$ a family defined over a number field; we say π is *arithmetically surjective* if and only if $X(L) \to B(L)$ is surjective for all finite extensions L/F.

If $X \to B$ is a family of curves of genus ≥ 1, is it the case that arithmetic surjectivity is equivalent to the existence of a section over F? This question is unapproachable in full generality.

Instead, let us take a very small fragment of it: let B be a nonempty open subset of $\mathbb{P}^1$ over $F = \mathbb{Q}$, $X \to B$ a family of genus 1 curves, we say it *belongs to its Jacobian* $E \to B$. We consider quadratic twist elliptic pencils; given any $E_1/\mathbb{Q} : y^2 = g(x)$, we have the pencil $E_t/\mathbb{Q} : ty^2 = g(x)$. We have the problem: For all $X \to B$ belonging to E_t, is is true that arithmetic surjectivity holds if and only if a section exists? Work of Skinner-Ono can be used to establish this for all elliptic curves $E_1/\mathbb{Q}$.

A.11 Peyre: Motivic height zeta functions

Manin's principle in the functional case

The setting

Notation: let p be a prime number, $q = p^k$, $\mathcal{C}$ a smooth projective curve over $\mathbb{F}_q$, $K = \mathbb{F}_q(\mathcal{C})$. A point $x \in \mathbb{P}^N_K$ induces a function

$$\tilde{x} : \mathcal{C} \to \mathbb{P}^N_{\mathbb{F}_q}$$

and we define a height

$$h_N(x) = \begin{cases} \deg(\tilde{x}^*(\mathcal{O}(1)) & \text{if } \tilde{x} \text{ is not constant} \\ 0 & \text{otherwise} \end{cases}$$

Now let V be a smooth, geometrically integral projective variety over K, let $U \subset V$ be an open subset, and define

$$Z_{U,k}(T) = \sum_{x \in U(k)} T^{h(x)}, \quad \zeta_{U,k}(s) = Z_{U,k}(q^{-s}). \tag{1}$$

We make the following assumptions

- ω_V^{-1} is very ample
- $\omega_V^{-1} = \phi^*(\mathcal{O}(1))$
- $H^1(V, \mathcal{O}_V) = 0$, $H^2(V, \mathcal{O}_V) = 0$
- $V(K)$ is Zariski dense

Problems

- Find the value of $\theta = \inf\{\sigma | \zeta_{V,k}(s)$ converges if the real part $\Re(s) = \sigma\}$.
- Find the order of the pole of $\zeta_{U,k}$ at θ.
- Find the leading coefficient of the Laurent series at θ.

Questions For small enough U,

- Is $\theta = 1$?
- Is the order of $\zeta_{U,k}(s)$ at θ equal to $t = \operatorname{rank} \operatorname{Pic}(V)$?
- Is the leading term of $\zeta_{U,k}(s)$ at θ equal to $\theta^*_h(V)/(s-1)^t$, where

  $$\theta^*_h(V) = \alpha^*(V) w_h(\overline{V(K)})$$

  where $\alpha^*(V)$ can be defined in terms of the cone of effective divisors $C^1_{eff}(V) \subset \operatorname{Pic} V \otimes \mathbb{R}$, $w(h)$ is some adelic measure, and $\overline{V(K)}$ is the closure of the rational points?

Results Answers are positive if

- $V = G/P$ where G is a reductive group over K and P is a smooth parabolic subgroup of G (Morris, EP).
- V is a smooth toric projective variety (D. Bourgui), U an open orbit of V.
- $V \subset \mathbb{P}^N_K$ is a hypersurface with $N >> \deg V$ (circle method).

Simplest example: $V=\mathbb{P}^n_K$. Let g be the genus of $\mathcal{C}$.

$$Z_{V,k}(t)=q^{n(1-g)}\frac{\zeta_K((n+1)s-n)}{\zeta_K((n+1)s)}+q^{(n-1)(1-g)}\frac{\zeta_K((n+1)s-(n-1))}{\zeta_K((n+1)s)}+\dots$$
$$+q^{1-g}\frac{\zeta_K((n+1)s-1)}{\zeta_K((n+1)s)}+\frac{Q(q^{-s})}{\zeta((n+1)s)}.$$

where Q is a polynomial.

Motivic setting

Work in progress with A Chambert-Loir.

The ring of motivic integration

(Kontsevich, Denef, Loeser)

Definition: Let k be a field, and let $\mathcal{M}_k$ be the ring with generators $[V]$ as V ranges through varieties over k, subject to the relations $[V]=[V']$ if $V=V'$ and $[V]=[U]+[V-U]$, for U open in V, and with multiplication given by the product of varieties.

(Note: De Jong pointed out some problem with this definition in positive characteristic.)

Now let $\mathbb{L}=[\mathbb{A}^1_k]$, $\mathcal{M}_{loc}=\mathcal{M}_k[\mathbb{L}^{-1}]$. Define a filtration by

$$F^m\mathcal{M}_{loc}=\text{subring generated by }[V]\mathbb{L}^{-i}\text{ if }i-\dim V\geq m.$$

Let $\hat{\mathcal{M}}=invlim\mathcal{M}_{loc}/F^m\mathcal{M}_{loc}$.

Motivic height Let the notation be as in Section . Given an embedding $\phi:V\to\mathbb{P}^N_K$ we get a height $h:V(K)\to\mathbb{N}$. Given an open $U\subset V$, we can define varieties U_n/k such that for all k'/k,

$$U_n(k')=\{x\in V(K')|h_{K'}(x)=n\},$$

where $K'=k'(\mathcal{C})$. Then define

$$Z_{U,k}(T)=\sum_{n\in\mathbb{N}}[U_n]T^n\in\mathcal{M}_k[[T]].$$

Examples:

- If V is defined over k, $V_0=V$, $V_n=\mathrm{Mor}_n(\mathcal{C},V)$, morphisms of degree n
- If $V=\mathbb{P}^n_K$,
$$Z_K(T)=\sum_{i\in\mathbb{N}}[\mathcal{C}^{(i)}]T^i$$
where $\mathcal{C}^{(i)}$ is the ith symmetric product.
$$Z_{\mathbb{P}^N_K,h}(T)=\mathbb{L}^{n(1-g)}\frac{Z_K(T^{n+1}\mathbb{L}^n)}{Z_K(T^{n+1})}+\frac{Q(T)}{Z_K(T^{n+1})}$$

Proposition (Kapanov)**.** A. *$Z_K(T)$ is a rational function.*
B. *$(1-T)(1-\mathbb{L}T)Z_K(T)$ is a polynomial.*
C. *$Z_K(1/\mathbb{L}T)=\mathbb{L}^{1-g}T^{2-2g}Z_K(T)$.*

Theorem (Follows from Kapanov)**.** *Let G be a split semi-simple proper algebraic group over k, $P\subset G$ a standard parabolic subgroup, $V=G/P$. Assume that $\phi^*(\mathcal{O}(1))=\omega_V^{-1}$. Then*

A. *$Z_{V,k}(T)$ converges in $\hat{\mathcal{M}}$ for $T = \mathbb{L}^{-k}$, $k > 1$.*
B. *$[(1 - \mathbb{L}T)^t Z_{V,k}(T)](\mathbb{L}^{-1})$ converges in $\hat{\mathcal{M}}$.*
C. *One can give a description of its value similar to the functional case.*

Theorem (D. Bourgui)**.** *Suppose that V is a split toric variety over k. Then 1, 2, and 3 of the previous theorem hold for $U \subset V$, U an open orbit.*

Hope: generalize this to smooth cellular varieties over k.

Remark: Batyrev has a nice idea to attack this when V is defined over k. But we have no idea what the relevant harmonic analysis is in this case.

A realization map Suppose $k = \mathbb{F}_q$, and define a map $\mathcal{M}_k \to \mathbb{Z}$, $[V] \mapsto \#V(\mathbb{F}_q)$. Then we get a map

$$\begin{array}{ccc} \mathcal{M}_{loc} & \to & \mathbb{Z}[q^{-1}] \\ \mathbb{L}^{-1} & \mapsto & q^{-1} \end{array}$$

which takes $Z_{U,k}^{Mot}(T)$ to $Z_{U,k}^{funct}(T)$.

A.12 Raskind: Descent on Simply Connected Algebraic Surfaces

This is joint work with V. Scharaskin.

$K3$ Surfaces of Picard Number 20

Let k be a field, usually finitely generated over the prime subfield ($\mathbb{Q}$), $\overline{k}$ a separable closure of k. Let X/k be a smooth, projective geometryicall connected, geometrically simply connected surface. ($\pi_1(\overline{X}) = \{1\}$, where $\overline{X} = X \times_k \overline{k}$.) Let $G = \mathrm{Gal}(\overline{k}/k)$, ℓ a prime number, $\ell \neq \operatorname{char} k$.

Point of the talk: It should be possible to do descent on (at least some) surfaces with nonzero geometric genus.

For example, we consider $K3$ surfaces with geometric Picard number 20 (maximal) in characteristic zero:

Proposition (Inose-Shioda)**.** *All $K3$ surfaces over $\mathbb{C}$ with Picard number 20 are defined over $\mathbb{Q}$, and may be realized as (double covers) of $\mathrm{Kum}(E \times E')$, where E, E' are isogenous elliptic curves with CM.*

Kummer theory says: There is an exact sequence

$$0 \to \mathrm{Pic}(\overline{X})/\ell^m \,\mathrm{Pic}(\overline{X}) \to H^2(\overline{X}, \mathbb{Z}/\ell^m(1)) \to \mathrm{Br}(\overline{X})[\ell^m] \to 0;$$

since $\mathrm{Pic}(\overline{X}) \cong NS(\overline{X})$, as you pass to the limit over m, one has the exact sequence

$$0 \to NS(\overline{X}) \otimes \mathbb{Z}_\ell \to H^2(\overline{X}, \mathbb{Z}_\ell(1)) \to T_\ell(\mathrm{Br}(\overline{X})) \to 0.$$

The term $NS(\overline{X}) \otimes \mathbb{Z}_\ell$ is algebraic, the term $T_\ell(\mathrm{Br}(\overline{X}))$ transcendental.

Tensoring with $\mathbb{Q}_\ell$, we expect:

Conjecture (Tate Conjecture)**.** *The map*

$$\mathrm{Pic}(\overline{X}) \otimes \mathbb{Q}_\ell \to H^2(\overline{X}, \mathbb{Q}_\ell(1))^G$$

is surjective.

Proposition. *If X is a geometrically simply connected surface, and the Tate conjecture is true, then the ℓ-primary component of* $\mathrm{Br}(X)/\mathrm{Br}(k)$ *is finite.*

Proposition. *Suppose X as above has a good reduction modulo p with the same geometric Picard number (not always true), and k is a number field. If the Tate conjecture is true, then* $\mathrm{Br}(X)/\mathrm{Br}(k)$ *is finite.*

Corollary. *If X is a $K3$ of geometric Picard number* 20*, then* $\mathrm{Br}(X)/\mathrm{Br}(k)$ *is finite.*

Sketch of proof. Use Inose-Shioda result and Faltings-Deligne which prove Tate for X, and go modulo a prime that splits in the CM-field of E. □

Rapid review of descent

Descent by Colliot-Thélène and Sansuc. Let X be a geometrically simply connected surface, and $p_g = 0$. Let S_k be the torus whose group of characters is $\mathrm{Pic}(\overline{X})$, and $S_X = S_k \times_k X$. There is an exact sequence

$$0 \to H^1(k, S) \to H^1(X, S) \xrightarrow{\chi} H^1(\overline{X}, S)^G \to H^2(k, S) \to H^2(X, S)$$

coming from the Hochschild-Serre spectral sequence. We identify

$$H^1(\overline{X}, S)^G \cong \mathrm{Hom}_G(\mathrm{Pic}\,\overline{X}, \mathrm{Pic}\,\overline{X}),$$

and we think of $H^1(X, S)$ as principal homogeneous spaces under S; an element $[\mathcal{T}] \in H^1(X, S)$ is a universal torsor if $\chi([\mathcal{T}]) = \mathrm{id}$.

One has a pairing

$$X(k) \times H^1(X, S) \to H^1(k, S)$$
$$P, [\mathcal{T}] \mapsto \mathcal{T}_P;$$

every torsor $\mathcal{T}$ comes with a map $f_{\mathcal{T}} : \mathcal{T} \to X$, and $\mathcal{T}_P = 0$ if and only if $P \in f_{\mathcal{T}}(\mathcal{T}(k))$.

Now assume X only geometrically simply connected (not necessarily $p_g = 0$). $H^2(\overline{X}, \mathbb{Z}_\ell(1))$ has no integral structure (i.e. there is not a $\mathbb{Z}[G]$ module M such that $M \otimes \mathbb{Z}_\ell \cong_G H^2(\overline{X}, \mathbb{Z}_\ell(1))$, so we must use étale cohomology.

If $p : X \to Y$ is any morphism of schemes, and $\mathscr{F}$ a sheaf on $Y_{\text{ét}}$, $\mathscr{G}$ a sheaf on $X_{\text{ét}}$, then there is a spectral sequence

$$E_2^{r,s} = \mathrm{Ext}^r_Y(\mathscr{F}, R^s p_* \mathscr{G}) \Rightarrow \mathrm{Ext}^{r+s}_X(p^*\mathscr{F}, \mathscr{G}).$$

Apply this general situation with $p : X \to \mathrm{Spec}(k)$ the structure morphism, $\mathscr{F} = H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1))$, $\mathscr{G} = \mathbb{Z}/n\mathbb{Z}(1)$. One obtains a map

$$\mathrm{Ext}^2_X(p^* H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1)), \mathbb{Z}/n\mathbb{Z}(1)) \to \mathrm{End}_k(H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1)))$$

coming from the $E_2^{0,2}$ term in the spectral sequence. We expect that the group $\mathrm{End}_k(H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1)))$ will play the role of $\mathrm{Hom}_G(\mathrm{Pic}\,\overline{X}, \mathrm{Pic}\,\overline{X})$ in the above.

Why is there a shift, and how does this relate to the Colliot-Thélène-Sansuc result when $p_g = 0$? Kummer theory on S gives

$$0 \to S[n] \to S \xrightarrow{n} S \to 0$$

and

$$0 \to H^1(X, S)/nH^1(X, S) \to H^2(X, S[n]) \to H^2(X, S)[n] \to 0.$$

We have a map

$$\begin{aligned} &H^2(X, \mathscr{H}om(p^*H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1)), \mathbb{Z}/n\mathbb{Z}(1)) \\ &\qquad \to \mathrm{Ext}^2_X(p^*H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1)), \mathbb{Z}/n\mathbb{Z}(1)) \end{aligned}$$

coming from the local-to-global spectral sequence, and we can identify

$$H^2(X, \mathscr{H}om(p^*H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(1)), \mathbb{Z}/n\mathbb{Z}(1)))) \cong H^2(X, p^*H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(2))).$$

Let χ be the composite of these three maps. Let $n = \ell^m$.

Definition. A *universal n-gerbe* is an element $\mathscr{G} \in H^2(X, p^*H^2(\overline{X}, \mathbb{Z}/n\mathbb{Z}(2)))$ such that $\chi([G]) = \mathrm{id}$.

One can (with care and difficulty) pass to $\varinjlim_m$ to speak of universal ℓ-adic gerbes. The set of universal ℓ-adic gerbes is either empty or a principal homogeneous space under the image of $H^2(k, H^2(\overline{X}, \mathbb{Z}_\ell(2)))$ in $H^2(X, p^*H^2(\overline{X}, \mathbb{Z}_\ell(2)))$.

One has a pairing

$$\begin{aligned} X(k) \times \mathrm{Gerbes}(X, k, \ell) &\to H^2(k, H^2(\overline{X}, \mathbb{Z}_\ell(2))) \\ P, \mathscr{G} &\mapsto \mathscr{G}_P \end{aligned}$$

which gives a partition of $X(k)$. This can be extended to a map

$$\theta_{\mathscr{G}} : CH_0(X) \to H^2(k, H^2(\overline{X}, \mathbb{Z}_\ell(2)))$$

where $\mathscr{G}$ is a chosen universal gerbe. On $A_0(X)$, zero-cycles of degree 0, this is the higher ℓ-adic Abel-Jacobi map, and the image of this map is a finitely generated $\mathbb{Z}_\ell$-module; if k is a number field, one can show in some cases that that the image is finite, e.g. $K3$ of Picard number 20 over $\mathbb{Q}$ or over the CM field.

So, in these cases, have $X(k) = \bigsqcup f_\alpha \mathscr{G}_\alpha(k)$, where α ranges over a finite set.

We can show $X(\mathbf{A}_k)^{\mathrm{Br}_\ell} \neq \emptyset$ if and only if there exists a universal gerbe $\mathscr{G}$ with points everywhere locally.

A.13 Rotger: Shimura varieties

Let $\overline{k}$ be an algebraically closed field, A, $\mathcal{L}/\overline{k}$ a polarized abelian variety. We are interested in:

A. Field of moduli of $(A, \mathcal{L})$ and field of moduli of $\mathrm{End}(A)$
B. Fields of definition of $(A, \mathcal{L})$ and fields of definition of $\mathrm{End}(A)$.

The field of moduli of $(A, \mathcal{L})$ $\mathcal{K}_{A,\mathcal{L}}$ is the unique minimal field in $\overline{k}$ such that $(A, \mathcal{L})^\sigma = (A, \mathcal{L})$ for all $\sigma \in \mathrm{Gal}(\overline{k}/\mathcal{K}_{A,\mathcal{L}})$.

$$\begin{tikzcd}
 & & \mathcal{K}_{\mathrm{End}(A)} \\
 & \mathcal{K}_S \arrow[ur, no head] & \\
\mathcal{K}_{(A,\mathcal{L})} \arrow[ur, no head] & &
\end{tikzcd}$$

$\mathbb{Z} \subset S \subset \mathrm{End}(A)$. The top field is the unique field fixed by all σ such that there exists $A = A^\sigma$ making the following diagram commute:

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\beta\in\mathrm{End}(A)"'] & A^\sigma \arrow[d, "\beta^\sigma"] \\ A \arrow[r] & A^\sigma \end{tikzcd}$$

Shimura: the generic odd dimensional polarized abelian variety admits a model over $\mathcal{K}_{A,\mathcal{L}}$. The generic even dimensional polarized abelian variety does not admit a model over $\mathcal{K}_{A,\mathcal{L}}$.

(Silverberg) Fix $\mathcal{K}_{A,\mathcal{L}}$. There is a (unique, Galois) minimal field of definition $\mathcal{K}_S/K_{(A,\mathcal{L})}$ of $S \subset \mathrm{End}(A)$.

(Silverberg) There is a $H_{d,r}$ such that $|\mathrm{Gal}(K_S/K_{A,\mathcal{L}})| \leq H_{d,r}$ for any abelian variety A such that $\dim A = d$ and $S \subset \mathrm{End}(A)$ with $[S : \mathbb{Z}] = r$.

If A is simple, $\mathrm{End}(A)$ is an order in either a totally real field, a division algebra over a CM-field, or a quaternion algebra.

We will focus on the latter case.

Forgetful maps between Shimura varieties and rational points

Let F be a totally real number field, with $[F : \mathbb{Q}] = n$. Let B be an indefinite quaternion algebra over F (that is, $B \otimes_{\mathbb{Q}} \mathbb{R} = M_2(\mathbb{R})^n$). Let $\mathcal{O}_B$ be a maximal order in B. Let

$$\Gamma_B = \{\gamma \in \mathcal{O}_B : N_{B/F}(\gamma) = 1\} \subset SL_2(\mathbb{R})^n.$$

Moduli problem $(\mathcal{O}_B, \mu)$: classify principally polarized abelian varieties $(A, i, \mathcal{L})$ where A is an abelian variety of $\dim A = 2n$, $i : \mathcal{O}_B \to \mathrm{End}(A)$,and the Rosati involution has the form $*_{\mathcal{L}} : \mathcal{O}_B \to \mathcal{O}_B$, $b \mapsto \mu^{-1}\bar{b}\mu$ where $\mu \in \mathcal{O}_B$ such that $\mu^2 + \delta = 0$ and $\delta \in F^\times$.

Proposition. *If $(A, \mathcal{L})$ is a principally polarized abelian variety, then it forces $\delta = D$ where D is a totally positive generator of* $\mathrm{disc}(B)$.

(Shimura): The moduli functor is coarsely represented over $\mathbb{Q}$ by a complete algebraic variety $X_D/\mathbb{Q} = X_{(\mathcal{O}_B,\mu)}/\mathbb{Q}$, with $\dim X_D = n$. We havea $X_D(\mathbb{C}) = \Gamma_B\backslash\mathfrak{h}^n$, where $\mathfrak{h}$ is the Poincaré upper half plane.

Let R_F be the ring of integers of F, $R_F \subset S \subset \mathcal{O}_B$, where S is a totally real quadratic order over R_F. There are forgetful finite maps over $\mathbb{Q}$

$$X_{\mathcal{O}_B,\mu} \longrightarrow \mathcal{M}_S \longrightarrow \mathcal{M}_{R_F} \longrightarrow \mathcal{A}_{2n}$$

$$[A, i, \mathcal{L}] = P \longmapsto [A, i|_S, \mathcal{L}] \longmapsto [A, i|_{R_F}, \mathcal{L}] \longmapsto [A, \mathcal{L}]$$

where $\mathcal{M}$ is the Hilbert modular variety classifying varieties with real multiplication by the subscript. The dimensions of these moduli spaces are, respectively, n, n, $3n$, $2n^2 + n$.

The picture in $n = 1$ is

$$\text{Shimura curve: } X_{(\mathcal{O},\mu)} \to \text{Hilbert surface:}\mathcal{M}_S \to \text{Igusa's space:}\mathcal{A}_2.$$

We have a tower of fields

$$\mathcal{K}_{\mathrm{End}(A)} = \mathbb{Q}(P) \subset \mathcal{K}_S = \mathbb{Q}(P|_S) \subset K_{R_F} = \mathbb{Q}(P|_F) \subset \mathcal{K}_{A,\mathcal{L}} = \mathbb{Q}(P_0).$$

The automorphism group of $X_D = X_{(\mathcal{O}_B,\mu)}$: is

$$(\mathbb{Z}/2)^{2r} = W = \frac{\mathrm{Norm}_{B_+^\times}(\Gamma_B)}{\Gamma_B \cdot F^\times} \subset \mathrm{Aut}_{\mathbb{Q}(X_D)}$$

where $2r = \#\{\mathfrak{p} | \operatorname{disc}(B)\}$.

Theorem. A.

$$\begin{tikzcd} X_{(\mathcal{O},\mu)} \arrow[r, "\pi_F"] & \mathcal{M}_{R_F} \arrow[d, "\textit{birational onto the image, isomorphism away from Heegner points}"] \\ & X_{(\mathcal{O}_B,\mu)}/W_0 \end{tikzcd}$$

where

$$W_0 = \begin{cases} (\mathbb{Z}/2)^{2w} & \textit{if } B + F + F\mu + F\chi + F\mu\chi = \left(\frac{-D,m}{F}\right) \textit{ (twisting case)} \\ (\mathbb{Z}/2)^2 & \textit{otherwise (non twisting case)} \end{cases}$$

$w = \#\{$*primitive roots of unity in* $F(\sqrt{-D})$ *of odd order*$\}$

B.

$$\begin{tikzcd} X_{(\mathcal{O},\mu)} \arrow[r, "\pi_F"] & \mathcal{M}_{S} \arrow[d, "\textit{birational onto the image, isomorphism away from Heegner points}"] \\ & X_{(\mathcal{O}_B,\mu)}/V_0 \end{tikzcd}$$

where $V_0 \subset W_0$,

$$V_0 = \begin{cases} (\mathbb{Z}/2) & \textit{in the twisting case} \\ \{1\} & \textit{otherwise} \end{cases}$$

Corollary. *Let* $(A, \mathcal{L})$ *be a principally polarized abelian variety with* $\mathrm{End}(A) = \mathcal{O}_B$, $\dim A = 2n$. *Then*

$$\mathrm{Gal}(\mathcal{K}_{\mathrm{End}\,A}/\mathcal{K}_F) \subset \begin{cases} (\mathbb{Z}/2)^{2w} & \textit{twisting case} \\ (\mathbb{Z}/2)^{w} & \textit{otherwise} \end{cases}$$

For any totally real R_F *properly in* S *properly in* $\mathcal{O}_B$.

$$\mathrm{Gal}(\mathcal{K}_{\mathrm{End}\,A}/\mathcal{K}_S) \subset \begin{cases} (\mathbb{Z}/2) & \textit{twisting case} \\ \{1\} & \textit{otherwise} \end{cases}$$

Field of definition for abelian surfaces

Let $(A, \mathcal{L})/K$ be a principally polarized abelian surface over a number field K with $\mathrm{End}_{\overline{K}}(A) = \mathcal{O}_B$, $\operatorname{disc}(B) = D$. There is a diagram

$$\begin{tikzcd} & K_{\mathrm{End}(A)} \arrow[dl, dash, "|G||48\ \text{(Silverberg)}"'] \arrow[dr, dash, "|G| \leq 2\ \text{(Jordan)}"] & \\ K \arrow[dr, dash, "|G| \leq 2\ \text{(Mestre)}"] & & \mathcal{K}_{\mathrm{End}(A)} \\ & \mathcal{K}_{A,\mathcal{L}} & \end{tikzcd}$$

A. If $B = \left(\frac{-D,m}{\mathbb{Q}}\right)$ for $0 < m < D$, $m|D$, then (with Dieulefait)

$$\mathrm{Gal}(K_{\mathrm{End}(A)}/K) = \begin{cases} \mathbb{Z}/2 \times \mathbb{Z}/2 & \text{in this case } \mathrm{End}_K(A) = \mathbb{Z} \\ \mathbb{Z}/2 & \mathrm{End}_K(A) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-D}), \mathbb{Q}(\sqrt{m}), \mathbb{Q}(\sqrt{D/m}) \\ \{1\} & \mathrm{End}_K(A) = \mathcal{O}_B \end{cases}$$

B. Otherwise,

$$\mathrm{Gal}(K_{\mathrm{End}(A)}/K) = \begin{cases} \mathbb{Z}/2 & \mathrm{End}_K(A) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-D}) \\ \{1\} & \text{otherwise} \end{cases}$$

A.14 Salberger: Arithmetic Bezout and Rational Points of Bounded Height

We take the height function

$$H : \mathbb{P}^n(k) \to \mathbb{R}_{>0}$$
$$x = (x_0 : \cdots : x_n) \mapsto \prod_v \sup_{0 \le i \le n} |x_i|_v$$

If $X \subset \mathbb{P}^n$ is a closed subvariety over k, $U \subset X$ an open subvariety also over k, we have the counting function

$$N(U, B) = \#\{x \in U(k) : H(x) \le B\}.$$

Conjecture (Batyrev-Manin)**.** *We have*

$$N(U, B) \ll_{X,\epsilon} B^{\alpha(D)+\epsilon}$$

if U is sufficiently small, X is smooth, and D a hyperplane divisor.

Already the case of smooth cubic surfaces, away from the 27 lines, this conjecture would imply linear growth, but it was only known recently for quadratic growth; therefore this is hard enough, looking for asymptotic formulas is often asking for too much.

Recently, there has been work which also works in low dimension (curves and surfaces), due to Heath-Brown (2002); this also has applications to other problems (e.g. Waring's problem).

Theorem (Heath-Brown)**.** *Let $X_d \subset \mathbb{P}^n$ be an absolutely irreducible curve of degree d; then*

$$N(X_d, B) \ll_{n,d,\epsilon} B^{2/d+\epsilon}.$$

The implicit constant does not depend on X_d; the results of Faltings have no uniformity. We have applications to surfaces. This result is also best possible, taking the Veronese embedding of $\mathbb{P}^1$. There was a result of Bombieri-Pila which proved $\ll_{d,\epsilon} B^{1+1/d+\epsilon}$. Broberg treats arbitrary number fields k (and the case $n > 3$).

This theorem relies on the following result, which is Theorem 14 in the paper of Heath-Brown.

Theorem (Theorem 14)**.** *Let $X_d \subset \mathbb{P}^n$ be an absolutely irreducible projective $\mathbb{Q}$-variety of dimension r defined by forms of degree $\le \delta$. Let $\epsilon > 0$, $B \ge 1$ be given. Then there exists a $\mathbb{Q}$-hypersurface $Y \subset \mathbb{P}^n$ such that:*

(i) $X_d \not\subset Y$;

(ii) *All $\mathbb{Q}$-points on X_d of height $\leq B$ lie on Y;*

(iii) *We have*

$$\deg(Y) \ll_{n,\delta,\epsilon} B^{\frac{r+1}{d^{1/r}}+\epsilon};$$

(iv) *The irreducible components of Y have degrees bounded in terms of n, δ, ϵ.*

Remark. Heath-Brown treats only the case $r = n-1$. Taking $r = 1$, the result of Heath-Brown is an immediate consequence of this theorem if one applies Bezout's theorem in the plane. The case $r < n-1$ is due to Broberg, and with arbitrary k.

If X is smooth, then you may replace δ by d in (iii) and (iv).

Lemma (Colliot-Thélène)**.** *Let $X_d \subset \mathbb{P}^3$ be a smooth projective surface. Then there exists at most $\ll_d 1$ curves of degree $d-2$ on X.*

This implies that a cubic has only finitely many lines, a quartic has only finitely many conics, and so on. This is best possible, for $d-1$ one might have infinitely many such curves, for example, infinitely many conics on a cubic surface. Removing these curves, we still have a surface, and we get:

Theorem (Heath-Brown)**.** *Let $X_d \subset \mathbb{P}^3$ be a smooth projective surface and let U be the complement of all curves of degree $\leq d-2$. Then*

$$N(U, B) \ll_{d,\epsilon} B^{\frac{3}{\sqrt{d}}+\frac{2}{d-1}+\epsilon}.$$

This is the best known result if $d \geq 6$. To do this, apply Theorem 14 by cutting with an auxiliary hyperplane; the same implicit constant applies everywhere, the $B^{3/\sqrt{d}+\epsilon}$ is the maximum number of irreducible components. We considering for example the Veronese embedding of the projective plane to see that we would expect $\ll B^{3/\sqrt{d}+\epsilon}$.

Theorem (S)**.** *Let $X_d \subset \mathbb{P}^n$ be a* smooth *absolutely irreducible projective $\mathbb{Q}$-variety of dimension r defined by forms of degree $\leq \delta$. Let $\epsilon > 0$, $B \geq 1$ be given. Then there exists a $\mathbb{Q}$-hypersurface $Y \subset \mathbb{P}^n$ such that:*

(i) *$X_d \not\subset Y$;*

(ii) *All $\mathbb{Q}$-points on X_d of height $\leq B$ lie on Y;*

(iii) *We have*

$$\deg(Y) \ll_{n,\delta,\epsilon} B^{\frac{r+1}{rd^{1/r}}+\epsilon}.$$

For the moment, it is not clear how to use this theorem to deduce $\ll B^{3/\sqrt{d}+\epsilon}$.

Proof. Let $Q_1(x), \ldots, Q_m(x)$ be monomials in $x = (x_0, \ldots, x_n)$ which form a basis of

$$\operatorname{img}(H^0(\mathbb{P}^n, \mathscr{O}(D)) \to H^0(X, \mathscr{O}(D))),$$

where $D \sim B^{(r+1)/(rd^{1/r})+\epsilon}$. Let $P_1, \ldots, P_\ell \in \mathbb{A}^{n+1}(\mathbb{Z})$ represent the $\mathbb{Q}$-points on X_d of height $\leq B$. We need to show that the rank of the matrix

$$\begin{pmatrix} Q_1(P_1) & \ldots & Q_1(P_\ell) \\ \vdots & \ddots & \vdots \\ Q_m(P_1) & \ldots & Q_m(P_\ell) \end{pmatrix}$$

is $< m$. This is trivial if $m > \ell$; otherwise, we must look at all sub $(m \times m)$-determinants. Since these points are of bounded height, each term in the determinant is bounded by B^D, so one has a bound on the archimedean height of the determinant. With more points, the determinants are divisible by high powers of prime numbers (by the Weil conjectures, points must coincide); under certain circumstances, these divisibilities contradict the bounds on the determinant. We use for example that

$$\sum_{p\le R}\frac{\log p}{p}\sim \log R.$$

This gives the result. □

Remark. The theorem is also true for surfaces with at most rational double points. Already, the theorem is not known for elliptic singularities.

We apply this theorem to count $\mathbb{Q}$-points on $X_d\cap Y$ when $\dim X_d = 2$. Then $\deg(Y)\ll_{d,\epsilon} B^{3/(2\sqrt{d})+\epsilon}$. By the adjunction formula (and Bezout),

$$\#(X_d\cap Y)_{\mathrm{sing}}(\mathbb{Q})\ll_d \deg(Y)^2\ll B^{3/\sqrt{d}+\epsilon}.$$

All $\mathbb{Q}$-points on irreducible, not absolutely irreducible components are singular. Therefore it suffices to count smooth $\mathbb{Q}$-points on absolutely irreducible components of $X_d\cap Y$. Let $Z_1,\dots,Z_s$ be absolutely irreducible components of $X_d\cap Y$ of degree $\le f(d,\epsilon)$, then

$$\sum_{i=1}^{s}\#N(Z_i,B)\ll_{d,\epsilon}(\textstyle\sum_i\deg Z_i)B^{(2/e)+\epsilon}$$

where $e=\min\deg(Z_i)$. This is

$$(\textstyle\sum_i\deg Z_i)B^{(2/e)+\epsilon}\ll_{d,\epsilon}B^{3/(2\sqrt{d})+2/e+\epsilon}.$$

If you throw out curves of smallest degree, this is smaller than $\ll B^{3/\sqrt{d}}$.

But we still must deal with curves of high degree, e.g. the case when $X_d\cap Y$ is irreducible.

Lemma. *Let $Z_\delta\subset\mathbb{P}^n$ be an absolutely irreducible degree δ, and p a prime $\gg_{n,\epsilon} B^{(2/\delta)+\epsilon}$. Then:*

(i) *The number of $\mathbb{Q}$-points on Z_δ of height $\le B$ which specializes to a given smooth $\mathbb{F}_p$-point on Z_δ is $\ll_{n,\epsilon}\delta$.*

(ii) *The number of $\mathbb{Q}$-points on Z_δ with smooth specialization at p is $\ll_{n,\epsilon}\delta B^{(2n/\delta)+\epsilon}$.*

Corollary. *We have*

$$\#N(Z_{\delta,smooth},B)\ll_{n,\epsilon}\delta^4B^{(2n/\delta)+\epsilon}.$$

If we could replace δ^4 by δ^2, then we would have get $N(U,B)\ll B^{(3/\sqrt{d})+\epsilon}$. It might still be useful to find something like $\delta^{5/2}$. Using arithmetic Bezout, bounding the heights of the subvarieties (due to Faltings), this might succeed. It would also be better to work systematically with all primes p, some savings might arise.

A.15 Skorobogatov: Counterexamples to the Hasse Principle...

This is joint work with Laura Basile.

We work over a field k with $\operatorname{char} k=0$, $\overline{k}$ its algebraic closure.

Definition. A *bielliptic surface* X is a $\overline{k}/k$-form of a smooth projective surface of Kodaira dimension 0 that is not $K3$, neither abelian nor Enriques.

There is a complete list of such available. We have $K_X \neq 0$, but $nK_X = 0$, for $n = 2, 3, 4$ or 6. Over the algebraic closure, $\overline{X} = E \times F/\Gamma$, where Γ acts on E' by translations.

Proposition. *There exists an abelian surface A/k, a principal homogeneous space Y of A, and a finite étale morphism $f : Y \to X$, $\deg f = n$.*

Proof. Since $nK_X = (g)$, then consider $t^n = g$ and normalize; the map is unramified, so $K_Y = f^*K_X = 0$. By the classification of surfaces, $\overline{Y}$ is an abelian surface. (f is a torsor under μ_n.) □

Remark. This will not hold in higher dimension; there are just many more possibilities.

Consider $A = E \times F$, $Y = C \times D$, C a principal homogeneous space of E, and likewise D for F. Now μ_n acts on Y so that μ_n acts on D by translations, $\mu_n \subset F$; the action on μ_n on C cannot be by translations or else X itself would be a principal homogeneous space, so the action has fixed points.

Proposition. $[C] \in \operatorname{img}(H^1(k, E^{\mu_n}) \to H^1(k, E))$.

Proof. Take $\overline{x} \in C(\overline{k})$, fixed by μ_n, and write down the usual cocycle: if $g \in \operatorname{Gal}(\overline{k}/k)$, $g\overline{x} - \overline{x} \in E^{\mu_n}(\overline{k})$.

(It arises from $[C^{\mu_n}]$.) □

Corollary. *Let $\alpha : E \to E_1$ be the isogeny with kernel E^{μ_n}. Then $[C] \in H^1(k, E)[\alpha_*]$.*

We have one of the following possibilities:

n	$\#E^{\mu_n}$
6	1 (so $C(k) \neq \emptyset$)
4	2
3	3
2	4

Now assume $k = \mathbb{Q}$, and $X(\mathbf{A}_{\mathbb{Q}}) = \prod_v X(\mathbb{Q}_v)$; we want an example where $X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$, but $X(\mathbb{Q}) = \emptyset$. We do the case $n = 3$.

With the notation as above:

Theorem. *Assume that:*

(i) $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *acts nontrivially on E^{μ_3}, which is $\cong \mathbb{Z}/3\mathbb{Z}$ as an abstract group;*
(ii) $\#Ш(E)[\alpha_*] = 3$*;*
(iii) $[C] \in Ш(E)[\alpha_*]$*;*
(iv) $\mu_3 \subset F$*;*
(v) $\operatorname{Sel}(F, \mu_3) = 0$*, that is, for any principal homogeneous space of F obtained from a class in $H^1(\mathbb{Q}, \mu_3)$, there exists a place v where it has no point.*

Then $X = (C \times F)/\mu_3$ is a counterexample to the Hasse principal not explained by the Manin obstruction.

Example. If $C : x^3 + 11y^3 + 43z^3 = 0$, μ_3 acts by $(x : y : z) \mapsto (x : y : \zeta_3 z)$, $F = D : u^3 + v^3 + w^3 = 0$, with μ_3 acting by $(u, v, w) \mapsto (u : \zeta_3 v : \zeta_3^2 w)$; looking at the Selmer group, you look at principal homogeneous spaces of the form $u^3 + av^3 + a^2u^3 = 0$, so if $p \mid a$, this has no $\mathbb{Q}_p$ point.

We have $\operatorname{Br}\overline{X} = \operatorname{Hom}(NS(\overline{X})_{\text{tors}}, \mathbb{Q}/\mathbb{Z})$ as Galois modules (this holds more generally if X is a surface and $h^{2,0} = 0$), and $NS(\overline{X})_{\text{tors}} = E^{\mu_3}$. Then (i) implies that $(\operatorname{Br}\overline{X})^{\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} = 0$.

The kernel of the restricted Cassels pairing $\text{Ш}(E)[\alpha_*] \times \text{Ш}(E)[\alpha_*] \to \mathbb{Q}/\mathbb{Z}$ consists of elements in the image of $\text{Ш}(E_1) \xrightarrow{\alpha_*^t} \text{Ш}(E)$, where $\alpha^t : E_1 \to E$ is the dual isogeny. Since $\text{Ш}(E)[\alpha_*] \cong \mathbb{Z}/3\mathbb{Z}$ must be zero because it is alternating, so lift $C_1 \to C$; then we have étale maps

$$C_1 \times F = Y_1 \to C \times F = Y \to X;$$

to find an adelic point, find a rational point $R \in F(\mathbb{Q})$ and a collection $\{P_v\} \in C_1(\mathbf{A}_{\mathbb{Q}})$; then $f_1 : Y_1 \to X$ has $f_1^*(\operatorname{Br}_1 X) \subset \pi^*(\operatorname{Br} F)$, where $\pi : Y_1 \to F$ is the projection.

The last condition (v) says that there are no rational points on X; rational points on X comes from twists of Y, but by assumption these have no point over a place v, so they arise from Ш.

A.16 Vojta: Big semistable vector bundles

Bigness

Throughout this talk, k is a field of characteristic zero, algebraically closed unless otherwise specified.

A **variety** is an integral scheme, separated and of finite type over a field.

Throughout this talk, X is a complete variety over k.

Definition: Let $\mathcal{L}$ be a line sheaf on X. We say that $\mathcal{L}$ is **big** if there is a constant $c > 0$ such that $h^0(X, \mathcal{L}^{\otimes n}) \geq cn^{\dim X}$ for all sufficiently large and divisible $n \in \mathbb{Z}$.

Lemma. (Kodaira) Let $\mathcal{L}$ be a line sheaf and $\mathcal{A}$ an ample line sheaf on X. Then $\mathcal{L}$ is big iff $\mathcal{L}^{\otimes n} \otimes \mathcal{A}^\vee$ has a (nonzero) global section for some $n > 0$.

Proof: " $\Longleftarrow$ " is obvious.

" $\Longrightarrow$ ": Write $\mathcal{A} \cong \mathcal{O}(A_1 - A_2)$ with A_1 a reduced effective very ample divisor. It will suffice to show that $\mathcal{L}^{\otimes n}(-A_1)$ has a global section for some $n > 0$. Consider the exact sequence

$$0 \to H^0(X, \mathcal{L}^{\otimes n}(-A_1)) \to H^0(X, \mathcal{L}^{\otimes n}) \to H^0(A_1, \mathcal{L}^{\otimes n}) .$$

The middle term has rank $\gg n^{\dim X}$, but the rightmost term has rank $\ll n^{\dim X - 1}$, for $n \gg 0$ divisible. $\square$

Definition: A vector sheaf $\mathcal{E}$ of rank r on X is **big** if there is a $c > 0$ such that

$$h^0(X, S^n\mathcal{E}) \geq cn^{\dim X + r - 1}$$

for all $n \gg 0$ divisible.

Equivalently, $\mathcal{E}$ is big iff $\mathcal{O}(1)$ on $\mathbb{P}(\mathcal{E})$ is big.

Essential base locus

Definition: Assume that X is projective, and let $\mathcal{L}$ be a (big) line sheaf on X. The **essential base locus** of $\mathcal{L}$ is the subset

$$\bigcap_{n \in \mathbb{Z}_{>0}} (\text{base locus of } \mathcal{L}^{\otimes n}(-A))$$

for any ample divisor A on X (it is independent of A). The essential base locus of a vector sheaf $\mathcal{E}$ on X is the set $\pi(E)$, where E is the essential base locus of $\mathcal{O}(1)$ on $\mathbb{P}(\mathcal{E})$ and $\pi\ \mathbb{P}(\mathcal{E}) \to X$ is the canonical morphism.

Question: If $\mathcal{E}$ is a big vector sheaf, is its essential base locus properly contained in X?
Answer: No. Example: Unstable $\mathcal{E}$ over curves.
Question: What if $\mathcal{E}$ is big and semistable?

Curves

Throughout this section, X is a (projective) curve.

Definition: (Mumford) A vector sheaf $\mathcal{E}$ on X is **semistable** if, for all short exact sequences

$$0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$$

of nontrivial vector sheaves on X,

$$\frac{\deg \mathcal{E}'}{\operatorname{rk} \mathcal{E}'} \le \frac{\deg \mathcal{E}}{\operatorname{rk} \mathcal{E}}$$

or (equivalently)

$$\frac{\deg \mathcal{E}''}{\operatorname{rk} \mathcal{E}''} \ge \frac{\deg \mathcal{E}}{\operatorname{rk} \mathcal{E}} \ .$$

Theorem. Let $\mathcal{E}$ be a big semistable vector sheaf on X. Then $\mathcal{E}$ is ample (i.e., $\mathcal{O}(1)$ is ample on $\mathbb{P}(\mathcal{E})$). In particular, the essential base locus of $\mathcal{E}$ is empty.

Proof: By Kleiman's criterion for ampleness, the sum of an ample and a nef divisor is again ample, so by Kodaira's lemma it suffices to show that if $\mathcal{E}$ is a semistable vector sheaf on X, then all effective divisors D on $\mathbb{P}(\mathcal{E})$ are nef.

So, let D be an effective divisor and C a curve on $\mathbb{P}(\mathcal{E})$. We want to show:

$$(DC) \ge 0 \ .$$

Since $\mathcal{E}$ is semistable, so is $\left(\pi\big|_C\right)^*\mathcal{E}$ (proof later).

Therefore we may assume that C is a section of π, and that D is a prime divisor.

Since C is a section, it corresponds to a surjection $\mathcal{E} \to \mathcal{L} \to 0$. Moreover, $\mathcal{L} \cong \mathcal{O}(1)\big|_C$. By semistability, therefore,

$$(\mathcal{O}(1)C) \ge \frac{\deg \mathcal{E}}{\operatorname{rk} \mathcal{E}} \ . \qquad (*)$$

Now consider D. Let d be the degree of D on fibers of π; $d > 0$. Then $\mathcal{O}(D) \cong \mathcal{O}(d) \otimes \pi^*\mathcal{M}$ for some $\mathcal{M} \in \operatorname{Pic} X$. Thus D corresponds to a section of $\mathcal{M} \otimes S^d\mathcal{E}$, hence we have an injection

$$0 \to \mathcal{O}_X \to \mathcal{M} \otimes S^d\mathcal{E}$$

with locally free quotient.

Since $\mathcal{E}$ is semistable, so is $S^d\mathcal{E}$ (proof later); hence

$$\deg(\mathcal{M} \otimes S^d\mathcal{E}) \ge 0 \qquad (**)$$

Let $r = \operatorname{rk} \mathcal{E}$; then $S^d\mathcal{E}$ has rank $r' := \binom{r+d-1}{d}$. The diagram

$$\begin{array}{ccc} GL_r(k) & \longrightarrow & GL_{r'}(k) \\ \downarrow & & \downarrow \\ k^* & \longrightarrow & k^* \end{array}$$

commutes for all diagonal matrices, hence for all diagonalizable matrices, hence for all matrices. Thus

$$\begin{aligned}\deg(\mathcal{M}\otimes S^d\mathcal{E}) \qquad &= r'\deg\mathcal{M} + \binom{r+d-1}{d-1}\deg\mathcal{E} \\ &= r'\deg\mathcal{M} + \frac{d}{r}r'\deg\mathcal{E}\end{aligned}$$

and therefore by (**),

$$\deg\mathcal{M} \geq -\frac{d}{r}\deg\mathcal{E}\ .$$

Thus by (*),

$$(DC) = d(\mathcal{O}(1)C) + \deg\mathcal{M} \geq \frac{d}{r}\deg\mathcal{E} - \frac{d}{r}\deg\mathcal{E} \geq 0\ . \quad \square$$

Higher Dimensional Varieties

Let X again be a complete variety of arbitrary dimension.

Construction: Given a vector sheaf $\mathcal{E}$ on X of rank r and a representation

$$\rho : GL_r(k) \to GL_{r'}(k)\ ,$$

we can construct a vector sheaf $\mathcal{E}^{(\rho)}$ on X of rank r' by applying ρ to the transition matrices of $\mathcal{E}$. Equivalently, if $\mathcal{E}$ corresponds to $\xi \in H^1(X, GL_r(\mathcal{O}_X))$, then $\rho(\xi) \in H^1(X, GL_{r'}(\mathcal{O}_X))$ corresponds to $\mathcal{E}^{(\rho)}$.

Examples of this include S^d, det, and $\wedge^d$.

Definition: (Bogomolov) A vector sheaf $\mathcal{E}$ of rank r on X is **unstable** if there exists a representation $\rho\, GL_r(k) \to GL_{r'}(k)$ of determinant 1 (i.e., factoring through $PGL_r(k)$) such that $\mathcal{E}^{(\rho)}$ has a nonzero section that vanishes at at least one point. It is **semistable** if it is not unstable.

Theorem. (Bogomolov) If X is a curve, then Bogomolov's definition of semistability agrees with Mumford's.

Remark: If ρ has determinant 1 then $Im\,\rho \subseteq SL_{r'}(k)$, but not conversely.

Indeed, the representation $GL_1(k) \to GL_2(k)$, $z \mapsto \begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix}$, has image contained in $SL_2(k)$ but its does not factor through $PGL_1(k)$.

To see that the (true) converse holds, first show that the vanishing of the determinant defines an irreducible subset of k^{r^2}; this is left as an exercise for the reader. Now suppose that $\rho\, GL_r(k) \to GL_{r'}(k)$ is a representation that factors through $PGL_r(k)$, and suppose also that its image is not contained in $SL_{r'}(k)$. Then $\det\circ\rho$ is a nonconstant regular function $PGL_r(k) \to k^*$, hence it determines a nonconstant rational function on $\mathbb{P}_k^{r^2}$ with zeros and poles contained in $\{\det = 0\}$. But the latter is irreducible, so it can't have both zeroes and poles there, contradiction.

So now we can pose:

Question: If X is a projective variety and $\mathcal{E}$ is a big, semistable vector sheaf on X, then is the essential base locus of $\mathcal{E}$ a proper subset of X?

Remark: We can't conclude that $\mathcal{E}$ is ample in the above, as the following example illustrates. Let X be a projective variety of dimension > 1, let $\mathcal{E}$ be a big semistable vector sheaf on X of rank > 1, let $\pi X' \to X$ be the blowing-up of X at a closed point, and let F be the exceptional divisor. Then the essential base locus of $\pi^*\mathcal{E}$ must contain F.

My Mitteljahrentraum

The question of an essential base locus being a proper subset comes up in Nevanlinna theory, and I hope to be able to use it in number theory, as well. Here's how.

Bogomolov has shown that Ω^1_X is semistable for a smooth surface X. One would hope to generalize this, to $\Omega^1_X(\log D)$ for a normal crossings divisor D on X, and also to higher dimensions. Then it would suffice to prove that one of these bundles is big to get arithmetical consequences.

Moreover, Bogomolov's definition of semistability can be generalized to defining semistability of higher jet bundles. These are not vector bundles, because they correspond to elements of $H^1(X, G(\mathcal{O}_X))$ for a group G other than GL_n. But, one can make the same definition, using those representations of G having the appropriate kernel: k^* again (Green-Griffiths), or a certain bigger group (Semple-Demailly). Probably the latter.

Bigness is easy to define in this context, and then one hopefully can use the two properties to talk about the exceptional base locus. Already the proof of Bloch's theorem in Nevanlinna theory can probably be recast in this mold.

Is Semistability Really Necessary?

The proof of the main theorem of this talk didn't really need the full definition of semistability; it only used the condition on the degrees of subbundles for subbundles of rank 1 and corank 1. Would the following definition make sense, and would it be preserved under pull-back and symmetric power?

Definition: Let X be a projective curve and let $\mathcal{E}$ be a vector sheaf of rank r on X. Then $\mathcal{E}$ is ± 1**-semistable** if the condition on degrees and ranks of subbundles holds for all full subbundles $\mathcal{E}'$ of rank 1 and corank 1.

Again, what would be a reasonable representation-theoretic formulation of this definition?

Loose Ends

In the proof of the main theorem it remains to show that semistability is preserved under pull-back and under taking S^d.

To show the first assertion, let $f X' \to X$ be generically finite, and let $\mathcal{E}$ be a semistable vector sheaf on X. Suppose that $f^*\mathcal{E}$ is unstable. Let $\rho GL_r(k) \to GL(V)$ be a representation such that $(f^*\mathcal{E})^{(\rho)}$ has a nonzero global section that vanishes somewhere. Let $d = \deg f$. Then taking norms gives a global section of

$$S^d(\mathcal{E}^{(\rho)}) = \mathcal{E}^{(S^d \circ \rho)}$$

with the same properties, contradiction.

The second assertion is proved similarly: suppose there is a representation

$$\rho\, GL(S^d(k^r)) \to GL(V)$$

with the required properties. Then $\rho \circ S^d$ gives a representation $GL_r \to GL(V)$, leading to a contradiction as before. It only remains to check that $\rho \circ S^d$ has determinant 1. This follows by commutativity of the following diagram:

$$\begin{tikzcd} GL_r(k) \arrow[r] \arrow[d] & GL_{r'}(k) \arrow[d] \\ PGL_r(k) \arrow[r] & PGL_{r'}(k) \end{tikzcd}$$

(here r' is the rank of $S^d\mathcal{E}$).

A.17 Wooley: The Circle Method

Introduction

The circle method is the Hardy-Littlewood method (1920s), "any method involving Harmonic analysis that counts solutions of Diophantine questions", including Kloosterman methods.

Example. Consider a homogeneous polynomial $F(x_1,\dots,x_s) \in \mathbb{Z}[x_1,\dots,x_s]$ of degree d. We count

$$\begin{aligned} N_F(B) &= \#\{(x_1,\dots,x_s) \in [-B,B]^s : F(x) = 0\} \\ &= \int_0^1 G(\alpha)\, d\alpha, \end{aligned}$$

where

$$G(\alpha) = \sum_{|x|\le B} e(\alpha F(x_1,\dots,x_s)),$$

and $e(z) = e^{2\pi i z}$.

Let $\psi(B) \to \infty$ as $B \to \infty$ as slowly as you like, $\psi(B) < B^{d/2}$. We look at

$$\mathfrak{M}(q,a) = \{\alpha \in [0,1] : |q\alpha - a| \le \psi(B)B^{-d}\},$$

and let

$$\mathfrak{M} = \bigcup_{\substack{0\le a\le q\le\psi(B)\\ \gcd(a,q)=1}} \mathfrak{M}(q,a),$$

the *major arcs*. Then

$$\int_{\mathfrak{M}} G(\alpha) d\alpha \sim v_\infty \prod_p v_p B^{s-d},$$

the product of local densities, where v_∞ is the volume of the real manifold defined by $F(x) = 0$ in $[-1,1]^s$, and

$$v_p = \lim_{h\to\infty} p^{h(1-s)} \#\{F(x) = 0 \pmod{p^n} : x \in (\mathbb{Z}/p^h\mathbb{Z})^s\}.$$

This particular statement is true in a very broad sence, provided that s is not small and that the geometry of $F = 0$ is not too wild, e.g. nonsingular.

For $\mathfrak{m} = [0,1) \setminus \mathfrak{M}$, the *minor arcs*, then $G(\alpha)$ should be "randomly" behaved, so one tries to show: $G(\alpha) = o(B^{s-d})$ when $\alpha \in \mathfrak{m}$. If true, then

$$N_F(B) = \int_{\mathfrak{M}} G(\alpha)\, d\alpha + \int_{\mathfrak{m}} G(\alpha)\, d\alpha \sim v_\infty \prod_p v_p B^{s-d} + o(B^{s-d}).$$

For this one needs non-singular $\mathbb{R}$ and $\mathbb{Q}_p$-points. When this method works, one gets weak approximation and the Hasse principle.

In particular, this will not work for varieties which fail the Hasse principle. The basic techniques work for all number fields $K/\mathbb{Q}$, or even for $\mathbb{F}_q[t]$ or other function fields.

Scope of the Circle Method

The circle method works with "sufficiently many" variables.

Proposition (Birch 1957)**.** *Given forms $F_1, \ldots, F_r \in \mathbb{Q}[x_1, \ldots, x_s]$, of respectively odd degrees $d_1, \ldots, d_r$, and provided that $s > s_0(d_1, \ldots, d_r)$ is large enough, then there exists a rational point on $F_1 = \cdots = F_r = 0$.*

This method diagonalizes each of the forms, but at a great cost:

$$s_0(d_1, \ldots, d_r) \leq \psi_{(d-5)/2}(d_1 + \cdots + d_r)$$

where $d = \max d_i$, and $\psi_0(x) = \exp(x)$, $\psi_1(x) = (\underbrace{\exp \circ \cdots \circ \exp}_{42 \log x})(x)$, $\psi_2(x) = (\underbrace{\psi_1 \circ \cdots \circ \psi_1}_{42 \log x})(x)$ and so on.

Example. For $d = 3$, one has $s_0(3) = 15$ (Davenport 1963); $s_0(\underbrace{3, \ldots, 3}_{r}) = (10r)^5$ (Schmidt 1984). $s_0(3, 3) = 831$ (Dietmann-W).

Proposition (Birch 1962)**.** *Let $F(x) \in \mathbb{Z}[x_1, \ldots, x_s]$ be homogeneous of degree d. Let $V = \{F(x) = 0\}$. Then whenever $s - \dim(V_{\text{sing}}) > (d-1)2^d$, one has $N_F(B)$ asymptotic to a product of local densities as before.*

The difficulty of this result depends on the singular locus being reasonably small in dimension. This holds for any number field, and it is probable that this holds for a function field assuming the characteristic is sufficiently large.

Proposition (Heath-Brown 1983, Hooley 1988)**.** *For $s_0(3) = 8$, we have the Hasse principle for nonsingular cubic forms.*

We now turn to some simpler situations.

Proposition (Brudem-W)**.** *If $F = \Phi_1(x_1, x_2) + \cdots + \Phi_{s/2}(x_{s-1}, x_s)$, $\Phi_i \in \mathbb{Z}[x, y]$ binary, homogeneous of degree d, then $N_F(B)$ is asymptotic to the product of local densities whenever*

$$s > \begin{cases} 2^d, & d = 3, 4 \\ (17/16)2^d, & 5 \leq d \leq 10 \\ 2d^2 \log d + \ldots, & d \text{ large.} \end{cases}$$

For a diagonal form $a_1 x_1^d + \cdots + a_s x_s^d = 0$, work by Hua, Vaughan, Heath-Brown, the same conclusion holds for

$$s > \begin{cases} 2^d, & d = 3 \leq d \leq 5 \\ (7/8)2^d & 6 \leq d \leq 8 \\ d^2 \log d + \ldots, & d \text{ large;} \end{cases}$$

One also has the weaker statement that $N_F(B)$ is greater than a constant times the product of local densities in the cases that

$$s \geq \begin{cases} 7, & d = 3 \\ 12, & d = 4 \\ \vdots & \\ d(\log d + \log\log d + 2 + o(1)), & d \text{ large.} \end{cases}$$

Presumably: $s > 2d$ should suffice for the method to work.

Simultaneous equations: we expect need $s_0(d)$ variables for 1 form of degree d makes it look we need $rs_0(d)$ variables for r forms of degree d. For $\sum_{j=1}^{s} a_{ij} x_j^d = 0$, $(1 \leq i \leq r)$, the number of variables required is given by: if the forms are in general position, and $s > (3r+1)2^{d-2}$, then we have an asymptotic formula. For r diagonal cubics, $s \geq 6r + 3$. For 2 diagonal cubics, one has the Hasse principle whenever $s \geq 13$ (Brudeur, W).

Keys to Success

We have the major arcs

$$\mathfrak{M}(q,a) = \{\alpha \in [0,1) : |q\alpha - a| \leq \psi(B) B^{-d}\}$$

with

$$\mathfrak{M} = \bigcup_{\substack{0 \leq a \leq q \leq \psi(B) \\ \gcd(a,q)=1}} \mathfrak{M}(q,a).$$

For $\alpha = a/q$ a rational number, we have

$$\begin{aligned} G(\alpha) = \sum_{|x| \leq B} e(\alpha F(x)) &= \sum_{r_1=1}^{q} \cdots \sum_{r_s=1}^{q} \sum_{\substack{x_i \equiv r_i \pmod{q} \\ 1 \leq i \leq s}} e((a/q) F(r_1, \ldots, r_s)) \\ &= (B/q)^s \sum_{r_1=1}^{q} \cdots \sum_{r_s=1}^{q} e((a/q) F(r)) + O((B/q)^{s-1} q^s) \\ &\sim q^{-s} S(q,a) B^s. \end{aligned}$$

One can handle the case $\alpha = (a/q) + \beta$ for β small by using the mean value theorem,

$$G(\alpha) = q^{-s} S(q,a) v(\beta) + O((q(1 + B^d|\beta|))^s)$$

and

$$v(\beta) = \int_{-B}^{B} \cdots \int_{-B}^{B} e(\beta F(\gamma_1, \ldots, \gamma_s))\, d\gamma.$$

One can apply Poisson summation and Kloosterman methods to get the error to be of type $B^{ds/4}$.

For the minor arcs, we want to show $\int_{\mathfrak{m}} G(\alpha)\, d\alpha = o(B^{s-d})$. One has Weyl differencing: letting $f(\alpha) = \sum_{|x| \leq B} e(\alpha x^d)$, we have

$$|f(\alpha)|^2 = \sum_{|x| \leq B} \sum_{|y| \leq B} e(\alpha(x^d - y^d)) = \sum_{h \in I} \sum_{y \in I(h)} e(\alpha((y+h)^d - y^d))$$

where now $(y+h)^d - y^d = hp_{d-1}(y,h)$. Repeating in this way, one can get down to sums of linear polynomials. Provided $\alpha \in \mathbb{R}$, $a \in \mathbb{Z}$, $q \in \mathbb{N}$, $\gcd(a,q) = 1$, with $|\alpha - a/q| \le q^{-2}$, then

$$|f(\alpha)| \ll B^{1+\epsilon}(a^{-1}B^{-1} + qB^{-d})^{2^{1-d}}.$$

Finally, there is recent work of Heath-Brown and Skorobogatov: For $at^\ell(1-t)^m = N(x)$, N a norm form of degree k, then the Brauer-Manin obstruction is the only one to weak approximation and the Hasse principle. One uses descent to $cN(y) + dN(z) = \lambda w^k$, where the circle method gives weak approximation and the Hasse principle. One can generalize this to the case

$$aL_1(x)^{\ell_1} L_{2r}(x)^{\ell_{2r}} = N(v),$$

where $L_i(x) \in \mathbb{Q}[x_1, \ldots, x_r]$ linear forms, $\gcd(\ell_1, \ldots, \ell_{2r}) = 1$. Again we have that the Brauer-Manin obstruction is the only one, and one has descent to

$$\sum_{j=1}^{2r} c_{ij} N(y_i) = \lambda_i w^k$$

for $(1 \le i \le r)$.

A.18 Yafaev: Descent on certain Shimura curves

Joint work with A. Skorobogatov.

Let B be an indefinite division quaternion algebra over $\mathbb{Q}$ (indefinite means that $\mathbb{R} \otimes B = M_2(\mathbb{R})$). Let $\mathcal{O}_B$ be a maximal order in B. Let D be the discriminant of B (the product of primes that do not split B), and suppose $D > 1$. Let $\mathbb{H}^\pm$ be the union of the upper and lower half planes and consider the Shimura curve

$$S = \mathcal{O}_B^\times \backslash \mathbb{H}^\pm.$$

Then S is a compact Riemann surface S with a canonical model over $\mathbb{Q}$.

Let N be a prime, $(N, D) = 1$. Let $\Gamma_0(N)$, $\Gamma_1(N)$ be the inverse images in $\mathcal{O}_B^\times$ of the usual subgroups of $GL_2(\mathbb{Z}/N)$. Let $X = \Gamma_1(N)\backslash\mathbb{H}^\pm$, $Y = \Gamma_0(N)\backslash\mathbb{H}^\pm$. Then $X \to Y$ is a Galois covering, with Galois group $\mathbb{Z}/N\mathbb{Z}^\times$, which is unramified if $\exists p, q | D$ such that $p \equiv 1 \pmod 4$, $q \equiv 1 \pmod 3$.

Theorem (Shimura)**.** *We have $S(\mathbb{R}) = \emptyset$, and if k is imaginary quadratic, $k \otimes B = M_2(k)$, and $|Cl(k)| = 1$, then $S(k) \neq \emptyset$.*

- Jordan and Livne gave a complete description of points of S over local fields.
- Jordan gave some results on points of S over imaginary quadratic fields. For example, if $D = 39$, $k = \mathbb{Q}(\sqrt{-3})$, then S_k does not satisfy the Hasse Principle.
- Skorobogatov and Siksek showed that if S_k does not have a k-rational divisor class of degree 1 and $(\mathrm{Jac}(S_k))$ is finite, then the failure of the Hasse Principle for S_k is accounted for by the Manin obstruction.

Consider now the covering $X \to Y$ of curves over $\mathbb{Q}$, as defined above. We want to find an imaginary quadratic field k and X and Y such that for any twist of X by a character $\mathrm{Gal}(\overline{k}/k) \xrightarrow{\sigma} (\mathbb{Z}/N)^\times/\pm 1$, $X^\sigma(\mathbb{A}_k) = \emptyset$ but $Y(\mathbb{A}_k) \neq \emptyset$. Since, as in Skorobogatov's talk, $Y(k) = \bigcup_\sigma X^\sigma(k)$, this shows that the Hasse principle for Y fails and provides a cohomological obstruction that explains this failure.

Suppose first that $v|p$ for a prime p dividing D. Then Y has bad reduction at v. Furthermore, it is known (Jordan-Livne-Varshavsky) that $Y(k_v) \neq \emptyset$ if p is inert. So we suppose that all primes dividing D are inert in k.

Now consider what happens at N. We have the usual model of $Y_{\mathbb{F}_N}$ with two components $S_{\mathbb{F}_N}$, intersecting at supersingular points defined over $\mathbb{F}_{N^2}$. We assume again that N is inert. It can be shown that $|S(\mathbb{F}_{N^2}) \setminus \{\text{Supersingular Points}\}| > 0$. This then shows that if N is inert, $Y(k_v) \neq \emptyset$ for $v|N$.

Finally, we consider places v which do not divide ND. If $\sigma : \mathrm{Gal}(\overline{k}/k) \to (\mathbb{Z}/N)^\times/\pm 1$ is ramified at such a place v, $X^\sigma(k_v) = \emptyset$. So we need only consider characters unramified outside ND. If we suppose further

A. that $(N-1)/2$ is prime to $p(p^2-1)$ for any $p|D$
B. $|Cl(k)|$ is prime to $(N-1)/2$

then we are left with characters corresponding to $\mathbb{Q}(\zeta_N)^+k/k$.

Now, Y and X^σ have good reduction outside ND. To deal with places $v \nmid ND$, we count points to show that the curve has points over $\mathbb{F}_v$ (which is $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ according as p is split or inert in k), then lift them using Hensels Lemma.

The point counts make use of the following trace formulas: $p \nmid ND$ then

$$\begin{aligned} \mathrm{Tr}(F_p^r | H^1_{\text{ét}}(Y_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)) &= \mathrm{Tr}(pT_{p^{r-2}} - T_{p^r} | H^0(Y_{\overline{\mathbb{F}}_p}, \Omega^1)) \\ \mathrm{Tr}(F_p^r | H^1_{\text{ét}}(X^\sigma_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)) &= \mathrm{Tr}(\gamma^r pT_{p^{r-2}} - \gamma^r T_{p^r} | H^0(X_{\overline{F}_p}, \Omega^1)) \end{aligned}$$

where F_p is Frobenius and $\gamma = \sigma(F_p)$. We get $Y(\mathbb{F}_{p^2})| > 0$, and $Y(\mathbb{F}_p)| > 0$ if $\exists t \in \mathbb{Z}$, $|t| < 2\sqrt{p}$ such that

A. all primes dividing D are split in $\mathbb{Q}(\sqrt{t^2-4p})$
B. $p \nmid t$ or p is not split in $\mathbb{Q}(\sqrt{t^2-4p})$
C. N is not inert in $\mathbb{Q}(\sqrt{t^2-4p})$.

Putting these together we get the following proposition:

Proposition (Local points on X^σ). *Suppose that for all $m \in \{0, 1, \ldots, (N-3)/2\}$ there exists $p \nmid ND$ split or ramified in k such that*

$$p^{2m} + tp^m + p \neq 0 \pmod{N} \qquad \textit{(for all } t \in \mathbb{Z},\ |t| < 2\sqrt{p}\textit{)} \tag{2}$$

then for all characters σ we have $X^\sigma(\mathbb{A}_k) = \emptyset$.

We can now find counterexamples to the Hasse principle as follows:

A. Choose $D = q_1 q_2$, with $q_1 \equiv 1 \pmod 4$ and $q_2 \equiv 1 \pmod 3$.
B. Choose N such that $(N-1)/2$ is coprime to $q_1(q_2^2-1)\ q_2(q_2^2-1)$.
C. Let p be a prime such that $p \nmid ND$. Call p good if there exists t such that condition 1 above is satisfied, bad otherwise. (The set of bad primes is finite.) Now find a good p such that (2) is satisfied.
D. Now choose a field k imaginary quadratic such that q_1, q_2, N are inert in k, bad primes are inert, primes from Step 3 are split or ramified, and $|Cl(k)|$ is prime to $(N-1)/2$. Ono can prove that if there is one $k$satisfying these conditions there are infinitely many.

Example: $D = 35$, $N = 23$, $k = \mathbb{Q}(\sqrt{-127})$.

CHAPTER B: PROBLEMS

The workshop featured two problem/discussion sessions. The sessions were moderated by Jean-Louis Colliot-Thélène and William McCallum. People took turns suggesting problems and the moderator led the other participants to share their thoughts and perspectives.

The material from both sessions has been combined into one list.

A followup session, discussing the progress made during the workshop, was moderated by Trevor Wooley. The material from the followup session has been incorporated in the problem list.

B.1 List of open problems

Problem/Question 1. Consider hypersurfaces $f_d \in \mathbb{Z}[x_0, \dots, x_n]$ of degree d in $\mathbb{P}^n$, $n \geq 2$. Let

$$N(H) = \{f_d : \text{max coefficient of } f_d \text{ is} \leq H,\ f_d \text{ has a solution in } \mathbb{Z}^{n+1} \setminus \{0\}\}.$$

(a) For $d > n+1$, is it true that $N(H)/N_{\text{tot}}(H) \to 0$? Does this follow from Lang's conjectures? (Voloch)

(b) Instead, look at those with those with points locally everywhere N_{loc} (Poonen). Is this a positive fraction, i.e. is $N_{\text{loc}}(H)/N_{\text{tot}}(H) > c$?

(c) As a special case, if you write down a plane cubic, how likely is it to have a rational point? (Voloch)

(d) For cubic surfaces, there are examples where the Hasse principle fails, but maybe for almost all values of a parameter in a family, the Hasse principle holds. We should have asympotically that the $N(H)/N_{\text{tot}}(H) \sim N_{\text{loc}}(H)/N_{\text{tot}}(H)$? (Colliot-Thélène) For $d \leq n$, we hope this will hold in general.

Remarks.

(i) The set of reducible such hypersurfaces are a very small fraction (usually codimension ≥ 2)—they affect this calculation very little (Poonen).

(ii) Serre looked at $d = 2$; here one has the Hasse principle. (Tschinkel) For $d = 2, n = 2$, the proportion of everywhere locally solvable ones tends to zero; but we should exclude this case because of the codimension 2 condition. (Heath-Brown) Instead, we should restrict to families $X \to S$ such that the codimension of reducible fibers is at ≥ 2.

(iii) Computational evidence is all over the place, so one must rephrase the question better to get some kind of answer. For example, for cubics, those with prime power discriminant and the general evidence are quite different. (Swinnerton-Dyer)

(iv) How is this related to 3-torsion elements in Ш? (Ellenberg)

Update (4/21/04): Poonen and Volloch have tackled this problem: http://www.math.princeton.edu/~ html/poonen-voloch/random.pdf

Problem/Question 2. If X is smooth projective geometrically rationally connected defined over a number field k, then the Brauer-Manin obstruction should be the only one to the Hasse principle. That is, is

$$\overline{X(k)} = X(\mathbf{A}_k)^{\operatorname{Br} X}?$$

As special cases, this should be the case for Fano varieties of dimension ≥ 3, e.g. (smooth) complete intersections of degree $(d_1, \dots, d_r)$ in $\mathbb{P}^n$ with $d_1 + \cdots + d_r \leq n$. (Colliot-Thélène)

Remarks.

(i) It would be worth doing a reasonably large search on diagonal quartic 3-folds. (Swinnerton-Dyer)

(ii) It is an old problem that for nonsingular cubic forms in at least 5 variables, the Hasse principle holds. For diagonal cubic forms over $\mathbb{Q}$, this is proved modulo finiteness of Ш. (Swinnerton-Dyer)

(iii) For the smooth intersection of two quadrics in $\mathbb{P}^5$, the Hasse principle should hold? If it has a rational point, then it in fact satisfies weak approximation. The critical problem is in 6 variables. (Colliot-Thélène)

Problem/Question 3. Let $f_1(x_0, \dots, x_n) = 0$, $f_2(x_0, \dots, x_n) = 0$ define the smooth complete intersection of two quadrics $X^{2,2} \subset \mathbb{P}^n$ over k a number field. For simplicity, assume $k = \mathbb{Q}$. If $n \geq 8$, $X(\mathbb{R}) \neq \emptyset$ implies $X(\mathbb{Q}) \neq \emptyset$. (Sansuc, Swinnerton-Dyer, Colliot-Thélène)

(a) For $n \geq 9$ (10 variables), this can be provably done by the circle method. (Heath-Brown)

(b) For $n = 7$, there is the concrete problem: given two quadratic forms f_1, f_2 as above in 8 variables over k a p-adic field, assume $f_1 = f_2 = 0$ is smooth, so that $\det(\lambda f_1 + \mu f_2) = p(\lambda, \mu)$ is separable. Does there exist $(\lambda, \mu) \in \mathbb{P}^1(k)$ such that $\lambda f_1 + \mu f_2$ contains 3 hyperbolics (split off an extra xy in its decomposition). Solution to this problem would give a local-global principle for $n = 7$. (Colliot-Thélène)

Remarks.

(i) It is possible in odd characteristic after an odd degree field extension (Heath-Brown), unwritten.

(ii) If in the pencil, there is one of rank ≤ 7, then it is possible; or other conditions with $n \geq 5$ (e.g. two conjugate lines or contains a conic defined over the ground field).

Problem/Question 4. Consider the hypersurface given by $\sum_i x_i y_i^2 = 0$ in $\mathbb{P}^3 \times \mathbb{P}^3$. Take the height

$$H(x, y) = \sup |x_i|^3 \cdot \sup |y_i|^2$$

and throw out the set where some $x_i = 0$, $y_i = 0$. Can one estimate the counting function? (Peyre)

Remarks. Some people are working on this. What news?

Problem/Question 5. Consider $xyz = t(x + y + z)^2$, with height function $H(x, y, z, t) = \max(|x|, |y|, |z|, |t|)$, and restrict to $\gcd(x, y, z, t) = 1$. Excluding trivial solutions (on lines), can you prove a counting function which is

$$\sim cB(\log B)^6 < B^{1+\epsilon}?$$

This is a singular cubic surface so we also expect an explicit constant. (Tschinkel)

Remarks.

(i) This has a D_4-singular point. On top of the singularity, one gets a configuration of 4 lines all of which have self-intersection 2.

(ii) Are numerics possible? (Voloch)

(iii) This is a compactification of the affine plane (solve for t), but it is not equivariantly embedded. (Tschinkel)

(iv) For the singular cubic surface $1/x + 1/y + 1/z + 1/t = 0$, Heath-Brown has established that the counting function has exact order of magnitude $B(\log B)^6$. Proceedings of the session in analytic number theory and Diophantine equations, Bonner Math. Schriften 360 (2003).

(v) Progress: Using the universal torsor (as calculated by Hassett and Tschinkel) Browning has established that the counting function has exact order of magnitude $B(\log B)^6$. See math.AG/0403530, http://front.math.ucdavis.edu/math.NT/0404245[1].

(vi) Update (4/21/04) Tim Browning has shown $B(logB)^6 \ll N(B) \ll B(logB)^6$. He makes use of the universal torsor. See [arXiv:math.NT/0404245]

(vii) Takloo-Bighash: for $w^2x+wy^2+z^3 = 0$, have an effective lower bound of $B \log B$, and should be able to get $B \log^2 B$ by a similar method, but can't push it any further. Expected upper bound in this case is again $B(\log B)^6$. Hassett: the universal torsor was in his lecture.

(viii) Hassett: there are 13(ish) singular cubics (zero-dimensional in moduli), the list is in a paper, reference available.

Problem/Question 6. (Swinnerton-Dyer)

(a) Is there a $K3$ surface X over $\mathbb{Q}$ which has a finite nonzero number of rational points $\#X(\mathbb{Q}) < \infty$?

(b) Is there a nonsingular quartic surface X with this property?

(c) Find a third rational point on $X_1^4 + 2X_2^4 = X_3^4 + 4X_4^4$. (There are only 2 points with height $\leq 2^{15}$, and other non-public reasons to believe that there are only finitely many points.)

(d) Find a smooth quartic $X^4 \subset \mathbb{P}^3$ with $\operatorname{Pic} X \cong \mathbb{Z}$ and $X(K)$ infinite.

Remarks.

(i) Over $\mathbb{Q}$ would be the first place to try, but over any number field is OK. It seems as though this is possible for either all such families or no such family.

(ii) There are $K3$ surfaces with no rational lines with infinitely many rational points. (Peyre)

(iii) Do you hope that the Brauer-Manin obstruction is the only one to weak approximation? (Harari)

(iv) The rank of the Neron-Severi group over $\mathbb{C}$ is rank 20, but is only rank 1 over $\mathbb{Q}$ coming from the hyperplane section. Therefore it looks like a Kummer surface, the product of two CM elliptic curves. What are the elliptic curves? (Read the right paper of Shioda.) The CM is by $\mathbb{Q}(\sqrt{-2})$?

(v) It does not seem helpful to look over a finite extension. (Colliot-Thélène)

(vi) Are there any heuristics looking modulo any primes? (Poonen) The zeta function does not say anything about solubility. (Swinnerton-Dyer)

(vii) On $x^4 + y^4 + z^4 = t^4$, Elkies found another point, with smallest height on the order of 2^{15} (Colliot-Thélène); he uses a fibered pencil of elliptic curves, looks at values of the parameter for which there was a point everywhere locally and then looked for a global point. There is no such fibration in this case. Maybe one could go to an extension and then look for rational points (Villegas).

(viii) What restrictions are necessary for such a surface to occur? (Poonen) The condition to ensure that $\operatorname{Pic} X \cong \mathbb{Z}$ is a black-board full. (Swinnerton-Dyer)

[1]http://front.math.ucdavis.edu/math.NT/0404245

(ix) Is it possible for the given surface that $(\operatorname{Br}\overline{X})^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ is finite? If so, there might be many rational points. (Harari) In the computations of Brauer-Manin obstructions, there are many with $\ker(\operatorname{Br} X \to \operatorname{Br} \overline{X}) = \operatorname{Br} X$, there are a lack of examples with 'transcendental elements'. We expect $(\operatorname{Br}\overline{X})^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ to be finite, proven in certain cases because of the Tate conjecture.

(x) Are there any known examples of quartic surfaces with $\operatorname{Pic} X \cong \mathbb{Z}$ with infinitely many rational points? (Poonen) Maybe almost always they have infinitely many. (Swinnerton-Dyer)

(xi) If there are infinitely many points on a quartic, will they be Zariski dense? Look in Mordell's book, perhaps. (Colliot-Thélène)

(xii) Silverman has examples of surfaces in $\mathbb{P}^2 \times \mathbb{P}^2$ with two noncommuting endomorphisms, so this gives infinitely many points, but this has Picard group rank 2. (Voloch)

Problem/Question 7. The distribution of rational points on Enriques surfaces has not been well studied. (Skorobogatov)

Let X be an Enriques surface.

(a) If $X(k) \neq \emptyset$, is $X(k)$ Zariski dense?

(b) Is there an X which violates the Hasse principle?

(c) Is there an X such that $X(\mathbf{A}_k)^{\mathrm{Br}} = \emptyset$ but $X(\mathbf{A}_k) \neq \emptyset$?

(d) Is there an X with $X(k) = \emptyset$, $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$?

Remark. There is a $\mathbb{Z}/2\mathbb{Z}$ cover of the Enriques surface X which is a $K3$ surface; is there some torsor over the $K3$ surface for the torus for which the total space is a torsor for X under a nonabelian group? For a bi-elliptic surface, is this possible? (Harari)

Problem/Question 8. Let X an Enriques surface over a number field K, $Y \xrightarrow{p} X$ the double cover (K3 surface), $X(\mathbb{A}_K)^{\mathrm{Br}}$ the Brauer-Manin set. Take $m_v \in X(\mathbb{A}_K)^{\mathrm{Br}}$, lift it to an adelic point P_v on Y. Under what assumptions on m_v will it be liftable to P_v on $Y(\mathbb{A}_K)^{\mathrm{Br}}$, or at least $Y(\mathbb{A}_K)^{\mathrm{Br}_1}$?

Remark. Guess (reported by Harari): there should be some nonabelian torsor $Z \xrightarrow{\phi} X$ for the group G which is the semidirect product $T \rtimes \mathbb{Z}/2$, where T is Neron-Severi torus of Y. The points $p(Y(\mathbb{A}_K)^{\mathrm{Br}})$ should correspond to $X(\mathbb{A}_K)^f$, where $f : Z \to X$.

Remark. About Pb/question 8 (which is closely related to Pb 7), David Harari adds the following update (2004-09-25): "Skorobogatov and myself have recently proved that there exist Enriques surfaces X with adelic points in $X(\mathbb{A}_k)^{\mathrm{Br}}$ but not in the closure of the set of rational points $X(k)$ ("The Manin obstruction to weak approximation is not the only one"). In particular, some adelic points of $X(\mathbb{A}_k)^{\mathrm{Br}}$ are not liftable to $Y(\mathbb{A}_k)^{\mathrm{Br}_1}$, see the paper "Non-abelian descent and the arithmetic of Enriques surfaces" at http://www.dma.ens.fr/˜harari/[2]."

Problem/Question 9. Use the intermediate Jacobian (when it is an abelian variety) in arithmetic? To fix ideas, $\dim X = 3$, look at algebraic 1-cycles modulo rational equivalence.

Compute this for a rigid Calabi-Yau 3-fold X (over $\mathbb{C}$), i.e. $K_X \sim 0$, X simply connected, $h^{1,0} = 0$, $h^{2,0} = 0$, $h^{2,1} = 0$, $h^{3,0} = 1$. In this case, the intermediate Jacobian $J^2(X) \cong E$ is of dimension 1. Determine E given X, i.e. give its j-invariant.

Remarks.

[2] http://www.dma.ens.fr/∼harari/

(i) For two quadratic forms f_1, f_2 in 6 variables, i.e. $X^{2,2} \subset \mathbb{P}^5$, look at the Jacobian of the genus 2 curve given by $y^2 = \det(\lambda f_1 + \mu f_2)$. (Colliot-Thélène) Over $\mathbb{F}_p$, you can prove the Weil conjecture for $X^{2,2}$. Can you use this to prove something? You can also look at the variety of lines on $X^{2,2}$, also a principal homogeneous space for an abelian variety; so over a finite field, this will have a rational point, so there will be a line over $\mathbb{F}_p$. We can say something with $X^{2,2}$ contains a pair of skew conjugate lines or a conic defined over the ground field; how can you do these things such as finding a line over a quadratic field...?

(ii) Explicit examples of rigid Calabi-Yau 3-folds? Take an elliptic curve E with complex multiplication by $\mathbb{Q}(\zeta_3)$, take the kernel of the endomorphism $\zeta_3 - 1$, T_1; $T_1 \times T_2 \times T_3$ has 27 singular points, blowing up these points gives $h^{2,1} = 0$ (Candela). Also the quintic hypersurface $\sum_{i=1}^5 x_i^5 - 5\psi \prod_{i=1}^5 x_i = 0$ with $\psi^5 = 1$ has 125 nodes; the resolution has $h^{2,1} = 0$. There are more such examples. (Yui)

Problem/Question 10. Are there results at the level of number fields arising from the techniques of rationally connected varieties? (Colliot-Thélène)

For example, recently Kollàr got nice results over local fields: if X/k is a projective variety, we say $P, Q \in X(k)$ are *R-equivalent* if you can link them by a chain of curves of genus zero over k; if X is smooth with $k \hookrightarrow \mathbb{C}$, then X is *rationally connected* if $X(\mathbb{C})/R$ is a single point. Kollar proved that if k is a local field, and X/k is rationally connected, then $X(k)/R$ is finite. (Szobó)

Kollàr and Szabo proved that if k is a number field, and X/k is rationally connected, then $X(k_v)/R$ is trivial for almost all v.

Remark. If X/k is a variety over a number field, and X is rationally connected, then does there exist a field $K \supset k$ such that for all $L \supset K$ that $X(L)/R$ consists of a point? (Ellenberg) Negative answer by a conic bundle over $\mathbb{P}^2$. (Raskind)

Problem/Question 11. Let X/k be a smooth projective rationally connected variety with the cohomological dimension of $k \leq 1$. Does X have a rational point? (Colliot-Thélène)

Remarks.

(i) There was a false proof for $X^{2,2} \subset \mathbb{P}^4$.

(ii) Yes if $k = \mathbb{F}_q$. (Esnault) Yes if k is the function field of a curve. (Harris, Graber, Starr)

(iii) At least for surfaces, we hoped that universal torsors would be nice objects, e.g. they are birational to homogeneous spaces under a nice group, so they would be close to k-rational if they had a k-point. An example of X/k (k a horrible field) a cubic surface with $X(k) = \emptyset$ but $(\operatorname{Br} k)[3] = 0$. (Madore, Colliot-Thélène)

(iv) Colliot-Thélène adds the following: With hindsight, Problem 11, as phrased, had been settled by J. Ax in Bull. Am. Math. Soc. 71 (1965) p. 717. Ax produced a smooth hypersurface in 9-dimensional projective space, of degree 5, over a field k of cohomological dimension 1, with no rational point (that such hypersurfaces are rationally connected was proven much later). Ax'example has index 1, i.e. the g.c.d. of the degree of the finite field extensions over which the hypersurface acquires a rational point is 1. In Journal of the Inst. of Math. Jussieu (2004) 3 p. 1-16, J.-L. Colliot-Thélène and D. Madore produce a field of cohomological dimension 1 and a smooth cubic surface over that field which has index 3, thus settling negatively a question of Kato and Kuzumaki (1986).

Problem/Question 12. Describe all pairs of sets $A, B \subset \mu_\infty$, $\#A = \#B$, stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, where the elements of A and B are alternately placed around the unit circle. (Rodriguez-Villegas)

Remarks.

(i) There is a solution but it is much more complicated than the statement of the problem. The solution is used in the classification of algebraic hypergeometric functions.

(ii) There is the infinite family $A = \mu_{m+n} \setminus \{1\}$ and $\mu_m \cup \mu_n$ with $\gcd(m, n) = 1$.

Problem/Question 13. Find a smooth quintic hypersurface in $\mathbb{P}^3$ with Picard number 1 over $\mathbb{F}_2$. (Voloch)

Remarks.

(i) This is used in constructing error correcting codes.

(ii) If you compute the analytic rank (the zeta function), by Tate's theorem, the second Betti number is 53 so compute the number of points up to something like $\mathbb{F}_{2^{28}}$ (Voloch). So testing them exhaustively would be very costly.

(iii) Shioda has examples over $\overline{\mathbb{Q}}$ of Picard number 1, so they might be defined over $\mathbb{F}_2$. (Raskind) This has been tried once. (Voloch)

Problem/Question 14. Consider cubic hypersurfaces $a_0X_0^3 + a_1X_1^3 + a_2X_2^3 + a_3X_3^3 = 0$. (Swinnerton-Dyer)

(a) If soluble, give upper bound for smallest solution in terms of the a_i.

(b) Look at $|a_i| < A$, tabulate the size of the smallest solution and conjecture a particular growth rate in terms of A.

Remarks. If $a_1x_1^3 + \cdots + a_4x_4^3 = 0$ has a solution $\underline{x} \in \mathbb{Z}^4 \setminus \{0\}$, how large is the smallest solution? Let $\underline{x}_0$ be a solution with $\max\{|x_i|\}$ minimal. Swinnerton-Dyer had suggested: if $A = \max_{1\le i\le 4}\{|a_i|\}$, then $\max_{\underline{x}=\underline{x}_0}\{|x_i|\} << A^{4/3}$. Wooley had suggested instead $A^{1+\epsilon}$.

Progress: Stoll, Stein: computations up to $|a_i| \le 60$ suggest an upper bound of A^2. Also, assuming Schinzel, finiteness of Sha, and one unproven lemma, Stoll can produce $\underline{a} \in \mathbb{Z}^4$ with least solution $>> A^{2-\epsilon}$. (Need the hypotheses to ensure that the examples do have rational solutions.)

Shape of examples: if p, q prime, look at $px_1^3 + 2px_2^3 + qx_3^3 + 5qx_4^3$. Assume $2p$ and $5q$ are approximately of the same size, $p \equiv q \equiv 1 \pmod 3$, that 2 is a cube mod p but not mod q, and that 5 is a cube mod q but not mod p (plus some additional technical conditions).

Remarks.

(i) The growth rate should be like $A^{4/3}$. If you do the corresponding thing with 3 squares, $a_0X_0^2 + a_1X_1^2 + a_2X^2 = 0$, the answer is A. (Swinnerton-Dyer)

(ii) Seems more like $A^{1+\epsilon}$. (Wooley)

(iii) Is there a heuristic which suggests this? (Poonen) No. (Swinnerton-Dyer)

Problem/Question 15. Characterize the rational numbers α that can be written as

$$\alpha = \frac{2}{x_1^2 - 2} + \frac{2}{x_2^2 - 2} + \cdots + \frac{2}{x_n^2 - 2}$$

for $x_i \in \mathbb{Q}$ and fixed n. (Poonen)

It is necessary that $|\alpha|_p \le 1$ for $(2/p) = -1$ and $p = 2$. Is it sufficient?

Remarks.

(i) You might repeat this kind of problem with any rational function with no rational poles. (As in Waring's problem.) Something has already been done for a function with rational poles. (Poonen)

(ii) You can phrase this problem a different kind of way: prove or disprove the Hasse principle for this equation for all $\alpha \in \mathbb{Q}$. (Swinnerton-Dyer) You can probably show for n sufficiently large (and fixed) that there is a solution locally.

(iii) There are applications to Diophantine definitions: this would show that inside $\mathbb{Q}$, the set of these rational numbers which are integral at half of the places, is Diophantine. (Poonen)

Problem/Question 16. Solve the local-global solubility problem for finding lines on a cubic hypersurface. (Wooley)

(a) Find an example of a cubic hypersurface over $\mathbb{Q}_p$ (in as many variables as possible) with no rational line.

(b) Find an example of a cubic hypersurface over $\mathbb{Q}$ (in as many variables as possible) with no rational line.

Remarks.

(i) For (a), we must have at least 10 variables, since there are cubic forms in ≤ 9 variables with no point. If you have 14 variables, then there is a rational line. (Wooley)

(ii) For (b), for 37? variables, there is a rational line. (Wooley)

(iii) Also, find one with a rational point but no rational line. (Colliot-Thélène)

Problem/Question 17. Draw a regular pentagon P, construct the circle through the 5 vertices C, and consider the curve $E : P + \lambda C^2 = 0$. This is a quintic curve with 5 double points, and therefore has geometric genus 1. This curve has five points at ∞ (given by the slopes of the lines). Compute the 5-torsion of E. (McCallum)

Remarks.

(i) The points at ∞ are among the 5-torsion.

(ii) The motivation is: these curves are principal homogeneous spaces, and are candidates for 5-torsion elements in Ш. If λ is the parameter on $X_1(5)$, then this is a twist of the universal elliptic curve of $X_1(5)$. Here we have explicit models. (McCallum)

(iii) If you consider this as a pencil of elliptic curves, how does this relate to the talks at this conference? (Ellenberg)

(iv) Does the pentagon have to be regular? (Voloch) There are various variations, such as replacing the circle with a star pentagon.

Problem/Question 18.

(a) Find a separable polynomial $g(t) \in \mathbb{Q}[t]$ such that the Jacobian of the hyperelliptic curve $s^2 = g(t)$ is isogeneous over $\mathbb{Q}$ to $E^r \times B$, E an elliptic curve, with $r \geq 4$ or $r = 3$ and $\dim B \leq 1$. (Silverberg)

(b) Related problem: Give an example of a map $\mathbb{P}^1 \to E^4/\{\pm 1\}$, where ± 1 acts diagonally, whose image does not lie in $H/\{\pm 1\}$ for any subgroup $H \subsetneq E^4$. (Ellenberg)

Remarks.

(i) The case $r = 2$ and $\dim B = 0$ is possible, as is the case $r = 3$ and $\dim B = 2$. A consequence of this construction would be better bounds on the density of quadratic twists of E of rank $\geq r$. (Silverberg)
(ii) What if you ask this question over $\mathbb{C}$? (Voloch) Can at least do $r = 3$ and $\dim B = 0$ over $\mathbb{C}$. (Poonen) Even over $\mathbb{C}$, maybe it cannot be done for large r. (Ellenberg)
(iii) One might consider the curve $s^2 = t^k + 1$ over $\mathbb{Q}$, for k composite. If $3 \mid k$, for example, it maps to $s^2 = t^3 + 1$?
(iv) Does it have to be hyperelliptic? (Rodriguez-Villegas) Yes, for applications. (Ellenberg)
(v) The random matrix heuristics suggest that there is a positive power, so there should be a curve there, and finding such a curve would give a proof of a density result. (Ellenberg)
(vi) Take $E_1, E_2, E_3/\mathbb{Q}$ pairwise isogeneous elliptic curves, $A = E_1 \times E_2 \times E_3$, and look at the set of principal polarizations on X. Find a nonsplit principal polarization on A; then it comes from $A = \mathrm{Jac}(C)$, $g(C) = 3$. Now you just need to show that C is hyperelliptic.

Problem/Question 19. Let X be a variety over a number field k and suppose that for every open Zariski dense $U \subset X$, the map $\pi_1(U) \to \mathrm{Gal}(\overline{k}/k)$ has a splitting s (e.g. if $X(k)$ is Zariski dense). In this case, if $X(\mathbf{A}_k) \neq \emptyset$, is there no Brauer-Manin obstruction to the Hasse principle for X, i.e. is $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$? (Ellenberg)

Remarks.

(i) Is it possible that $X(\mathbf{A}_k) \neq \emptyset$ follows from the splitting condition? (Poonen) You might also ask the corresponding question for a local field. (McCallum)
(ii) You might also ask this question for other obstructions. (Ellenberg)

Problem/Question 20. Let $p(t) = 3(t^4 - 54t^2 - 117t - 243)$. Write the system of two equations $y^2 = p(t)(x^2 + 1)$, $z^2 = p(t)(x^2 + 2)$; think of this as a one-parameter family X of curves of genus one; $X(\mathbb{Q})$ is empty and $X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$ (Skorobogatov).

Is $X(k) \neq \emptyset$ for some $[k : \mathbb{Q}]$ odd? (Colliot-Thélène)

Remarks.

(i) The secret reason for asking: then X has a zero-cycle of degree 1. (Colliot-Thélène) If you have a zero cycle of degree 1, then there is such a point.
(ii) Even in a given number field of degree 3, looking at a random way, the evidence you will find is zero. (Colliot-Thélène)
(iii) What about $X \times X \times X$ modulo the action by three? (Ellenberg)
(iv) Reduce the search by finding one elliptic curve with many rational points (fix x, consider $y^2 = p(t)(x^2 + 1)$), then search for z. (Voloch) But the ratio y/z is only dependent on x. (Poonen)
(v) Do we expect $[k : \mathbb{Q}] = 3$? (McCallum) Not necessarily. (Colliot-Thélène)
(vi) Consider instead $w^2 = (x^2+2)(x^2+1)$ and $y^2 = p(t)(x^2+1)$; search now in the first curve for a cubic point, and search for t. (Poonen) Put the first one in Weierstrass form, and generate the cubic fields.

Problem/Question 21. Let $A/\mathbb{Z}$ be an algebra with $\mathrm{rk}_{\mathbb{Z}} A = 9$ given by its multiplication table. Suppose you know that $A \simeq M_3(\mathbb{Z})$; find an algorithm which gives an explicit isomorphism. (Stoll)

Remarks.

(i) The motivation comes from very explicit 3-descent on elliptic curves.
(ii) The case of $M_2(\mathbb{Z})$ reduces to finding rational points on conics. (Stoll)
(iii) Is this an LLL problem? (Voloch) In some sense, but one needs nine 3×3-matrices, not one 9×9-matrix; the equations are not all linear. (Stoll)

Problem/Question 22. Let k be a number field, $k \not\subset \mathbb{R}$. Construct an algebraic set $S \subset k^n$ for some n such that the projection onto one of the coordinates is exactly the set of elements of k with $|k| \leq 1$ for some (archimedean) absolute value $|\,|$ of k. (Shlapentokh)

Remark. This would imply results on Hilbert's tenth problem for rings of integers. It probably is hard because it is close to being equivalent.

Problem/Question 23. Let $E \subset \mathbb{P}^2$ be an elliptic curve over $\mathbb{Q}$, and suppose $E(\mathbb{Q}) \simeq \mathbb{Z}$. (Poonen)

(a) Describe $S \subset E(\mathbb{Q})$ where $S = \{(x, y) : y = a^2 + b^2,\ a, b \in \mathbb{Q}\}$. Is S is finite?
(b) More generally, $\pi : X \to E$ gives a subset $\pi(X(\mathbb{Q})) \subset E(\mathbb{Q})$; what others can you build?

Remark. It is possible to describe in a Diophantine way the set of points $S = \{(x, y) : 1 \leq y \leq 2\}$; this is an infinite set. (Poonen)

Problem/Question 24. Given an elliptic curve $E/\mathbb{Q}$, $\operatorname{rk} E(\mathbb{Q}) > 0$, describe the set of primes p such that $E(\mathbb{Q})$ is dense in $E(\mathbb{Q}_p)$. Is this set nonempty? Is there a modular interpretation of this problem? (Takloo-Bighash)

Remarks.

(i) You need surjectivity of the reduction map (Murty and Gupta have some results) and the surjectivity of the map on formal groups (Silverman). One suspects that for any such curve E there exists a prime p with this property.
(ii) This is related to Brauer-type problems for surfaces.
(iii) You should be able to collect data on this to see if there is a positive density. (McCallum)

Problem/Question 25. Is there an algorithm to decide solubility of a system of linear equations

$$a_{i1}x_1 + \cdots + a_{in}x_n = b_i$$

for $a_i, b, x_i \in \mathbb{Z}$, together with equations of the form

$$\{x_i\alpha_j\} < r_j$$

for $\alpha_j \in \mathbb{R} \setminus \mathbb{Q}$, $r_i \in \mathbb{Q}$? (Poonen)

Remarks.

(i) This is a problem in linear programming; add variables. (Voloch)
(ii) A negative answer would have implied undecidability for Hilbert's tenth problem over $\mathbb{Q}$.

Problem/Question 26. Describe the variety of curves of low degree on the Fermat variety $F : x_1^d + x_2^d + \cdots + x_6^d = 0$. (Heath-Brown)

Remarks.

(i) Lines are known, but that is all. Hope that there are none or very few.
(ii) The curves should be over $\mathbb{C}$ (for now).

Problem/Question 27. Given a plane curve of degree d, the number of points on X of height at most d is $\ll d^3$. There are curves which have the number of rational points $\gg d^2$. Can you do better than $\ll d^3$? (Heath-Brown)

Remarks. (Roger Heath-Brown, 2004-09-25) observes that actually $d^{5/2}$ is easy, so the challenge should be to improve on this.

Problem/Question 28. Let E be an elliptic curve over $\mathbb{Q}$, and $P \in E(\mathbb{Q})[3]$, $P \neq O$, such that $\operatorname{rk} E(\mathbb{Q}) = 0$. Let $K/\mathbb{Q}$ be a cyclic extension of degree 3 of conductor f, and let $\nu = \nu(f)$ be the number of distinct primes dividing f. It is true that $3^{\nu-1} \mid \# \operatorname{Sel}^3(E, K)$? (Chantal David)

Remarks. Let $K/\mathbb{Q}$ be a cyclic cubic extension. Then the 3-rank of the class group of K is controlled by primes dividing discriminant of K; if there are d such primes, then 3^{d-1} divides the class number h_K (genus theory). Problem: carry this over to a guaranteed contribution of 3-primary component of the 3-Selmer group (over K) of an elliptic curve $E/\mathbb{Q}$. Does 3^{d-1} divide the Selmer order?

Progress: Fix $E/\mathbb{Q}$ with a rational 3-torsion point, and let K vary as above. Then there is a constant c_E depending only on E such that 3^{d-c_E} divides the Selmer order. (Clarification request: do the mean the algebraic part of the L-function, or the 3-part of the Selmer group, or the group obtained from a 3-descent? That affects the value of c_E.)

This has been checked computationally (by checking special values of L-series).

Other problems? Poonen: replace 3 by another prime p, or replace $\mathbb{Q}$ by another number field, etc.

Problem/Question 29. If K is a field such that all $\mathscr{O}$-acyclic varieties over K have a point, is $\operatorname{Gal}(\overline{K}/K)$ topologically generated by one element?

Problem/Question 30. This problem has been withdrawn.

Problem/Question 31. Harmonic analysis and nonabelian torsors: Takloo-Bighash: Do these give you methods to find rational points? Hassett: Is there a harmonic analysis argument to count points on the quintic del Pezzo surface? Wooley: no examples known where you can combine harmonic analysis with torsors.

Problem/Question 32. (Voloch): Given a family of hypersurfaces, show that "almost all" members of the family satisfy the Hasse Principle in "interesting" circumstances.

Colliot-Thélène: maybe the opposite?

Poonen: the family was all hypersurfaces of degree d in $\mathbb{P}^n$ with coefficients of height $\leq H$, over some fixed number field K. The problem was: find the proportion of these that satisfy the Hasse Principle (originally, that have rational points, but we can find the local points easily).

Wooley and Venkatesh (tentative):

$$A^{-s}\#\{(a_1, \ldots, a_s) : |a_i| \leq A,\ a_1 x_1^d + \cdots + a_s x_s^d = 0 \ \text{ satisfies HP}\}$$

is asymptotic to the product of local densities, at least for $s \geq 3d+1$. This is progress for d large: for an individual $\underline{a}$, one has HP (using current technology) for $s >> d \log d$. Proof uses (of course) circle method.

de Jong: for cubics in $\mathbb{P}^2$, what do conclusions of this type say about 3-Selmer groups of elliptic curves?

Stoll: given local points, proportion that have rational points (i.e., satisfy HP) should be 0.

Mazur: can you put an exponent on that?

Stoll: wait for experimental evidence.

Problem/Question 33. (Poonen) Instead of counting points of bounded height on a variety, count points of bounded height in a Diophantine set. (I.e., counting points in a base the fibre above which has a rational point.) What rates of growth can you get? Example: conic bundle over an elliptic curve. Heuristically, it appears rate of growth can be $\log\log B$, whereas for varieties it always turns out to be $cB^{\alpha}(\log B)^{\beta}$.

Problem/Question 34. (Bogomolov) Replace Heath-Brown by Arakelov (et al).

$$\#\{(x,y,z)\in\mathbb{P}^2 : |x|,|y|,|z|\le B, P(x,y,z)=0\} << B^{\alpha+\epsilon}$$

with $\alpha \le \frac{2}{d}$, $d = \deg P$. Analogue for surfaces, etc.

Problem/Question 35. Weak approximation for complex function fields: Weak approximation over a finite extension L of $\mathbb{C}(t)$, from Hassett's lecture.

Colliot-Thélène: Known for X a connected linear algebraic group over L (reduce to reductive groups immediately; since field has cohomological dimension 1, one has Borel subgroup, reduce to tori; reduce to quasi-trivial tori, which are open subsets of affine space).

CT: $X = G/H$, where H is a subgroup of G (not necessarily normal). Same should go through if H is connected (techniques of Borovoi et al.).

CT: Question: Decide whether weak approximation holds for GL_n/G, where G is a finite subgroup of GL_n. This seems nontrivial. (de Jong thinks he can do this; Graber is unsure.) CT says de Jong claims: Let X/L be an arbitrary smooth projective, geometrically and rationally connected variety. Then weak approxmation holds. (de Jong: do this by reducing to characteristic p. Not in the dJ-H-S paper.)

CT: there is an Enriques surface over $\mathbb{C}(t)$ that has a rational point but does not satisfy weak approximation.

Remarks. Yuri Tschinkel remarks that there is progress on Nr 35 due to Colliot-Thelene/Gille and Madore. To this Brendan Hasset adds that Madore has announced a proof of weak approximation in smooth fibers for a cubic surface over the function field $K(C)$, where C is a curve and K is algebraically closed of characteristic zero.

B.2 Photos

William Stein has prepared a gallery of photos[3].

Chapter C: Glossary

Abelian variety: A smooth projective geometrically integral group variety over a field. Over the complex numbers abelian varieties are tori.

Brauer-Manin obstruction: The terminology is utterly awful! Many families don't satisfy Hasse Principle. One explanation of Manin (see his paper): a cohomological obstruction using the Brauer group of the variety.

[3] http://modular.fas.harvard.edu/pics/ascent11/12-2002/AIM_rational-points-workshop/

If a variety has a local point everywhere then it has an adelic point. Manin defined, using a cohomological condition involving Brauer group, a subset of the adelic points that must contain the global points. Let $X(\mathbb{A}_k)$ be the adelic points of X. Consider the subset of points P with the property that for every element $z \in \mathrm{Br}(X)$ the system of elements $(z_v(P))_v$ has sum of invariants $= 0$.

The B-M is an interesting construction in English. It is a nounal-phrase defined purely in terms of the sentences in which in which it may occur. There is no such actual object "the Brauer-Manin obstruction".

Example: A variety that satisfies $X(\mathbb{A}_k) \neq \emptyset$ and $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction.

For a long time people were interested in whether there are counterexamples ot Hasse principle not explained by the Brauer-Manin obstruction. $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ but still has no global point (Skorobogotav found first example).

After one glass of wine, McCallum advocates "$X(\mathbb{A}_k)^{\mathrm{Br}}$ should be called the set of Brauer points".

Brauer-Severi variety: A twist of projective space $\mathbf{P}^n$. Brauer-Severi varieties satisfy the Hasse principle.

BSD conjecture—BSD—Birch and Swinnerton-Dyer: Let A be an abelian variety over a global field K and let $L(A, s)$ be the associated L-function. The Birch and Swinnerton-Dyer conjecture asserts that $L(A, s)$ extends to an entire function and $\mathrm{ord}_{s=1} L(A, s)$ equals the rank of $A(K)$. Moreover, the conjecture provides a formula for the leading coefficient of the Taylor expansions of $L(A, s)$ about $s = 1$ in terms of invariants of A.

Calabi-Yau variety: An algebraic variety X over $\mathbf{C}$ is a Calabi-Yau variety if it has trivial canonical sheaf (i.e., the canonical sheaf is isomorphic to the structure sheaf). [Noriko just deleted the simply connected assumption.]

Del Pezzo surface: A Del Pezzo surface is a Fano variety of dimension two.

It can be shown that the Del Pezzo surfaces are exactly the surfaces that are geometrically either $\mathbf{P}^1 \times \mathbf{P}^1$ or a blowup of $\mathbf{P}^2$ at up to 8 points in general position. By *general position* we mean that no three points lie on a line, no six points lie on a conic, and no eight lie points lie on a singular cubic with one of the eight points on the singularity.

Descent:

A. The process of expressing the rational points on a variety as the union of images of rational points from other varieties.
B. The descent problem is as follows: Given a field extension L/K and a variety X over L, try to find a variety Y over K such that $X = Y \times_K L$.

Diophantine set: Let R be a ring. A subset $A \subset R^n$ is diophantine over R if there exists a polynomial $f \in R[t_1, \ldots, t_n, x_1, \ldots, x_m]$ such that

$$A = \{\vec{t} \in R^n : \exists \vec{x} \in R^m \text{ such that } f(\vec{t}, \vec{x}) = 0\}.$$

Enriques Surface: A quotient of a K3 surface by a fixed-point free involution.

Equivalently, the normalization of the singular surface of degree 6 in $\mathbf{P}^3$ whose singularities are double lines that form a general tetrahedron.

Over $\mathbf{C}$ an Enriques surface can be characterized cohomologically as follows: $H^0(\Omega_X^2) = 0$ and $2K_X = 0$ but $K_X \neq 0$.

Fano variety—Fano: Anticanonical divisor $\omega^{\otimes -1}$ is ample. This class of varieties is "simple" or "close to rational". For example, one conjectures that Brauer-Manin is only obstruction. Manin-Batyrev conjecture: asymptotic for number of points of bounded height. A Fano variety of dimension two is also called a Del Pezzo surface.

Fermat curve: A curve of the form $x^d + y^d = z^d$. Good examples of many phenomenon. Good source of challenge problems. (E.g., FLT.) Lot of symmetry so you can compute a lot with them. Computations are surprising and nontrivial. They're abelian covers of $\mathbf{P}^1$ ramified at 3 points, so they occur in the fund. group of...

More generally $x_1^d + \cdots + x_n^d = 0$ is sometimes called a Fermat variety.

General type: A variety X is of general type if there is a positive power of the canonical bundle whose global sections determine a rational map $f : X \to \mathbf{P}^n$ with $\dim f(X) = \dim X$. (If X is of general type then there exists some positive power of the canonical bundle such that the corresponding map is birational to its image.)

"It is a moral judgement of geometers that you would be wise to stay away from the bloody things." – Swinnerton-Dyer

Hardy-Littlewood circle method: An analytic method for obtaining asymptotic formulas for the number of solutions to certain equations satisfying certain bounds.

Hasse principle: A family of varieties satisfies the Hasse principle if whenever a variety in the family has points everywhere locally it has a point globally. Here "everywhere locally" means over the reals and p-adically for every p, and "globally" means over the rationals.

Everywhere local solubility is necessary for global solubility. Hasse proved that it is also sufficient in the case of quatratic forms.

Hilbert's tenth problem: Let R be a commutative ring. Hilbert's tenth problem for R is to determine if there is an algorithm that decides whether or not a given system of polynomial equations with coefficients in R has a solution over R.

Jacobian: The Jacobian of a nonsingular projective curve X is an abelian variety whose points are in bijection with the group $\mathrm{Pic}^0(X)$ of isomorphism classes of invertible sheaves (or divisor classes) of degree 0.

K3 surface: A surface with trivial canonical bundle and trivial fundamental group (i.e., a Calabi-Yau variety of dimension 2).

Lang's conjectures:

A. Suppose k is a number field and X is a variety over k of general type. Then $X(k)$ is not Zariski dense in X. (Also there are refinements where we specify which Zariski closed subset is supposed to contain $X(k)$.)
B. Suppose k is a number field and X is a variety over k. All but finitely many k-rational points on X lie in the special set.
C. Let X be a variety over a number field k. Choose an embedding of k into the complex number $\mathbf{C}$, and suppose that $X(\mathbf{C})$ is hyperbolic: this means that every holomorphic map $\mathbf{C} \to X(\mathbf{C})$ is constant. Then $X(k)$ is finite.

Local to global principle: Another name for the Hasse principle.

Picard group: The Picard group of a variety is the group of isomorphism classes of invertible sheaves.

Prym variety: A Prym variety is an abelian variety constructed in the following way. Let X and Y be curves and suppose $f : X \to Y$ is a degree 2 étale (unramified) cover. The associated Prym variety is the connected component of the kernel of the Albanese map $\mathrm{Jac}(X) \to \mathrm{Jac}(Y)$. The Prym variety can also be defined as the connected component of the -1 eigenspace of the involution on $\mathrm{Jac}(X)$ induced by f.

Rationally connected variety: There are three definitions of rationally connected. These are equivalent in characteristic zero but not in characteristic p.

A. For any two points $x, y \in X$ there exists a morphism $\phi : \mathbf{P}^1 \to X$ such that $\phi(0) = x$ and $\phi(\infty) = y$.
B. For any n points $x_1, \ldots, x_n \in X$ there exists a morphism $\phi : \mathbf{P}^1 \to X$ such that $\{x_1, \ldots, x_n\}$ is a subset of $\phi(\mathbf{P}^1)$.
C. For any two points $x, y \in X$ there exist morphisms $\phi_i : \mathbf{P}^1 \to X$ for $i = 1, \ldots, r$ such that $\phi_1(0) = x$, $\phi_r(0) = y$, and for each $i = 1, \ldots, r-1$ the images of ϕ_i and ϕ_{i+1} have nontrivial intersection.

Schinzel's Hypothesis: Suppose $f_1, \ldots, f_r \in \mathbf{Z}[x]$ are irreducible and no prime divides

$$f_1(n)f_2(n)\cdots f_r(n)$$

for all $n \in \mathbf{Z}$. Then there are infinitely many integers n such that $|f_1(n)|, \ldots, |f_r(n)|$ are simultaneously prime.

Selmer group: Given Galois cohomology definition for any $A \subset B$. Example $A = \ker(\phi)$ where ϕ is an isogeny of abelian variety. Accessible. It's what we can compute, at least in theory.

Shimura variety: A variety having a Zariski open subset whose set of complex points is analytically isomorphic to a quotient of a bounded symmetric domain X by a congruence subgroup of an algebraic group G that acts transitively on X. Examples include moduli spaces $X_0(N)$ of elliptic curves with extra structure and Shimura curves which parametrize quaternionic multiplication abelian surfaces with extra structure.

Special Set: The (algebraic) special set of a variety X is the Zariski closure of the union of all positive-dimensional images of morphisms from abelian varieties to X. Note that this contains all rational curves (since elliptic curves cover $\mathbf{P}^1$).

Torsor: Let B be a variety over a field k and let G be an algebraic group over k. A left B-torsor under G is a B-scheme X with a B-morphism $G \times_k X \to X$ such that for some étale covering $\{U_i \to B\}$ there is a G-equivariant isomorphism of U_i-schemes from $X \times U_i$ to $G \times U_i$, for all i. If $B = \mathrm{Spec}(k)$ these are also called principal homogenous spaces.

Waring's problem: Given k, find the smallest number g_k such that every positive integer is a sum of g_k positive kth powers. The "easier" Waring's problem refers to the analogous problem where the kth powers are permitted to be either positive or negative. Modification: Given k, find the smallest number G_k such that every sufficiently large positive integer is a sum of G_k positive kth powers.

Weak approximation: For a projective variety X over a global field, say weak approximation holds if $X(K)$ is dense in the adelic points $X(\mathbb{A}_K)$. Simplest example where it holds:

$\mathbf{P}^0$, also $\mathbf{P}^1$. It does not hold for an elliptic curve over K. (For example, if E has rank 0 it clearly doesn't hold... but more generally could divide all generators by 2 and choose a prime that splits completely.)

Example: "Weak approximation does not hold for cubic surfaces."

Example: "The theory of abelian descent in some cases reduces the question of whether the Brauer-Manin obstruction is the only obstruction to Hasse on a base variety X to the question of whether weak approximation holds for a universal torsor."

Example: "Weak approximation on a moduli space of varieties yields the existence of varieties over a global field satisfying certain local conditions. For example, we want to know there is an elliptic curve over $\mathbf{Q}$ with certain behavior at 3, 5, 13, as long as can do it over local fields with that behavior, weak approximation on the moduli space gives you a global curve that has those properties (because $\mathbf{P}^1$ satisfies weak approximation).'

Chapter D: Miscellaneous Photos

William Stein has prepared a gallery of photos[4].

[4]http://modular.fas.harvard.edu/pics/ascent11/12-2002/AIM_rational-points-workshop/