Rational Points Notes

Niven Achenjang

April 2022

These are notes on talks given in "Rational Points 2022 Workshop" which took place at Franken-Akademie Schloss Schney. Unfortunately for the reader, these notes are live-texed and so their quality is upper bounded both by my (quite) limited ability to understand the material in real time and by my typing speed. With that in mind, they are doubtlessly missing content/insight present in the talks and certainly contain confusions not present in the talks. Despite all this, I hope that you can still find some use of them. Enjoy and happy mathing.

The website for this seminar is available here.

Contents

List of Figures

List of Tables

1 Day 1 (3/28/2022)

1.1 Tom Fischer: Computing the Cassels-Tate pairing on 2-Selmer groups of genus 2 Jacobians

Let C be a smooth genus 2 curve over a number field k, and write $C : y^2 = f(x)$ with $f \in k[x]$ of degree 6. Furthermore, f has nonzero discriminant $\Delta(f) \neq 0$. Consider $L = k[x]/(f(x)) = k[\theta]$ (so $f(\theta) = 0$), the étale algebra for the set of Weierstrass points W (roots of f). We also let $J = \mathrm{Jac}(C)$ be the Jacobian.

Remark 1.1.1. partition of W into 2 sets of even size ($2^{\#W-2} = 2^4$ such things) are in bijection with $J[2]$. Furthermore, partitions of W into 2 sets of odd size form a $J[2]$-torsor, i.e. given an element $c \in \mathrm{H}^1(k, J[2])$. ∘

(I missed why, but if there is a rational Weierstrass point, then c will be trivial).

We're interested in the 2-Selmer group $S^{(2)}(J/k) \subset \mathrm{H}^1(k, J[2])$.

Fact. $c \in S^{(2)}(J/k)$

Traditionally, people don't consider the 2-Selmer group itself, but instead the **fake Selmer group**

$$S^{(2)}_{\text{fake}}(J/k) = S^{(2)}(J/k)/\langle c \rangle \subset \mathrm{H}^1(k, J[2])^{\cup c=0}/\langle c \rangle \cong \left(L^\times/(k^\times (L^\times)^2)\right)^{N=\square}.$$

The utilitiy of this is that the map from $J(k)/2J(k)$ to the RHS above could be written down explicitly.

It was later realized (by Stoll and another) that

$$\mathrm{H}^1(k, J[2])^{\cup c=0} \cong \frac{\left\{(\xi, m) \in L^\times \times k^\times : \mathrm{Nm}_{L/k}(\xi) = m^2\right\}}{\{(r\nu^2, r^3 \,\mathrm{Nm}(\nu)) \mid r \in k^\times, \nu \in L^\times\}}.$$

Ways to represent elements of $S^{(2)}(J/k)$:

- Pairs (ξ, m) as above
- Pairs of quadratic forms $G = x_1x_6 + x_2x_5 + x_3x_4$ and $H = \sum_{i,j=1}^6 a_{ij}x_ix_j$ (first one always the same, second one general)
- 4×4 skew symmetric matrices Φ over L

Let's describe how to go between these representations.

Remark 1.1.2. Given $(x, x') \in C(k)$, its image in $(L^\times/(k^\times(L^\times)^2))$ is $(x - \theta)(x' - \theta)$. ∘

(1) Can we write $(x - \theta)(x' - \theta) = \xi(u_0 + u_1\theta + \cdots + u_5\theta^5)^2$. Look at coeffs of $\theta^3, \theta^4, \theta^5$ which leads to equations of (a twisted form of?) the desingularized Kummer $\{G = H = S = 0\} \subset \mathbb{P}^5$ (a degree 8 surface). Here, G corresponds the coeff of θ^5 and G, H vanish together correspond to coeffs of θ^5, θ^4 together. Once you have G, H, it's apparently possible to recover S, so only need the pair G, H. We still need to say why we can always take G is the form given earlier. Note that the standard G has a 3-dimensional isotropic subspace ($x_1 = x_2 = x_3 = 0$). In general, the coeff of θ^5 will always have such a thing (coming from it representing a Selmer element).

Fact. 3-dimensional isotropic subspaces for G are parameterized by $\mathbb{P}^3 \sqcup \mathbb{P}^3$.

(working with something that's not a Selmer element, would get a Brauer-Severi $\sqcup$ its dual above instead)

(2) Say we have G, H quadratic forms (we'll use same variables for corresponding 6×6 symmetric matrices). It turns out that $\det(xG+H)$ is $f(x)$, up to scaling (if I heard correctly). Hence, $\det(\theta G+H) = 0$. In fact, $\operatorname{rank}(\theta G + H) = 5$, so its kernel is spanned by a single vector v. This v (which is 6 numbers) gives our skew symmetric matrix Φ ($\dim(4 \times 4$ skew symmetric matrices$) = 6$).

(3) $\xi = \operatorname{Pf}(\Phi)/f'(\theta)$ with $\operatorname{Pf}(-)$ the *Pfaffian*. There is also a formula for m, but it's more messy.

Notation 1.1.3. For A a 4×4 skew symmetric matrix, we write $A^* := \operatorname{Pf}(A)A^{-1}$, so $AA^* = A^*A = \operatorname{Pf}(A)I$.

Let's now turn to the Cassels-Tate pairing

$$\langle -, - \rangle_{\mathrm{CT}} : S^{(2)}(J/k) \times S^{(2)}(J/k) \longrightarrow \mathbb{F}_2.$$

It is

- (skew-)symmetric, bilinear
- kernel is image of $S^{(4)}(J/k)$ (in particular, includes things in the image of $J[2]$)
- $\langle x, x + c \rangle = 0$ for all $x \in S^{(2)}(J/k)$
- $\langle c, c \rangle = \#(\text{deficient places}) \mod 2$

An $\varepsilon \in S^{(2)}(J/k)$ will give a two covering of the Jacobian: $J_\varepsilon \to J$ which is isomorphic to $J \xrightarrow{\cdot 2} J$ over $\overline{k}$. Note we have $J \to J/[-1] = K \subset \mathbb{P}^3$ the standard Kummer. J_ε above has an involution ι and so we get $J_\varepsilon \xrightarrow{\pi_\varepsilon} J_\varepsilon/\iota = K_\varepsilon \subset \mathbb{P}^3$ with K_ε a twisted Kummer.

Consider the dual Kummer surface $(K_\varepsilon)^\vee \subset \left(\mathbb{P}^3\right)^\vee$

Fact.

(i) $(K_\varepsilon)^\vee = K_{\varepsilon+c}$ (these become isomorphic over a field of definition for a Weierstrass point (since $c = 0$). In fact, they become isomorphic over L)

(ii) The isomorphic $K_\varepsilon \to (K_\varepsilon)^\vee$ defined over L is given by Φ (a linear map between 4-dimensional vector space and its dual)

(iii) There is a formula to go from Φ to an equation for K_ε

How to compute $\langle \varepsilon, \eta \rangle_{\mathrm{CT}}$?

Assumption. We need to suppose that we can find a point $P_\eta \in K_\eta(k)$ (in particular, $K_\eta(k) \neq \emptyset$). This will lift to a $k(\sqrt{a})$-point of J_η.

(Can assume a is not a square. If it is, then the pairing is trivial, I think?)

Let $x_1, \ldots, x_4$ be the coordinates on $\mathbb{P}^3 \supset K_\varepsilon$. We want a compute a quadratic form $g \in k[x_1, \ldots, x_4]$ such that the quaternion algebra

$$\left(a, \pi_\varepsilon^* \left(\frac{g}{x_1^2}\right)\right) \in \operatorname{Br}(J_\varepsilon)$$

corresponds to η. Then,

$$\langle \varepsilon, \eta \rangle_{CT} = \sum_v (a, g(\pi_\varepsilon(P_v)))_v$$

where $(-,-)_v : k_v^\times/(k_v^\times)^2 \times k_v^\times (k_v^\times)^2 \to \mathbb{F}_2$ (Hilbert symbol?) and $P_v \in J_\varepsilon(k_v)$ (any local point?).

How to compute g?

Recall 1.1.4. The standard Kummer surface is $K = J/[-1] \subset \mathbb{P}^3$ with coordinates $x_1, \dots, x_4$.

The group law on J does not give a group law on K, but one can show that

$$x_i(P+Q)x_j(P-Q) + x_i(P-Q)x_j(P+Q)$$

is a $(2,2)$-form in $x_1(P), \dots, x_4(P), x_1(Q), \dots, x_4(Q)$. This writes down $\binom{4}{2} = 6$ forms, and so can be packaged together into a $(2,2,2)$-form on $\mathbb{P}^3 \times \mathbb{P}^3 \times \left(\mathbb{P}^3\right)^\vee$ (think of these 6 forms as coefficients of another quadratic form).

Remark 1.1.5. You can twist the group law on J to get a map $J_\varepsilon \times J_\eta \to J_{\varepsilon+\eta}$. ∘

We have $K_\varepsilon, K_\eta \subset \mathbb{P}^3$ and $(K_{\varepsilon+\eta})^\vee \subset \left(\mathbb{P}^3\right)^\vee$. One can get a twisted $(2,2,2)$-form F on $\mathbb{P}^3 \times \mathbb{P}^3 \times \left(\mathbb{P}^3\right)^\vee$. We take

$$g(x_1, \dots, x_4) = F(x_1, \dots, x_4; P_\eta; 1, 0, 0, 0).$$

(third set of variables could be whatever you like)

How to compute F?

Write L_{10} for the étale algebra for ways to partition W into 2 sets of size 3 (note $10 = \binom{6}{3}/2$). There is an isomorphism $K_\varepsilon \to (K_\varepsilon)^\vee$ over L_{10} given by a 4×4 symmetric matrix over L_{10}. This gives a quadratic form H_ε. We can get a $(2,2,2)$-form by considering

$$F(x,y,z) = \mathrm{Tr}_{L_{10}/k} \left(\frac{H_\varepsilon(x) H_\eta(y) H^\vee_{\varepsilon+\eta}(z)}{\delta \prod_{i=1}^3 f'(\theta_i) \nu(\theta_i)} \right),$$

where

- the partition of W is $(\{\theta_1, \theta_2, \theta_3\}$,the rest)
- $\delta = (\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta_1)$
- $H_\varepsilon = \Phi_\varepsilon(\theta_1)\Phi_\varepsilon(\theta_2)^*\Phi_\varepsilon(\theta_3)$

  (switch which Φ's have the $*$ for $H^\vee$)
- Φ_ε gives rise to a pair $(\xi_\varepsilon, m_\varepsilon)$ as before (in particular, $\xi_\varepsilon = \mathrm{Pf}(\Phi_\varepsilon)/f'(\theta)$). Furthermore,

  $$(x i_\varepsilon \xi_\eta \xi_{\varepsilon+\eta}, m_\varepsilon m_\eta m_{\varepsilon+\eta}) = \left(r\nu^2, r^3 \,\mathrm{Nm}_{L/k}(\nu)\right)$$

  is trivial in the Selmer group

1.2 Himanshu Shukla: Computing Cassels-Tate pairing on the 2-Selmer group of odd-degree hyperelliptic curve

Notation 1.2.1. Let k be a number field with absolute Galois group G_k. Let

$$C : y^2 = f(x) \text{ with } \deg f = 2g + 1,$$

so $g(C) = g$ and let J be its Jacobian.

Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g + 1\}$ be the set of points corresponding to roots e_i of f. Let T_0 be the point at ∞.

More notation I missed...

Recall 1.2.2.

$$\mathrm{Sel}^{(n)}(J) := \ker\left(\mathrm{H}^1(G_k, J[n]) \to \prod_v \mathrm{H}^1(G_{k_v}, J)\right)$$

and also Sha...

Consider the Cassels-Tate pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J) \times Ш(J) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

which is anti-symmetric and non-degenerate (on the quotient $Ш(J)_{nd}$). It was defined by Cassels for elliptic curves, generalized to abelian varieties by Tate, and then Poonen-Stoll gave another definition (Albanese-Albanese definition).

Remark 1.2.3 (Albanese-Albanese definition of CTP). Choose uniforizers t_P for $P \in C$ Galois-equivariants. Consider Galois-equivariant pairings

$$\begin{array}{rccc} \langle -, - \rangle_1 : & \mathrm{Prin}(C) \times \mathrm{Div}^0(C) & \longrightarrow & \mathbb{G}_m \\ & (\mathrm{div}(f), D) & \longmapsto & \displaystyle\prod_{P \in \mathrm{supp}(D)} \left(f t_P^{-v_P(f)}(P)\right)^{v_P(D)} \end{array}$$

and missed the other... ∘

This is too fast for me to reasonably expect to take notes...

1.3 Timo Keller: Verification of the Strong BSD Conjecture for Abelian Surfaces over $\mathbb{Q}$

(joint w/ Michael Stoll)

1.3.1 BSD State of the art

- BSD was formulated in 1965
- Coates-Wiles (1977): $r_{an} = 0 \implies r = 0$ for E CM
- Gross-Zagier (1986): $r_{an} = 1 \implies r \geq 1$ for E modular

- Rubin (1987): $r_{an} = 0 \implies Ш(E/K)$ finite for E/K CM
- many more, but too fast for me...

Let A be a modular abelian variety over $\mathbb{Q}$ wi/ associated newform f. Assume the L-rank $\operatorname{ord}_{s=1} L(f,s)$ equals 0 or 1. This implies by Gross-Zagier that $r \geq r_{an}$ and $\#Ш(A/\mathbb{Q})_{an} \in \mathbb{Q}_{>0}$. The Heegner point Euler system gives $r = r_{an}$ and $\#Ш < \infty$. It doesn't directly give $\#Ш = \#Ш_{an}$.

- For elliptic curves, strong BSD verified exactly for levels $N < 5000$
- In dimension > 1:
  - BSD fors some Jacobians of dimension 2numerically
  - GL_2 Iwasawa Main Conjecture for primes p of good orindary reduction and ρ_p irreducible
  - GL_2 IMW for primes p of bad multiplicative reducation and ρ_p irreducible
  - BSD for some hyperelliptic Jacobians numerically up to squares
  - $v_p(\#Ш(A/\mathbb{Q})) = v_p(\#Ш(A/\mathbb{Q})_{an})$ if N square-free, $p \nmid N$, and ρ_p irreducible

Theorem 1.3.1 (corollary of Serre's Modularity Conjecture)**.** *Let $A/\mathbb{Q}$ be an absolutely simple abelian variety. Then, TFAE*

- *$A/\mathbb{Q}$ has real multiplication*
- *A is of GL_2-type over $\mathbb{Q}$, i.e. $\dim_{\mathrm{End}(A)\otimes\mathbb{Q}_\ell}(V_\ell A) = 2$*
- *A is an isogeny quotient of $J_0(N)$ for some N*
- *$L(A/\mathbb{Q}, s) = \prod_{\alpha:\mathscr{O}\hookrightarrow\mathbb{C}} L(f^\alpha, s)$ for some newform $f \in S_2(\Gamma_0(N), \mathscr{O})$*

If this is the case, we call $A/\mathbb{Q}$ modular, and then $N^{\dim A}$ is the conductor of A

Remark 1.3.2 (Problems if $\dim A > 1$). We don't have an analog of Mazur's classification of rational isogenies of prime degree for all A: $\dim \mathcal{A}_2 = 3 \cdot 2 - 3 = 3$

We don't have an explicit Serre's open image theorem for $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/Q) \to \mathrm{GL}_2(\mathscr{O}_\mathfrak{p})$ ∘

In this talk, for a given modular abelian surface A, we

- explicitly prove that almost all $\rho_\mathfrak{p}$ are irreducible and maximal
- compute the Heegner index $I_K = [A(K) : \mathscr{O} y_K]$
- and use this to compute $\#Ш$...

Theorem 1.3.3 (K.)**.** *Let A be a modular abelian variety over $\mathbb{Q}$. One has $Ш(A/\mathbb{Q})[\mathfrak{p}] = 0$ for all $\mathfrak{p}$ with*

- *$\rho_\mathfrak{p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_\mathfrak{p}}(A[\mathfrak{p}](\overline{\mathbb{Q}}))$ irreducible and*
- *$\mathfrak{p} \nmid 2d \gcd_K(I_K)$ with Heegner indices I_K and Tamagawa product c (both can be refined to $\mathscr{O}$-ideals)*

These $\mathfrak{p}$ are explicitly computable

(gives finite support of Ш)

Slides going too fast for me...

1.4 Masahiro Nakahara: The elliptic sieve and Brauer groups

(w/ Subham Bhakta, Daniel Loughran, and Simon Rydin Myerson)

No Brauer groups until the end.

Question 1.4.1. *How often is a natural number a sum of two squares?*

Fermat: $p = \square + \square \iff p = 2$ or $p \equiv 1 \pmod 4$

Proposition 1.4.2. *Let $n \in \mathbb{N}$. Then, $n = \square + \square$ iff every prime $p \equiv 3 \pmod 4$ occurs to an even power in the prime factorization of n.*

Theorem 1.4.3 (Landau-Ramanujan)**.** $\#\{n \in \mathbb{N} : n < B, n = \square + \square\} \asymp B/(\log B)^{1/2}$

(they even give an explicit constant for the growth rate, but we don't care for this talk)

Note $n = \square + \square$ can be rephrased as a certain conic having rational points.

Theorem 1.4.4 (Serre, 1990)**.** *Let $\pi : X \to \mathbb{P}^n_{\mathbb{Q}}$ be a conic bundle. As long as π doesn't have a section,*

$$\#\{x \in \mathbb{P}^n(\mathbb{Q}) : H(x) \leq B, x \in \pi(X(\mathbb{Q}))\} \ll B^{n+1}/(\log B)^{\omega},$$

for some $\omega > 0$. here H denotes the naive height on $\mathbb{P}^n_{\mathbb{Q}}$.

(Compare: rational points on $\mathbb{P}^n$ grow like B^{n+1})

This has been generalized

- Loughran-Smeets '16

  Extended this to general fibrations $X \to \mathbb{P}^n$. Give bound for number of every locally soluble fibers which is conjecture to be the true bound

- Browning-Loughran '19

  Similar results for fibrations $X \to Y$ where Y is an almost Fano variety

What about more general base varieties, like an elliptic curve?

Theorem 1.4.5 (Bhakta, Loughran, Rydin Myerson, N, 2021)**.** *Let E be an elliptic curve, and let $\pi : X \to E$ be a conic bundle. Let $P \in E(\mathbb{Q})$ be a point of infinite order, and assume that the fiber over some multiple mP is non-split ($\implies$ singular?) w/ imaginary quadratic splitting field. Assume furthermore that $E(\mathbb{R})$ is connected. Then,*

$$\#\{n \in \mathbb{Z} : |n| < B, nP \in \pi(X(\mathbb{Q}))\} \ll B/(\log B)^{\omega}$$

for some $\omega > 0$.

Warning 1.4.6. This theorem is false if $E(\mathbb{R})$ is not connected or it the fiber over mP does not have an imaginary quadratic splitting field.

On can also stat this in terms of heights, but the curren formulation is more natural given the proof.

Corollary 1.4.7. *Let E be an elliptic curve. Let $P \in E(\mathbb{Q})$ be a point of infinite order. Assume that $E(\mathbb{R})$ is connected. Then,*

$$\#\{n \in \mathbb{Z} : |n| < B, y(nP) = \square + \square\} \ll B/(\log B)^{\omega}$$

for some $\omega > 0$

Warning 1.4.8. The same result with x-coordinates is false. The for example the curve $y^2 = x^3 - 1$. Then,

$$x = \left(\frac{y}{x}\right)^2 + \left(\frac{1}{x}\right)^2$$

is always a sum of two squares.

1.4.1 Proof for the sum of squares example

For simplicity, assume $P = (a_1, b_1)$ with $a_1, b_1 \in \mathbb{Z}$. Write

$$nP = \left(\frac{a_n}{d_n^2}, \frac{b_n}{d_n^3}\right) \text{ with } a_n, b_n, d_n \in \mathbb{Z}$$

in lowest terms and $d_n > 0$. Is b_n/d_n^3 a sum of squares? Forgetting about b_n, the answer is NO if $p \equiv 3 \mod 4$ divides d_n to an odd power. Furthermore, if $d_n \equiv 3 \mod 4$, there must be a prime $p \equiv 3 \mod 4$ dividing d_n to an odd power.

Examine how often $d_n \equiv 3 \mod 4$.

Definition 1.4.9. An **elliptic divisibility sequence** is a sequence ψ_n of integers such that $\psi_1 = 1$, $\psi_n \mid \psi_m$ if $n \mid m$, and

$$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2$$

for all integers $m > n > r$.

Motivation comes from division polynomials associated to an elliptic curve $E : y^2 = x^3 + ax + b$. These are

$$\Psi_1 = 1, \Psi_2 = 2y, \Psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \Psi_4 = 2\Psi_2(...), \ldots$$

Plugging in a point $(x, y) \in E(\mathbb{Z})$, then $\psi_n = \Psi_n(x, y)$ gives an elliptic divisibility sequence. Moreover,

$$nE(x, y) = \left(\frac{x\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{???}^2}{???}\right)$$

Fact. Up to sign, d_n is an EDS if P has everywhere good reduction

Theorem 1.4.10 (Verzobio 2021)**.** *Let $e_n = \text{sign}(\psi_n)d_n$. Let kP be the smallest positive multiple of P that has every good reduction. Then,*

$$e_{m+n}e_{m-n}e_r^2 = e_{m+r}e_{m-r}e_n^2 - e_{n+r}e_{n-r}e_m^2$$

holds for any integers $m > n > r$ as long as k divides at least two of them.

The periodic properties of EDSs (modulo primes) has been studied extensively by Ward '48, Ayad '93, Shipsey '00, Stange '11.

Proposition 1.4.11. *The sequence $e_n \mod 4$ is periodic, say with period $\delta \in \mathbb{N}$.*

Going back, we have $d_n \equiv 3 \mod 4$ if $e_n \equiv 1 \mod 4$ and $e_n < 0$.

Theorem 1.4.12. *There is a sign $\sigma \in \{\pm 1\}$ and an irrational number α such that if $P \in E(\mathbb{R})^0$, then $\sigma^{n-1} \operatorname{sign}(e_n) = (-1)^{\lfloor n\alpha \rfloor}$ for all $n \in \mathbb{N}$*

Since $E(\mathbb{R})$ is connected, $\operatorname{sign}(e_n)$ is equidistributed among $n \mod \delta$. Since $e_1 = 1$, we get many $e_n \equiv 1 \mod 4$ and $e_n < 0$ by periodicity. Using this, we can obtain

$$\#\{\text{primes } \ell \leq x : d_\ell \equiv 3 \mod 4\} \gg \frac{x}{\log x}.$$

For any such ℓ, there are no rational points above $n\ell P$ for "most" integers n. If we ignore the "most" part, we get

$$\#\{|n| \leq B : nP \in \pi(X(\mathbb{Q}))\} \leq \#\{|n| \leq B : d_\ell \equiv 3 \mod 4 \implies \ell \nmid n\} = B \prod_{d_\ell \equiv 3 \mod 4, \ell \leq B} \left(1 - \frac{1}{\ell}\right) \ll \frac{B}{(\log B)^\omega}$$

for some $\omega > 0$.

1.4.2 Generalization to Brauer groups

A conic bundle of $E \longrightarrow$ Quaternion algebra $b \in \mathbb{Q}(E)$.

Non-split fiber over $mP \in E(\mathbb{Q}) \longrightarrow$ Ramification of b at mP

$nP \in \pi(X(\mathbb{Q})) \longrightarrow$ The restriction of b to nP, $b(nP) = 0 \in \operatorname{Br} \mathbb{Q}$

In our special case: $|e_n| \equiv 3 \mod 4 \longrightarrow \chi(|e_n|) \neq 0, 1$ where χ Dirichlet character associated to b obtained using the residue map ???

Theorem 1.4.13. *Let $P \in E(\mathbb{Q})$ have infinite order. Assume that $b \in \operatorname{Br} \mathbb{Q}(E)$ is ramified at some multiple mP and let the associated Dirichlet character χ have modulus $q(\chi)$. Let e_n be the sequence as before and let δ be the period of the sequence $e_n \mod q(\chi)$. Assume that there is some index $\alpha \in \mathbb{N}$ with $\gcd(\alpha, \delta) = 1$ where*

- *$\chi(|e_\alpha|) \neq 0, 1$ or*
- *$\chi(-|e_\alpha|) \neq 0, 1$ and $P \in E(\mathbb{R})^0$, or*
- *$\chi(-|e_\alpha|) \neq 0, 1$ and $4 \nmid \delta$*

Then,

$$\#\{|n| \leq B : b(nP) = 0 \in \operatorname{Br} \mathbb{Q}\} \ll \frac{B \log\log B}{(\log B)^{1/2\varphi(?)}}.$$

Open Question 1.4.14. *Any lower bounds? Is the set of points with $y = \square + \square$ even infinite?*

Open Question 1.4.15. *What about conic bundles $X \to E$ when E has rank > 1? Can we get similar bounds when counting by height*

Open Question 1.4.16. *Do the assumptions in the last general theorem always hold for any elliptic curve and Brauer class?*

1.5 Ludwig Fürst: Explicit methods for hyperelliptic genus 4 Kummer varieties

Let $F(X,Z) = f_0 Z^{2g+2} + \cdots + f_{2g+2} X^{2g+2}$ be a homogeneous polynomial of degree $2g+2$ over a number field k with $\mathrm{Disc}(F) \neq 0$. Then, $Y^2 = F(X,Z)$ defines a nonsingular curve C of genus g in the weighted projective plane $\mathbb{P}(1, g+1, 1)$. To this curve, we associate is Jacobian $J(C) = \mathrm{Pic}^0_{C/k}$ and its Kummer variety $K(C) = J(C)/(-1)$. The Kummer varieties retains traces of the group law on the Jacobian such as scalar multiplication, addition of the 2-torsion, pseudo-addition, and the notion of the height of points. Using the linear system of twice a theta-divisor, we can embed K into a projective space of dimension $2^g - 1$. Using such an embedding, we can do explicit versions of these things.

- For $g = 2$, an embedding and many related objects have been constructed by Flynn (1993) and generalized by Duquesne (2007) and Müller (2010)

  The theory of heights was further developed by Stoll (1999, 2002) and Müller,Stoll (2016)

- For $g = 3$ in the case of odd degree an embedding has been found by Stubbs (2000) in his thesis. This was further studied by Duquesne (2001) and Müller (2012). The general case was analyzed extensively in Stoll (2017).

- Some results have been found for arbitrary genus. So developed Holems and Müller a height algorithm on the Jacobian using Arakelov intersection theory.

In the case $g = 4$, Ludwig found explict descriptions of

- Embedding of the (dual) Kummer variety
- Defining equations of the Kummer (*)
- Addition of $J[2]$
- Duplication formulas
- height algorithm (*)
- Pseudo-Addition (*)
- Lifting of points to the Jacobian

Let's see these in a bit more detail.

Embedding Represent a point on the Jacobian using the reduced Mumford representation (A, B, C) with $F = B^2 - AC$. This is in $g = 4$ unique up to scaling and to $B \mod A$. Behind this is the identifiction of J with $\mathrm{Pic}^4(C)$.

For a divisor of degree 4 (i.e. $\deg A = 4, \deg B = 5, \deg C = 6$), we find functions on the Jacobian as invariant polynomials in the coefficients with certain weights. Using this, Ludwig finds a basis for $L(2\Theta)$ which give embedding $J \to K \to \mathbb{P}^{15}$

The image of divisors of degree 2 can be found via a specialization argument

The dual of the Kummer comes from $\mathrm{Pic}^5(C)$ and corresponds to representations (A, B, C) with (A having?) odd degree. Here Ludwig finds a basis similar to the case of genus 3.

Defining equations The embedded Kummer variety can be defined by 1820 quartics. 1780 of them have been explicitly found.

There are 10 quadrics vanishing on the Kummer and 16 independent cubics.

Currently, there are 35 quartics missing and the equations do not define the Kummer in $\mathrm{char}(k) < 11$.

I'm gonna stop taking notes for now...

2 Day 2

2.1 Philipp Habegger: Uniformity for the Number of Rational Points on a Curve (I)

Note 1. Almost 5 minutes late

Let F be a number field, and let $\mathcal{C}$ be a smooth, project irred scheme of dimension 1 over F (i.e. a curve) of genus g.

Theorem 2.1.1 (Faltings 1983)**.** $g \geq 2 \implies C(F)$ *finite*

Vojta gave a new proof in 1991 and Lawrence-Venkatesh gave a new new one in 2019.

Question 2.1.2. *Effectivity? No news*

except maybe Levent's paper

Can we bound $\#C(F)$ from above (instead of bounding heights of points)?

Parshin (Szpiro) showed that Falting's proof gave an upper bound in principle (roughly 1985)

Vojta's proof showed $\#C(F)$ boundable. Rémond, David-Philppon ($\sim$ 2000) gave some bound. Say $\mathcal{C}$ as before, now with genus $g \geq 2$. Assume there's some rational point and use this to give an embedding $\mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C})$. Together, these two groups of author's show that

$$\#\mathcal{C}(F) \leq \left[\left(2^{34} g [F:\mathbb{Q}] \max(1, h(\mathrm{Jac}(\mathcal{C})))\right)^{g^{20}}\right]^{1+\mathrm{rank}\,\mathrm{Jac}(\mathcal{C})(F)}$$

(height of Jacobian measuring size of coefficients cutting it out as a projective variety). This bound is in practice too big to be sharp.

What invariants showing up are indeed necessary?

Example. $\mathcal{C} : y^2 = x(x-1)\dots(x-2022)$. This has genus $g = 1011$ and at least 2024 rational points ($(0,n)$ for $n \leq 2022$ + the point at ∞). This gives

$$\#C(\mathbb{Q}) \geq 2g + 2.$$

$\triangle$

Using a different construction, Menstre found $\mathcal{C}$ with $\#\mathcal{C}(\mathbb{Q}) \geq 8g + 16$.

Thus, the number of points must depend at least linearly on the genus.

Example. $\mathcal{C} : y^2 = x^5 - 1$. This has points

$$(1,0), (2, \pm\sqrt{31}), (3, \pm\sqrt{242}), \dots$$

Each new square root basically doubles the degree, so this construction shows bound must grow at least logarithmically in the degree of the field. △

Apparently looking at CM points on high degree modular curves can give a linear lower bound in the degree of the field.

Conjecture 2.1.3 (Caporaso-Harris-Mazue)**.** *There exists some $B(g,F) \geq 1$ s.t. any $\mathcal{C}/F$ of genus $g \geq 2$ satisfies $\#\mathcal{C}(F) \leq B(g,F)$.*

Conjecture 2.1.4 (Poocheli (spelling?))**.** *Same as above but with F replaced by $[F:\mathbb{Q}]$*

Evidence for this conjecture:

- If $\operatorname{rank}\operatorname{Jac}(\mathcal{C})(F) \leq g-3$, then CHM holds by work of Stoll, Zureick-Brown, Katz, Rabinoff (using Chabauty, I think)

Question 2.1.5 (Mazur)**.** *Can we bound*

$$\#\mathcal{C}(F) \leq B(g, F, \operatorname{rank}\operatorname{Jac}(\mathcal{C})(F))?$$

(not needing e.g. the (Falting's) height of the Jacobian)

Remark 2.1.6. g is geometric, while $F, \operatorname{rank}\operatorname{Jac}(\mathcal{C})(F)$ are both arithmetic ∘

2.1.1 Vojta's method

Recall 2.1.7 (height machinery)**.** There's the **absolute logarithmic Weil height** $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0,\infty)$. E.g.

$$h([a_0,\dots,a_n]) = \log \max_i |a_i| \text{ if } (a_0,\dots,a_n) \in \mathbb{Z}^{n+1} \setminus 0 \text{ and } \gcd_i(a_i) = 1.$$

Say $(A,\mathscr{L})$ is a polarized abelian variety over F. Say $\mathscr{L}$ is very ample and symmetric, so it given an embedding $\iota : A \hookrightarrow \mathbb{P}^n$. Pulling back the weil height gives a naive height $h_{\mathscr{L}}(P) = h(\iota(P))$ on A. This won't be compatible with the group structure in general, so one normalizes it by setting

$$\widehat{h}_{\mathscr{L}}(P) = \lim_{k\to\infty} \frac{h_{\mathscr{L}}(2^k P)}{4^k} \geq 0.$$

Fact. We can define a pairing $\langle P,Q\rangle = \frac{1}{2}\left(\widehat{h}(P+Q) = \widehat{h}(P) - \widehat{h}(Q)\right)$.

- $\langle -,-\rangle$ is bilinear
- $\langle P,P\rangle = \widehat{h}(P)$
- $\widehat{h}(P) = 0 \iff P$ is torsion
- $|\cdot| := \sqrt{\widehat{h}}$ defines a Euclidean norm on $A(\overline{\mathbb{Q}}) \otimes \mathbb{R}$ (positive definite since tensoring with $\mathbb{R}$ kills torsion)

Now assume there's at least one rational point, so we get an immersion $\mathcal{C} \hookrightarrow \operatorname{Jac}(\mathcal{C})$. Note we have a height on $\operatorname{Jac}(\mathcal{C})$ e.g. coming from (an appropriate modification of) the theta divisor. This gives maps

$$\mathcal{C}(F) \hookrightarrow \operatorname{Jac}(\mathcal{C})(F) \to \operatorname{Jac}(\mathcal{C})(F) \otimes \mathbb{R}.$$

Theorem 2.1.8 (**Vojta's inequality**). *There exists constants $c_1, c_2, c_3 > 1$ so that for all $P, Q \in C(\overline{\mathbb{Q}})$ satisfying*

$$|Q| \geq c_2 |P| \quad \textit{and} \quad |P| \geq c_1,$$

one has

$$\langle P, Q \rangle \leq \left(1 - \frac{1}{c_3}\right) |P| \, |Q| \, .$$

Think of this as an improvement on Cauchy-Schwarz.

"This is like breaking the speed of light. Once you improve something that's fundamental to mathematics, you know you have a very strong tool."

Picture 2.1.9. Maybe later I'll come back and draw the picture for this...

For now, you have a ball with finitely many points. Outside of this, cover by cones. Each cone has finitely many points by Vojta (+ Northcott. If there is a point, the heights of all points are bounded in terms of its height). There are only finitely many cones needed by geometry.

Mumford's inequality can be used to improve the bound. Furthermore, c_1 is proportional to $h(\mathrm{Jac}(\mathcal{C}))$ by work of de Diego, Bombieri, Vojta.

Finally, the main result is

Theorem 2.1.10 (Dimitrov, Gao, H.). *$\exists c = c(g, [F : \mathbb{Q}]) > 1$ so that $\#\mathcal{C}(F) \leq c^{1+\mathrm{rank}\, \mathrm{Jac}(\mathcal{C})(F)}$. (Call this (*))*

There's a second version which implies the above

Theorem 2.1.11 (same authors). *$\exists c_1, c_2 = c_1(g), c_2(g) > 1$ so that*

$$h(\mathrm{Jac}(\mathcal{C})) \geq c_1 \implies \#\mathcal{C}(F) \leq c_2^{1+\mathrm{rank}(\ldots)}.$$

- David-Philippon ('07) got (*) for $\mathcal{C} \subset E^g$
- GDH 1 -parameter family of $\mathcal{C}$ (2019)
- Kühne (2021): $c = c(g)$, not $c(g, [F : \mathbb{Q}])$
- Yuan-Zhang: different proof
- Gao-Ge-Kühne: Higher dimensional version on A

Note 2. Distracted so missed comments when he was writing the above

2.1.2 Proof ideas

Fix $g \geq 2$ and some auxilliarly $\ell \geq 3$. Let $\mathbb{M}_g$ be the moduli space of genus g curves with (symplectic) level ℓ structure. Let $\mathfrak{C}_g \to \mathbb{M}_g$ be the universal curve. Similarly let $\mathbb{A}_g$ be the moduli space of PPAV with ℓ-level structure and universal family $\mathcal{A}_g \to \mathbb{A}_g$. Note there's the Torelli morphism $\mathbb{M}_g \to \mathbb{A}_g$ classifying

the universal Jacobian $\mathrm{Jac}(\mathfrak{C}_g/\mathbb{M}_g)$.[1] These fit into a diagram

$$\begin{array}{ccccc} \mathfrak{C}_g \times_{\mathbb{M}_g} \mathfrak{C}_g & \longrightarrow & \mathrm{Jac}(\mathfrak{C}_g/\mathbb{M}_g) & \longrightarrow & \mathcal{A}_g \\ & \searrow & \downarrow & & \downarrow \\ & & \mathbb{M}_g & \longrightarrow & \mathcal{A}_g \end{array}$$

(The top left map is $(P, Q) \mapsto [P - Q]$)

In fact, one needs to consider the map

$$\begin{array}{ccc} \mathfrak{C}_g^{[m+1]} & \longrightarrow & \mathcal{A}_g^{[m]} \\ (P_0, \ldots, P_m) & \longmapsto & (P_1 - P_0, \ldots, P_m - P_0) \end{array}$$

(square exponent denotes fiber power)

Remark 2.1.12. All these spaces are quasi-projective, so we can embed

$$\mathbb{M}_g \hookrightarrow \mathbb{P}^N \text{ and } \mathcal{A}_g \hookrightarrow \mathbb{P}^M \times \mathbb{A}_g.$$

This gives a height $h : \mathbb{M}_g(\overline{\mathbb{Q}}) \to [0, \infty)$ and a fiberwise Néron-Tate height $\widehat{h} : \mathcal{A}_g(\overline{\mathbb{Q}}) \to [0, \infty)$ ∘

Proposition 2.1.13 (DGH). *Let $m = 3g - 2 = \dim \mathbb{M}_g + 1$. There exists constants $c_{3,4}(g) > 0$ and a dense Zariski open $U \subset \mathfrak{C}_g^{[m]}$ so that for all $P = (P_0, \ldots, P_m) \in U(\overline{\mathbb{Q}})$, one has*

$$\sum_{i=1}^{m} \widehat{h}(P_i - P_0) \geq c_3 h(\pi(P)) - c_4,$$

where $\pi : \mathfrak{C}_g \to \mathbb{M}_g$ the projection map (same name for its powers).

Remark 2.1.14. If P is in the diagonal (all P_i the same), then LHS is zero while RHS (may be) positive, so need this U. ∘

Picture 2.1.15. Say $|P_0|^2 \leq c_1 =: R^2$. If $h(\pi(P)) \gg 0$ (compared to c_4), we'll have

$$\max \widehat{h}(P_i - P_0) \geq \frac{c_3}{2m} h(\pi(P)).$$

Consider also $r := \sqrt{\frac{c_3}{2m} h(\pi(P))}$ (so each ball of radius r has $\leq m$ points). Note $R = \sqrt{c_1} \ll \sqrt{h(\mathrm{Jac}\, \mathfrak{C})}$. Note $h(\mathrm{Jac}\, \mathfrak{C}) \ll_g h(\pi(P))$, so $R/r \ll_g 1$. Some sphere packing tells us that we can cover a ball of radius R using a number of balls of radius r which is roughly $c_6^{1+\mathrm{rank}\, \mathrm{Jac}(F)}$. This combined with the Vojta-style bound on large points let's one conclude.

To get a height lower bound, need a nonzero global section of a line bundle. One way to do this is to show that the line bundle is big (so a power has a nonzero global section)

2.2 Ziyang Gao: Uniformity for the Number of Rational Points on a Curve (II)

(joint w/ V. Dimitrov and P. Habegger)

[1] This is finite, but not an immersion because of level structures

All curves smooth, geometrically irreducible, and projective.

Theorem 2.2.1 (Dimitrov-G-Habegger)**.** *Let C/F be a curve over a number field F of genus $g = g(C) \geq 2$. Then, $\#C(F) \leq c(g, [F:\mathbb{Q}])^{1+\operatorname{rank} \operatorname{Jac}(C)(F)}$.*

Their proof is based on Vojta's method. Prior to their result

- Mazur asked whether or not a result of the above form could be obtained in '86 and/or '00
- David-Phillipono ('07) proved it if $C \subset E^g$ is contained in a power of an elliptic curve, as well as for certain families (with Nakayamye, spelling?)
- Levent Alpöge has some results on the average number of points on genus 2 curves

  Above 3 all based on Vojta's approach
- Stoll, Katz-Rabinoff-Zurieck-Brown gave a proof if $\operatorname{rank} J(C)(F) \leq g-3$, using Chabauty-Coleman

  This bound is usually sharper when it applies

Let C/F be some curve with Jacobian $J = \operatorname{Jac}(C)$. Let L by a symmetric very ample line bundle on J. This gives a Néron-Tate height $\widehat{h} = \widehat{h}_L : J(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ which is in fact quadratic and positive definite on $J(F) \otimes_{\mathbb{Z}} \mathbb{R}$.

Remark 2.2.2. The map $J(F) \to J(F) \otimes_{\mathbb{Z}} \mathbb{R}$ kills torsion and also $\widehat{h}(P) = 0 \iff P \in J(\overline{\mathbb{Q}})_{tors}$ ∘

Theorem 2.2.3. *There exists $R = R(C) > 1$ s.t. for any $P \neq Q \in C(\overline{\mathbb{Q}})$ with*

$$|Q| \geq |P| \geq R \text{ and } \langle P, Q \rangle \geq \frac{3}{4} |P| \, |Q| \,,$$

one has

- ***(Mumford's inequality)*** $|Q| \geq 2\,|P|$
- ***(Vojta's inequality)*** $|Q| \leq \kappa\,|P|$ *with* $\kappa = \kappa(g) \geq 1$

Together, these tell you that the number of large points in each cone is $\leq \log_2 \kappa + 1$. The number of cones is $\leq 7^{\operatorname{rank} J(F)}$, so you get an upper bound on the number of large points depending only on g and $\operatorname{rank} J(F)$. What about the small points?

Theorem 2.2.4 (DGH+Kühne)**.** *There exists constants $c_1, c_2 > 1$ depending only on g s.t. for each $P \in C(\overline{\mathbb{Q}})$*

$$\# \left\{ Q \in C(\overline{\mathbb{Q}}) : \widehat{h}(Q - P) \leq c_1 \max\{h(J), 1\} \right\} \leq c_2$$

It has been shown that the $R = R(C)$ in the statement of Vojta grows $\ll \max\{h(J), 1\}$. Now, one can cover the ball of radius R by small balls of radius $r = \sqrt{c_1 \max\{h(J), 1\}}$, each having finitely many rational points. The number of such balls is roughly $R/r \ll 1$.

To prove Theorem 2.2.4, we work with universal families, and in particular with the map

$$D_m : \mathfrak{C}_g^{[m+1]} \longrightarrow \mathcal{A}_g^{[m]}$$

from last lecture. Let $X = D_m(\mathfrak{C}_g^{[m+1]}) \subset \mathcal{A}_g^{[m]}$. Key steps

- The notion of "non-degenerate subvarity" (Habegger 2013)
- Show that X is a non-deg subvar of $\mathcal{A}_g^{[m]} \to \mathbb{A}_g$

  Uses a version of Ax-Schanuel
- Prove a height inequality on non-deg subvarities

  Uses a theorem of Siu

2.2.1 Non-degenerate subvars

Look at the power map $[A] \mapsto [A^{[m]}]$ gives a Cartesian square

$$\begin{array}{ccc} \mathcal{A}_g^{[m]} & \longrightarrow & \mathcal{A}_{mg} \\ \downarrow & & \downarrow \\ \mathbb{A}_g & \longrightarrow & \mathbb{A}_{mg}. \end{array}$$

Remark 2.2.5. Let $\mathfrak{H}_g$ be the Siegal upper half space, i.e the set of $g \times g$ symmetric matrices τ with $\mathrm{Im}(\tau) > 0$ (an open in $\mathbb{C}^{\binom{g+1}{2}}$). There is a uniformization $\mathfrak{H}_g \twoheadrightarrow \mathbb{A}_g^{an}$ is the category of complex spaces. This sends $z \in \mathfrak{H}_g$ to the abelian variety $\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$. One can get a similar uniformization

$$\mathbb{C}^g \xrightarrow{u} \mathcal{A}_g^{an}$$

lying over $\mathfrak{H}_g \to \mathbb{A}_g^{an}$. Fixing $\tau \in \mathfrak{H}_g$, one has $u_\tau = (\mathbb{C}^g \to \mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g))$. ∘

Instead of varying the lattice, one can fix a lattice and vary the complex structure. First consider

$$\begin{array}{ccc} \mathbb{R}^{2g} \times \mathfrak{H}_g & \longrightarrow & \mathbb{C}^g \times \mathfrak{H}_g \\ (a, b, \tau) & \longmapsto & (a + \tau b, \tau) \end{array}$$

so the lattice (in the domain) is always $\mathbb{Z}^{2g} \times \mathfrak{H}_g$. In each fiber, the quotient will be $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$ as a real analytic variety; it is only the complex structure which varies. Projecting onto the first factor on the LHS and composing with the inverse of the above isomorphism, one gets the **Betti map**

$$b : \mathbb{C}^g \times \mathfrak{H}_g \longrightarrow \mathbb{R}^{2g}.$$

Note that all fibers of this map are complex analytic. One use of this map is its relation to the Betti form.

Definition 2.2.6 (N. Mok)**.** On $\mathbb{R}^{2g} \times \mathfrak{H}_g$, one has the 2-form $2(\mathrm{d}a)^\tau \wedge \mathrm{d}b$. This becomes a $(1,1)$-form on $\mathbb{C}^g \times \mathfrak{H}_g$ which descends to a form (the **Betti form**) on $\mathcal{A}_g$. One can show that the Betti form ω is semi-positive. Furthermore, if $\widetilde{C} \subset \mathbb{C}^g \times \mathfrak{H}_g$ is a holomorphic curve, then $\omega|_{\widetilde{C}} \equiv 0 \iff \widetilde{C}$ is collapsed to a point by the Betti map.

Fact. $\left[\omega|_{\mathcal{A}_{g,[\tau]}}\right] = c_1(\mathscr{L}_{[\tau]})$ is the class of the polarization.

If $\mathscr{L}$ is the tautological line bundle on $\mathcal{A}_g \to \mathbb{A}_g$, then $[\omega] = c_1(\mathscr{L})$.

Definition 2.2.7. An irreducible subvariety $X \subset \mathcal{A}_g$ is called **non-degenerate** if either of the two equivalent conditions hold

(1) $\omega|_X^{\wedge \dim X} \not\equiv 0$

(2) $\operatorname{rank}_{\mathbb{R}} \left(\mathrm{d}b|_{\widetilde{C}}\right) = 2 \dim X$ (at some point of $\widetilde{X}$), where $\widetilde{X}$ a component of $u^{-1}(X)$.

(2) is more practical for determining whether or not a subvariety is non-degenerate. From **(1)** we can roughly think of non-degenerate as "$\mathscr{L}|_X$ is big."

2.2.2 Construction of non-degenerate subvarities

Observation 2.2.8. If $\dim X > g$, then X is degenerate (rank of Betti map at most $2g = \dim_{\mathbb{R}} \mathbb{R}^{2g}$). Call these naive degenerate subvarities.

Theorem 2.2.9 (G.)**.** *$X \subset \mathcal{A}_g$ is degenerate $\iff$ under suitable assumption, there exists an abelian subscheme $\mathcal{B}$ of $\mathcal{A} \to S$ so that*

$$\begin{array}{ccccc} \mathcal{A} & \xrightarrow{\quad\iota\quad} & \mathcal{A}/\mathcal{B} & \longrightarrow & \mathcal{A}_{g'} \\ \downarrow & & \downarrow & & \downarrow \\ S & = & S & \longrightarrow & \mathbb{A}_{g'} \end{array}$$

$\dim X - \dim \iota(X) > g - g'$. *Above, have*

$$\begin{array}{ccccc} X & \subset & \mathcal{A} & \longrightarrow & \mathcal{A}_g \\ & \searrow & \downarrow & & \downarrow \pi \\ & & S & \longrightarrow & \mathbb{A}_g \\ & & \| & & \\ & & \pi(X) & & \end{array}$$

Application. For all $S \subset \mathbb{M}_g$ irreducible subvariety,

$$S \times_{\mathbb{M}_g} \mathfrak{C}_g^{[m+1]} \longrightarrow \mathcal{A}_g^{[m]} \times_{\mathbb{A}_g} S$$

has non-degenerate image if $m \geq \dim S + 1$.

In general, given $X \subset \mathcal{A} \xrightarrow{\pi} S$ with $\pi(X) = S$, if

(a) $\dim X > \dim S$

(b) X_s generates $\mathcal{A}_s$ for all $s \in S(\overline{\mathbb{Q}})$

(c) $\operatorname{Stab}_{A_{\overline{\eta}}}(X_{\overline{\eta}})$ is finite

then $\forall m \gg 1$ s.t. $X^{[m]}$ is non-degenerate in $\mathcal{A}^{[m]}$ if the modular map restricted to $X^{[m]}$ is quasi-finite.

2.3 Nirvana Coppola: Coleman integrals over number fields

(joint w/ E. Kaya, T. Keller, M. Mmileen, S. Mursass, spelling?)

Motivation comes from the chabauty-coleman method. Say C/K is a "nice" curve (nice = smooth, projective, geometrically integral) over a number field K.

Theorem 2.3.1 (Faltings)**.** *If $g(C) \geq 2$, then $\#C(K) < \infty$*

Theorem 2.3.2 (Chabauty)**.** *If $C/\mathbb{Q}$ is a nice curve of genus g and $J = \mathrm{Jac}(C)$ has rank $r < g$, then $\#C(\mathbb{Q}) < \infty$.*

Idea. Let p be a prime of good reduction. Then we get $C(\mathbb{Q}) \hookrightarrow C(\mathbb{Q}_p) \cap \overline{J}(\mathbb{Q})$ inside $J(\mathbb{Q}_p)$. Coleman integration also gives a map $\log : J(\mathbb{Q}_p) \to \mathbb{Q}_p^g$. In fact, there is a bilinear pairing

$$\begin{array}{ccc} J(\mathbb{Q}) \times \mathrm{H}^0(J, \Omega^1_J) & \longrightarrow & \mathbb{Q}_p \\ (D, \omega) & \longmapsto & \displaystyle\int_D \omega \end{array}$$

giving rise to $\log : J(\mathbb{Q}) \to \mathrm{Hom}(\mathrm{H}^0(J, \Omega^1), \mathbb{Q}_p)$. If $r < g$, then $\exists \omega_J \in \mathrm{H}^0(J, \Omega^1)$ s.t. $\int_D \omega_j = 0$ for all $D \in \overline{J(\mathbb{Q})}$. This has a corresponding $\omega \in \mathrm{H}^0(C, \Omega^1_J)$. Defining

$$\int_P^Q \omega := \int_{[P-Q]} \omega_J \text{ for all } P, Q \in C(\mathbb{Q}),$$

we get that $\int_P^Q \omega = 0$ for all $P, Q \in C(\mathbb{Q}_p)$. Integration against ω_J will have finitely many zeros, so $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.

Let's take a closer look at this finite number of zeros class. Fix a point $Q \in C(\mathbb{Q}_p)$ reducing to $\widetilde{Q} \in \widetilde{C}(\mathbb{F}_p)$. Let

$$D_{\widetilde{Q}} = \left\{ Q' \in C(\mathbb{Q}_p) : Q' \mapsto \widetilde{Q} \right\}.$$

Fix a uniformizer t at Q so that locally $\omega = f \mathrm{d}t$ with $f \in \mathbb{Z}_p[\![t]\!]$. Then,

$$\int_Q^{Q'} \omega = \int_0^{t(Q')} f \mathrm{d}t$$

with the latter integral evaluated formally. This is enough to get the claim about finitely many zeros, but is maybe not enough to compute integrals between points not in the same residue disk. The above sorts of integrals are called **tiny integrals**.

Theorem 2.3.3 (Coleman)**.** *The integral $\int_P^Q \omega$, for $P, Q \in C(\overline{\mathbb{Q}}_p)$ (p good) and $\omega \in \mathrm{H}^0(C, \Omega^1)$ exists and satisfies the following*

- *linear in ω (for fixed P, Q)*
- *additivity at endpoints*
- $\int_{\varphi(P)}^{\varphi(Q)} \omega = \int_P^Q \varphi^* \omega$
- $\int_P^Q \mathrm{d}f = f(Q) - f(P)$

- *Galois-invariance. if $P, Q \in C(\mathbb{Q}_p)$ then $\int_P^Q \omega \in \mathbb{Q}_p$*

Let C^{an} be the analytification of C, and let W be the union of the Weierstrass disks of C (disks consisting of points reducing to a Weierstrass point for $C/\mathbb{F}_p$?). Let $V = C^{\mathrm{an}} \setminus W$. Then, $P, Q \in V(\overline{\mathbb{Q}}_p)$ are called **good points** of C. A Weierstrass point of $C(\overline{\mathbb{Q}}_p)$ is a **very bad point**, and a point in the same residue disk as a very bad point is a **bad point**.

Definition 2.3.4. ω is a form "**of the second kind**" if we can write

$$\omega = \mathrm{d}k + \sum a_i \omega_i,$$

where the ω_i form a basis for $\mathrm{H}^1_{dR}(C)$.

By linearity and FTC, integrating against ω reduces to integrating against each ω_i.

Theorem 2.3.5 (BBK)**.** *There is a function φ for which we can compute $\varphi^* \omega_i = \mathrm{d}h_i + \sum m_{ji} \omega_j$. Furthermore, φ is a Frobenius lift.*

Hence,

$$\int_{\varphi(P)}^{\varphi(Q)} \omega_i = h_i(Q) - h_i(P) + \sum_j m_{ji} \int_P^Q \omega_j.$$

Consequently,

$$\int_P^Q \omega_i = \left(M^t - I\right)^{-1} \left(h_i(Q) - h_i(P) - \int_P^{\varphi(P)} \omega_i - \int_{\varphi(Q)}^Q \omega_i \right) \text{ where } M = (m_{ij}).$$

If $P, \varphi(P)$ and $Q, \varphi(Q)$ are in the same residue disk, then the integrals on the RHS are tiny, and everything above is computable.

φ is defined on the (Monsky-Watsker weak completion, spelling?, of) the coordinate ring of V. Say $C : Q(x, y) = 0$ on V. We map $x \mapsto x^p$ and compute the new y using Hensel's lemma. It turns out the result lives in this completion of the coordinate ring $K[x, y]/Q(x, y)$. This choice of φ indeed leads to tiny integrals on the RHS.

Gonna stop taking notes here...

2.4 Steffen Müller: p-adic Arakelov theory on abelian varieties and quadratic Chabauty

Note 3. Missed initial discussion on history/motivation

Quadratic Chabauty uses p-adic heights, and a general principle says any real-valued heights should give a construction of p-adic heights. We'll discuss a construction using (p-adic valued) metrics on line bundles.

2.4.1 Real-valued metrics and heights

Let v be a place of $\mathbb{Q}$, and let $X/\mathbb{Q}_v$ be a nice variety. Throughout the talk, L will be a line bundle on X.

We want something like a logarithmic height, so we won't introduce a metric, but a log-metric.

Definition 2.4.1. A function $\lambda : L(\mathbb{Q}_v) \to \mathbb{R}$ is a **log-metric** if for all $u \in L(\mathbb{Q}_v)$ and $a \in \mathbb{Q}_v^\times$, we have

$$\lambda(au) = \lambda(u) + \log |a|_v .$$

Actually, u should not be 0 in its fiber, so this metric really leaves on $L^\times$, the total space of the associate $\mathbb{G}_m$-torsor (i.e. L minus the zero section).

(Can define tensor products, pullbacks, and isometrices)

Warning 2.4.2. log-metric has nothing to do with log-geometry

Example. Say $v < \infty$ and $\mathcal{X}/\mathbb{Z}_v$ is a model of X. Let $\mathscr{L} \in \mathrm{Pic}(\mathcal{X})$ be a model of L. Let $x \in X(\mathbb{Q}_v)$ with associated section $\overline{x} \in \mathcal{X}(\mathbb{Z}_v)$. For $u \in L_x^\times(\mathbb{Q}_v)$, we define

$$\lambda_{\mathscr{L}}(u) := \inf_{a \in \mathscr{O}_v^\times} \{\log |a|_v : u \in a \cdot \overline{x}^* \mathscr{L}\} .$$

This gives a "model log-metric" taking values in $\mathbb{Q} \log v$. △

We want to use these to define global heights on jacobians.

Say $X/\mathbb{Q}_v$ is an abelian variety with line bundle L/X. Suppose that L is symmetric (with $n = 4$) or L is antisymmetric (with $n = 2$), so there's an iso $(*) : [2]^* L \simeq L^{\otimes n}$.

Definition 2.4.3. A log-matric λ on L is **good** if (*) is an isometry.

If you rigidify at 0, then $(*)$ is the unique isomorphism of rigidified line bundles. Extends this notion to all L using $L^{\otimes 2} \simeq L_{sym} \otimes L_{anti}$.

Proposition 2.4.4 (Zhang)**.** *There is a unique good log-metric $\widehat{\lambda}$ on L. If $v < \infty$, then* $\mathrm{im}(\widehat{\lambda}) \subset \mathbb{Q} \log v$.

(If you have good reduction, the good log-metric is a model metric using the Néron model. In general, do a sort of Tate trick.)

Let's talk about the global theory. Say $X/\mathbb{Q}$ is a nice variety with line bundle L/X. Consider $\overline{L} = (L, (\lambda_v))$ s.t. for all v, λ_v is a log-metric on $L \otimes \mathbb{Q}_v$ with the compatibility condition that for almost all v, $\lambda_v = \lambda_{\mathscr{L}_v}$ for $\mathscr{L}/\mathbb{Z}$ some model of L. This defines a height

$$\begin{array}{rccc} h_{\overline{L}} : & X(\mathbb{Q}) & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \sum \lambda_v(u) \end{array}$$

for any $u \in L_x^\times(\mathbb{Q})$. The product formula will give u independence. If X is an abelian variety, then $h_{\overline{L}}$ is quadratic.

2.4.2 p-adic log-metrics and heights

Fix a continuous idèle class character $\chi : \mathbb{A}_{\mathbb{Q}}^\times / \mathbb{Q}^\times \longrightarrow \mathbb{Q}_p$. The p component will be $\chi_p = \log_p$ (with $\log_p(p) = 0$). Note $\chi_\infty = 0$ so won't contribute to height.

Say $v < \infty$ a non-arch place. Want a function $L^\times(\mathbb{Q}_v) \to \mathbb{Q}_p$ with $\lambda(au) = \lambda(u) + \chi_v(a)$. In construction of model log-metrics, you set

$$\lambda_{\mathscr{L}}(u) = \inf_{a \in \mathscr{O}_v^\times} \{\log |a|_v : u \in a \cdot \overline{x}^* \mathscr{L}\} \cdot \frac{\chi_v(v)}{\log v} \in \mathbb{Q} \log_p v$$

(not sure if I copied this down correctly).

Good log metric has same definition. If $v \neq p$, use Zhang's construction and it takes values in $\mathbb{Q} \log_p v$. Get global height $h_{\overline{L}} : X(\mathbb{Q}) \to \mathbb{Q}_p$ as sum of local heights as before.

Theorem 2.4.5 (BMS)**.** *Say $X/\mathbb{Q}_p$ an abelian variety with L/X. Then, there exists a good log-metric on L (locally, $\widehat{\lambda}$ is a double integral)*

2.4.3 Quadratic Chabauty

Say $C/\mathbb{Q}$ is a nice curve of genus $g \geq 2$. Fix rational point $b \in C(\mathbb{Q})$ so we get Abel-Jacobi map $i = i_b : C \hookrightarrow J = \mathrm{Jac}(C)$. Assume

(1) $\mathrm{rank}\, J(\mathbb{Q}) = g$

(2) $\mathrm{rank}\, \mathrm{NS}(J) > 1$

(3) p prime s.t. $[J(\mathbb{Q}_p) : \overline{J(\mathbb{Q})}] < \infty$

(2) lets us find some $L \in \mathrm{Pic}(J) \setminus \mathrm{Pic}^0(J)$ s.t. $\iota^* L = \mathscr{O}_C$. Let $\overline{L} = (L, (\lambda_v)_{v<\infty})$ where all λ_v good log-metrics. The assumptions will allow one to show that $h_{\overline{L}} : X(\mathbb{Q}) \to \mathbb{Q}_p$ extends to a locally analytic function $G : J(\mathbb{Q}_p) \to \mathbb{Q}_p$. If $x \in C(\mathbb{Q})$, then

$$h_{\overline{L}}(\iota(x)) = h_{\iota^* \overline{L}}(x) = \sum \underbrace{\iota^* \lambda_v \circ 1}_{\mu_v : C(\mathbb{Q}_v) \to \mathbb{Q}_p} (x),$$

so have a nice local decomposition.

Theorem 2.4.6 (BMS)**.** *Let $F = G \circ \iota - \mu_p : C(\mathbb{Q}_p) \to \mathbb{Q}_p$. This maps $C(\mathbb{Q})$ into a computable finite set, and it has finite fibers.*

Proof sketch. $x \in C(\mathbb{Q}) \implies F(x) = \sum_{v \neq p} \mu_v(x)$ and we don't have enough time to say more... ■

2.5 Stevan Gajović: Symmetric Chabauty for cubic points on certain modular curves

(joint w/ Josha Box and Pip Goodman)

Let X be a nice curve defined over $\mathbb{Q}$ of genus g (or g_X). Let $X^{(d)} := X^d / S_d$ be the dth symmetric power of X, its $\mathbb{Q}$-points are $\mathbb{Q}$-rational effective degree d divisors. If $X^{(d)}(\mathbb{Q})$ is finite, knowing $X^{(d)}(\mathbb{Q})$ lets one know all points $X(L)$ for all degree d extensions $L/\mathbb{Q}$.

People study symmetric powers of modular curves e.g. to

(1) extend Mazur's results on classifying potential torsion subgroups and isogenies of elliptic curves over $\mathbb{Q}$ to number fields

(2) Extending modularity statements from $\mathbb{Q}$ to number fields

2.5.1 Symmetric Chabauty

Let p be a pirme of good reduction for curve X. Let $\widetilde{Q} \in X^{(d)}(\mathbb{F}_p)$. Its inverse image under the reduction map is denoted $D(\widetilde{Q}) \subset X^{(d)}(\mathbb{Q}_p)$ and called a **residue class** of $\widetilde{Q}$. Let $J(X)$ be the Jacobian of rank r. Assume there is some $Q \in X^{(d)}(\mathbb{Q})$ to get map $X^{(d)} \to J$.

If $r + d \leq g$, we hope that $X^{(d)}(\mathbb{Q})$ has finitely many points (in each residue class?). When $d = 1$, classic Chabauty shows that $\iota(D(\widetilde{P})) \cap \overline{J(X)(\mathbb{Q})}$ is finite and determinable.

Warning 2.5.1. If $d \geq 2$, $\iota(D(\widetilde{P})) \cap \overline{J(X)(\mathbb{Q})}$ might not be finite, even if $d + r \leq g$

Example. If $\rho : X \to \mathbb{P}^1$ is hyperelliptic, get $\rho^*(x_0) = (x, \sqrt{f(x_0)}) + (x_0, -\sqrt{f(x_0)})$ for any $x_0 \in \mathbb{P}^1(\mathbb{Q})$, so $X^{(2)}(\mathbb{Q})$ always infinite. In general, if you have a morphism $X \to \mathbb{P}^1$ or $X \to E$ of degree at most d (and rank $E \geq 1$), then $X^{(d)}(\mathbb{Q})$ is infinite. △

Definition 2.5.2. An **isolated point** $P \in X^{(d)}(\mathbb{Q})$ is one not coming from previous maps, and such that...

Theorem 2.5.3. *Only finitely many isolated points (missed the hypotheses)*

Slides too fast for me...

3 Day 3

3.1 Isabel Vogt: Obstructions to rationality of conic bundle threefolds

(joint w/ Sarah Frey, Lina Ji, Soumya Sankar, and Bianca Viray)

Let k be an arbitrary field with char $\neq 2$ and Galois group $G_k = \mathrm{Gal}(\overline{k}/k^P)$

We want to talk about rationality of conic bundle threefolds. Let's start with a reminder on a more familiar case.

3.1.1 Conics

Say X a smooth conic.

Theorem 3.1.1. $X \cong \mathbb{P}^1 \iff X(k) \neq \emptyset$

(for the reverse direction, $\mathscr{O}_X(P)$ induces an isomorphism $X \xrightarrow{\sim} \mathbb{P}^1$. Equivalently, embed the conic in $\mathbb{P}^2$ and stereographically project away from a point onto a line)

Definition 3.1.2. A variety X/k is **rational** if there exists a birational map $X \overset{\sim}{\dashrightarrow} \mathbb{P}^N_k$ for some N.

(a dense open in X is isomorphic to a dense open in projective space)

Remark 3.1.3. Any smooth projective curve birational to $\mathbb{P}^1$ is isomorphic to $\mathbb{P}^1$. ∘

Two features to note from the conic story

- There's an obstruction to rationality (existence of rational point)
- A construction if obstructions vanish (get an isomorphism to $\mathbb{P}^1$ when there is a rational point)

3.1.2 Conic Bundles

Definition 3.1.4. A **conic bundle** $\pi : X \to B$ is a fibration with generic fiber a smooth conic. Also require X smooth and B smooth, geometrically connected, and projective.

Let $\Delta \subset B$ be the locus above which the fibers are not smooth.

Question 3.1.5 (Motivating Question)**.** *When is a conic bundle rational?*

- If $\dim B = 0$, X is a conic, so rational $\iff X(k) \neq \emptyset$
- $\dim B = 1$. For X to be rational, B must be a unirational curve, so $B \simeq \mathbb{P}^1_k$. Say also X is relatively minimal (no (-1)-curves in fibers). Then, X is rational $\iff X(k) \neq \emptyset$ AND $\deg(\Delta) \leq 3$.
- $\dim B = 2$. There are many unirational surfaces, but let's focus on the simplest case in which $B = \mathbb{P}^2_k$.

  There is a étale double cover $\widetilde{\Delta} \to \Delta$ parameterizing the components of the bad fibers. In the previous two cases, the rational bundles were also geometrically rational, but that no longer holds here. Here, $X_{\overline{k}}$ is rational iff

  (a) $\deg \Delta \leq 4$; OR

  (b) $\deg \Delta = 5$ and $\widetilde{\Delta}/\Delta$ corresponds to even theta characteristic

  Question: What?

  Lemma 3.1.6 (Prokharov + ε [FJSVV])**.** *If $X(k) \neq \emptyset$ and $\deg(\Delta) \leq 3$, then X is rational.*

  First interesting case is Δ being a smooth plan quartic.

Definition 3.1.7. A **degree 4 conic bundle** is a conic bundle over $\mathbb{P}^2$ where Δ is a smooth plane quartic.

Question 3.1.8. *Do there exist degree 4 conic bundles that are rational/irrational?*

Answer. Yes to rational. If $\widetilde{\Delta}(k) \neq \emptyset$, the degree ≤ 3 argument from above extends to degree ≤ 4.

Yes to irrational. Necessarily, k non-algebraically closed; we'll take $k = \mathbb{R}$.

Construction 3.1.9 (Models of degree 4 conic bundles). We'll give them as double covers of $\mathbb{P}^1_{[t_0:t_1]} \times \mathbb{P}^2_{[u:v:w]}$ ramified over a $(2,2)$-divisor of the form $t_0^2 Q_1 + 2t_0 t_1 Q_2 + t_1^2 Q_3$ (Q_i a quadratic poly). X has natural map $X \to \mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^2$ whose fibers are conics ($X : z^2 = t_0^2 Q_1 + 2t_0 t_1 Q_2 + t_1^2 Q_3$) and whose discriminant locus is $\Delta = V(Q_1 Q_3 - Q_2^2)$ (vanishing of discriminant). X is also a quadric surface bundle over $\mathbb{P}^1$.

Example. Can take e.g.
$Q_1 = -31u^2 + 12uv - 6v^2 + 9uw + 531vw + 25w^2$
$Q_2 = -25u^2 + 120uv + 30v^2 - 31uw + 37vw$
$Q_3 = -8047u^2 + 1092uv - 1446v^2 - 423uw - 375vw - 25w^2$ △

Claim 3.1.10. *$X(\mathbb{R})$ is disconnected ($\implies$ X not rational)*

By [CT-P] this can be detected algebraically using unramified cohomology:

$$\mathrm{H}^4_{nr}(\mathbb{R}(X), \mathbb{Z}/2\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^{\#\text{real connected component}}$$

(unramified cohomology apparently only depends on function field)

Let's understand the real topology of X over $\mathbb{P}^1(\mathbb{R})$. It is locally constant, only changing over the 4 points on the base where the quadric is singular. These 4 points break $\mathbb{P}^1(\mathbb{R})$ into 4 regions where the quadric has signature $(1,3)$, $(0,4)$, $(1,3)$, $(0,4)$. The signature $(1,3)$ part has real points looking like a sphere, while the $(0,4)$ part has no real points. Therefore $X(\mathbb{R})$ disconnected since it lives over a disconnected subset of $\mathbb{P}^1(\mathbb{R})$.

3.1.3 Intermediate Jacobian (torsor) Obstructions

Let's start with the story of intermediate Jacobians (over $\mathbb{C}$) in relation to the story of Jacobians over curves.

- Let C be a curve and X a 3-fold which is rationally connected. Think of $\mathrm{Jac}(C)$ as related to Hodge structures $\mathrm{H}^{1,0} \oplus \mathrm{H}^{0,1}$

  [Clemens-Griffiths] The intermediate Jacobian of X corresponds to the Hodge structure on the middle cohomology

  $$\mathrm{IJ}(X) \longleftrightarrow [0 = \mathrm{H}^{3,0}] \oplus \mathrm{H}^{2,1} \oplus \mathrm{H}^{1,2} \oplus [\mathrm{H}^{0,3} = 0]$$

  with outer pieces vanishing by the rationally connected assumption. Hence just getting some weight one hodge structure.

  Fact.

  $$\mathrm{IJ}(\mathrm{Bl}_C X) \simeq \mathrm{IJ}(X) \times \mathrm{Jac}(C)$$

  when you blowup along a curve $C \subset X$.

  Theorem 3.1.11 (Clemens-Griffths)**.** *$X/\mathbb{C}$ as above rational $\implies$ $\mathrm{IJ}(X) \simeq \prod \mathrm{Jac}(C_i)$ for some curves C_i*

- Now work over an arbitrary field k. The Jacobian is the identity component $\mathrm{Pic}^0_{C/k}$ of the Picard scheme. The component group here is

  $$\mathrm{Pic}_{C/k} \,/\, \mathrm{Pic}^0_{C/k} \simeq \mathrm{NS}^1(C_{\overline{k}}) \xrightarrow[\deg]{\sim} \mathbb{Z}.$$

  This produces torsors $\mathrm{Pic}^d_{C/k}$ for $\mathrm{Pic}^0_{C/k}$.

  Let $X_{\overline{k}}$ is rational. Then (by [Benoist-Wittenberg]) one can look at the codim 2 Chow scheme $\mathrm{CH}^2_{X/k}$. It's identity component is the intermediate Jacobian.

  Theorem 3.1.12 (Benoist-Wittenberg)**.** *X/k is rational $\implies$ $\left(\mathrm{CH}^2_{X/k}\right)^0 \simeq \prod \mathrm{Pic}^0_{C_i/k}$ for some smooth, projective C_i/k*

  The component group here is

  $$\mathrm{CH}^2_{X/k} \,/\, \left(\mathrm{CH}^2_{X/k}\right)^0 \simeq \mathrm{NS}^2(X_{\overline{k}})$$

  For all $\gamma \in \mathrm{NS}^2(X_{\overline{k}})^{G_k}$, get a torsor $(\mathrm{CH}^2_{X/k})^\gamma$.

Theorem 3.1.13 (Benoist-Wittenberg). *Let X/k be rational. For simplicity, assume that $\left(\mathrm{CH}^2_{X/k}\right)^0 \simeq \mathrm{Pic}^0_{C/k}$. Then, for all $\gamma \in \mathrm{NS}^2(X_{\overline{k}})^0$, there is an integer $d = d(\gamma)$ so that*

$$\left(\mathrm{CH}^2_{X/k}\right)^\gamma \simeq \mathrm{Pic}^0_{C/k}\,.$$

Remark 3.1.14 (from audience quesionts). The map $\gamma \mapsto d(\gamma)$ is a group homomorphism. Even when the intermediate Jacobian is the Jacobian of a single curve, NS^2 is not necessarily $\mathbb{Z}$. ∘

Previous results

(Hassett-Tschinkel, Benoist-Wittenberg) Say $X \subset \mathbb{P}^5$ smooth complete intersection of 2 quadrics w/ $X(k) \neq \emptyset$. Then, X is rational $\iff$ IJT obstruction vanishes (i.e. all the componets are Pic^d's). In this case, X will contain a line and projection from the line is the birational map you want.

(Kuznestov-Prokhorav) All Fano 3-folds w/ $\mathrm{Pic}(X_{\overline{k}}) \simeq \mathbb{Z}$ are rational

Theorem 3.1.15 (FJSVV).

(1) *$\exists$ a degree 4 conic bundle over $\mathbb{Q}$ s.t.*

- ***(a)*** *$X(\mathbb{R})$ connected*
- ***(b)*** *$X(\mathbb{Q}) \neq \emptyset$ ($\implies$ unirational over $\mathbb{Q}$)*
- ***(c)*** *X has an IJT obstruction to rationality (even over $\mathbb{R}$)*

(2) *$\exists$ degree 4 conic bundle over $\mathbb{Q}$ s.t.*

- ***(a)*** *IJT obstruction vanishes over $\mathbb{Q}$*
- ***(b)*** *$X(\mathbb{R})$ disconnected ($\implies$ X irrational over $\mathbb{R}$)*

(This is the example from before with the explicit Q_i's)

3.1.4 Proof ideas: compute torsors

Have étale double cover $\varpi : \widetilde{\Delta} \to \Delta$. This doesn't specify the conic bundle, but it's a large piece of it.

Fact (Mumford, Beauville, FJSVV). $\left(\mathrm{CH}^2_{X/k}\right)^0 \simeq \mathrm{Prym}(\widetilde{\Delta}/\Delta) =: P$

In the current situation, this P will be the Jacobian of a curve $P \simeq \mathrm{Pic}^0_{\Gamma/k}$.

Fact. Here, $\Delta = V(Q_1Q_3 - Q_2^2)$ and $\widetilde{\Delta} = V(Q_1 - r^2, Q_3 - s^2, Q_3 - rs)$ and

$$\Gamma : y^2 = -\det\left(t^2M_1 + 2tM_2 + M_3\right)$$

where M_i symmetric matrix corresponding to Q_i.

I'm kinda lost, but for some reason we want to look at the set

$$\left\{[D] \in \mathrm{Pic}^0_{\widetilde{\Delta}} : \varpi_* D \sim \mathscr{O}_\Delta\right\}$$

which has two components $P \cup \widetilde{P}$ (and $\mathscr{O}_{\widetilde{\Delta}} \in P$). You also want to look at the analogous set with $\omega_\Delta = \mathscr{O}_\Delta(1)$ in place of $\mathscr{O}_\Delta$, which again splits as $P^{(1)} \cup \widetilde{P}^{(1)}$. Looks like these components separated by $h^0(D)$ even or odd.

Theorem 3.1.16. *For all* $\Gamma \in \mathrm{NS}^2(X_{\overline{k}})^{G_k}$, $\left(\mathrm{CH}^2_{X/k}\right)^\gamma$ *is isomorphic to one of* $P, \widetilde{P}, \widetilde{P}^{(1)}$, *or* $P^{(1)}$.

Isabel quickly sketched the idea behind the proof, but I didn't follow

Corollary 3.1.17. *IJT obstruction vanishes* $\iff$ $\widetilde{P}(K)$ *or* $\widetilde{P}^{(1)}(k)$ *is nonempty.*

She finished by sketching why part **(2)** of their main result should be (slash is) true, but again, I did not follow

3.2 Bianca Viray: Quadratic points on intersections of quadrics

(joint w/ Brendan Creutz[2])

History. The joint work almost didn't happen. They first talked about collaborating at a conference shortly after they both finished grad school. At this conference, Bianca was being harassed by a more senior member of the community, and so was spending breaks and lunches hiding.

Let $X \subset \mathbb{P}^N$ be a smooth degree d variety over a field k. Then X laways has a point of degree at most d (slicing with a hyperplane), and so $\mathrm{ind}(x) := \gcd_{x \in X}[k(x) : k]$ dividies d (x ranging over closed points).

Question 3.2.1. *Is this the best we can say?*

Answer. In complete generality, yes. e.g. there are cubic curves w/ no point of index smaller than 3

Can we do better in certain families. Consider $X \subset \mathbb{P}^n$ smooth complete intersection of 2 quadrics w/ $\mathrm{char}(k) \neq 2$. $\mathrm{ind}(X)$ will divide 4. Does X have index dividing 2, and if so is there a quadratic (or rational) point?

Theorem 3.2.2 (Springer + Amer-Brumer)**.** *X has index 1* $\iff$ $X(k) \neq \emptyset$

(not true for arbitrary varieites)

Some results (case of archimedean fields left as an exercise) on complete intersection of 2 quadrics in $\mathbb{P}^n$:

- $n \geq 8$: k a p-adic field gives $\mathrm{ind}(X) = 1$ [Demyanov '56] (sharp). k a number field means local-global (LGP) holds [CTSSD '87]
- $n \geq 5$: [CTSSD '87] conjecture LGP holds ($\implies \mathrm{ind}(X) = \mathrm{lcm}_\nu \mathrm{ind}(X_\nu)$)
- $n \geq 7$: k number fields means LGP holds [Heath-Brown '18]
- $n = 3$: All possibilities for the index occur
- $n = 4$: Exists counterexamples to LGP, so $\mathrm{ind}(X) \neq \mathrm{lcm}_\nu \mathrm{ind}(X_v)$.

[2] They first met at one of the rational points conferences

Assumption. For the rest of the talk, assume $n \geq 4$.

Theorem 3.2.3 (Creutz-V.)**.** *Let $n \geq 4$. If k is a local field or number field, then X has index dividing 2.*

(This is false for arbitrary fields. The "smallest" fields which they have index 4 examples have transcendence degree 2. It's open for C_2 fields)

Also looked at the possibility of getting quadratic point.

Definition 3.2.4. Say global field satisfies $(*)$ is...

(hypotheses which are expected to hold do hold, e.g. X a number field satisfying Schnizel's hypothesis)

Theorem 3.2.5 (Cretz-V.)**.** *Let $n \geq 4$. X has a quadratic point if any of the following hold:*

- *k a local field w/* $\mathrm{char}(k) \neq 2$
- *k global function field of* $\mathrm{char}(k) \neq 2$ *and $n \geq 5$*
- *k number fields satisfying $(*)$ and $n \geq 5$*
- *k a global field of* $\mathrm{char}(k) \neq 2$ *satisfying $(*)$, $n = 4$, and*

  every rank 4 quadric containing X that's defined over a quadratic extenion fails to have local points at an even number of places.

  Example. Say $X = V(Q_0, Q_\infty) \subset \mathbb{P}^n$, $n \geq 4$. X smooth implies $t_0 Q_\infty + t_\infty Q_0$ generically rank 5 and is rank ≤ 4 for a reduced degree 5 subscheme $\mathscr{S} \subset \mathbb{P}^1$ (where determinant vanishes) and for these points, rank $= 4$. $\triangle$

  The condition will hold in any of the following cases:

  - *$X(\mathbb{A}_k) \neq$ (fail to have local points at 0 places)*
  - *The degeneracy locus of the pencil is irreducible*
  - *Every rank 4 quadric ontaining X that's defined over a quadratic extension has square discriminant*
  - *many other cases*

3.2.1 Local fields

Theorem 3.2.6 (Spring + Amer, Brumer)**.** *$X(k') \neq \emptyset$ for $[k' : k]$ odd $\implies$ $X(k) \neq \emptyset$*

Very powerful for unramified extensions of local fields!

Get points over finite fields of large degree and so, by Hensel, over unramified field of large odd degree, and so a rational point.

Upshot. If $X \mod \pi$ split over the quadratic exntesion $\mathbb{F}'/F$, then X has a quadratic point.

(I missed what 'split' means)

What is $X \mod \pi$ is never split over $\mathbb{F}'$?

Answer. Use Tian's semistable models of intersections of 2 quadrics. If X never split over $\mathbb{F}'$, then $X \mod \pi$ is a union of 4 planes transitively premuted by $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$. Such models become split over $k(\sqrt{\pi})$.

3.2.2 Global fields

Using local results and LGP for $n \geq 5$ automatically get $\mathrm{ind}(X) = \mathrm{lcm}_v \mathrm{ind}(X_v) \mid 2$.

For $n \geq 4$, counterexamples to LGP exist, so have to use out $2 = \mathrm{lcm}_v \mathrm{ind}(X_v) < \mathrm{ind}(X)$. Instead of looking for quadratic points on X, look for rational points on $\mathrm{Sym}^2 X$.

Assumption. Assume $n = 4$.

Consider $\mathrm{Sym}^2(X) \dashrightarrow \mathrm{Gr}(1,4)$ sending a pair of points (x_1, x_2) to the line $\ell_{x_1,x_2} \subset \mathbb{P}^4$ joining them. Note

$$\ell_{x_1,x_2} \supset V(q_0, q_\infty) \supset \{x_1, x_2\},$$

so q_0, q_∞ linearly independent and hence ℓ_{x_1,x_2} lies on one of the quadrics $t_0 Q_\infty + t_\infty Q_0 =: Q_t$. Hence, image of above rational map lands in

$$\mathscr{G} := \{(\ell, t) : \ell \subset Q_t\} \longrightarrow \mathbb{P}^1.$$

The map $\mathrm{Sym}^2 X \dashrightarrow \mathscr{G}$ is birational, and $\mathscr{G} \to \mathbb{P}^1$ is a fibration of Severi-Brauer threefolds of order (dividing) 2, smooth away from $\mathscr{S}$ (degree 5 subscheme from before).

Theorem 3.2.7 (Breutz-V.)**.** *There exists an adelic* 0*-cycle of degree 1 on* $\mathscr{G}$ *that is orthogonal to* $\mathrm{Br}(\mathscr{G})$*. Furthermore, if 'every rank 4 quadric containing* X *that's defined over a quadratic extension fails to have local points at an even number of places,' then* $\mathscr{G}(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$*.*

Apply the fibration method to this (e.g. [CTSD94]), get that there is a 0-cycle of degree 1 on $\mathscr{G}$ (i.e. $\mathrm{ind}(\mathscr{G}) = 1$) and that under the long hypothesis above + k number field satisfying $(*)$, there is furthermore a k-rational point.

Question 3.2.8. *Can one directly show* $\mathrm{ind}(\mathscr{G}) = 1 \implies \mathscr{G}(k) \neq \emptyset$*?*

$\mathrm{ind}(\mathscr{G}) = 1$ gives a 0-cycle of degree 1.

Remark 3.2.9. Hard to manufacture points out of thing air, so usually people go from 0-cycles to rational points by showing that every 0-cycle of degree 1 is equivalent to a rational point. ∘

Theorem 3.2.10 (CTC '79)**.** *Let* $\mathscr{C} \to \mathbb{P}^1$ *be a conic bundle that is smooth away from a degree 5 subscheme. Then, every 0-cycle of positive degree is rationally equivalent to an effective 0-cycle.*

Corollary 3.2.11. $\mathrm{ind}(\mathscr{C}) = 1 \implies \mathscr{C}(k) \neq \emptyset$ *and every 0-cycle on* $\mathscr{C}$ *is rationally equivalent to a sum of rational points.*

The second part above is false for $\mathscr{G}$, so can't prove it by showing every 0-cycle of degree 1 is equivalent to an effective 0-cycle.

Theorem 3.2.12 (Creutz-Viray)**.** *There is an adelic* 0*-cycle of degree 1 on* $\mathscr{G}$ *that is orthogonal to* $\mathrm{Br}\,\mathscr{G}$*. Furthermore, if 'blah', then* $\mathscr{G}(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$*.*

For any extension F/k, there is a pairing

$$\begin{array}{ccc} \mathscr{G}(\mathbb{A}_k) \times \mathrm{Br}\,\mathscr{G} & \longrightarrow & \prod_v \mathrm{Br}\, k_v \\ ((P_v), \alpha) & \longmapsto & P_v^* \alpha \end{array}$$

Can show this lands in the direct sum and so you get

$$\begin{array}{ccc} \mathscr{G}(\mathbb{A}_k) \times \operatorname{Br}\mathscr{G} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ ((P_v), \alpha) & \longmapsto & \sum_\nu \operatorname{inv}_\nu P_\nu^* \alpha. \end{array}$$

Note $\mathscr{G}(k) \times \operatorname{Br}\mathscr{G} \mapsto 0$. Thus, we define

$$\mathscr{G}(\mathbb{A}_k)^{\mathrm{Br}} := \{(P_v) \in \mathscr{G}(\mathbb{A}_k) : \langle (P_v)_v, \alpha \rangle = 0 \text{ for all } \alpha \in \operatorname{Br}\mathscr{G}\} \supset \mathscr{G}(k).$$

Recall we have $\mathscr{G} \to \mathbb{P}^1$ a Sever-Brauer fibration, smooth away from $\mathscr{S} \subset \mathbb{P}^1$. For every $s \in \mathscr{S}$, $\mathscr{G}_s$ is geometrically reducible with components defined over the extension $k(\sqrt{\varepsilon_s})$ with $\varepsilon_s := \operatorname{disc}(Q_s|_H)$. Get Brauer class when you have a pair of points on s with the same discriminant?

Upshot. Get Brauer classes from $\mathscr{T} \in \operatorname{Sym}^2 \mathscr{S}$ s.t. $\operatorname{disc} Q_{\mathscr{T}} \in \operatorname{im}\left(k^\times/(k^\times)^2 \longrightarrow k(\mathscr{T})^\times/(k(\mathscr{T})^\times)^2\right)$

Proposition 3.2.13 (CV). *There is a $(P_v) \in \mathscr{G}(\mathbb{A}_v)$ s.t. for all $\alpha_{\mathscr{T}}$*

$$\langle (P_v), \alpha_{\mathscr{T}} \rangle = \sum_{t \in \mathscr{T}} \#\left\{w \in \Omega_{k(\mathscr{T})} : Q_{\mathscr{T}}^{sm}(k(\mathscr{T})_w) = \emptyset\right\} \mod 2$$

(compare to condition 'blah')

Proposition 3.2.14 (CV). *If $\mathscr{T} \in \operatorname{Sym}^2 \mathscr{S}(k)$, and above big expression is 1, then $\mathscr{G}(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$.*

Corollary 3.2.15. *$\mathscr{G}(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ if $\operatorname{Br}\mathscr{G}/\operatorname{Br} k$ is*

- *generated by pairs $\tau \in \operatorname{Sym}^2(\mathscr{S}(k))$; or*
- *sum in first of previous two props is always even (condition 'blah' from before)*

4 Day 4

4.1 Carlos Rivera: Persistence of the Brauer-Manin obstruction on cubic surfaces

(joint w/ Bianca Viray)

4.1.1 Index 1 problem

Let X be a variety over a field k, and let $I(X) := \gcd_{x \in P}[k(x) : k]$ be its index. Think of a measure of how far your variety is from having a degree 1 zero-cycle, e.g. $X(k) \neq \emptyset \implies I(X) = 1$.

Question 4.1.1. *When does $I(X) = 1 \implies X(k) \neq \emptyset$?*

This does not hold in general, but does in certain cases

- quadrics (Springer, 1952)
- Torsors of abelian varieties

- Severi Brauer varieties

  (for previous two, use inflation-restriction sequences in cohomology?)

- Some principal homogeneous spaces under connected, reductive linear algebraic groups

Conjecture 4.1.2 (Cassesls and Swinnerton-Dyer)**.** *Let k be a field and $f(x_0, \ldots, x_n)$ a form of degree 3. If f has a nontrivial zero over an extension L/k of degree prime to 3, then it has a nontrivial zero on k.*

In other words, if $X \subset \mathbb{P}^n_k$ is a cubic hypersurface, we expect $I(X) = 1 \implies X(k) \neq \emptyset$.

Theorem 4.1.3 (Coray, 1974)**.**

- *Conecture holds over local fields*
- *Let k be a perfect field. Any smooth cubic surface $X \subset \mathbb{P}^3_k$ with $I(X) = 1$ has a closed point of degree 1,4, or 10.*

(Sounds like perfect field hypothesis later removed)

Coray's descent argument: start with a degree d point P coprime to 3. Find curves of low genus on X passing through P and a point of degree 3 on X (exists by intersecting with hyperplane). Using Riemann-Roch, get effective zero cycles of degree lower than d.

Question 4.1.4 (45 year old open question)**.** *Can we eliminate 4,10? both?*

Remark 4.1.5. Any counterexample to (CS), the conjecture by Cassels-Swinnerton-Dyer, over global fields would need to fail the local global principle ∘

Conjecture 4.1.6 (CT-Sansuc, 1980)**.** *For a smooth cubic surface X over a global field k, $\overline{X(k)} = X(\mathbb{A}_k)^{\mathrm{Br}}$*

(presumably closure inside $X(\mathbb{A}_k)$)

Theorem 4.1.7 (R.-Viray, 2021)**.** *Let X be a smooth cubic surface over a global field k. If L/k is an extension with degree coprime to 3, then*

$$X(\mathbb{A}_L)^{\mathrm{Br}} = \emptyset \iff X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset.$$

4.1.2 Proof idea

Say $X(\mathbb{A}_k)^{\mathrm{Br}}$ is empty. By Coray's result for local fields, $X(\mathbb{A}_L) \neq \emptyset$ implies $X(\mathbb{A}_k) \neq \emptyset$, so we are reduced to the case in which X is everywhere locally soluble over k (sum of degrees over local extensions adds up to $[L : k]$ which is coprime to 3, so some local extension has degree coprime to 3).

Lemma 4.1.8 (CT-Poonen, 2000)**.**

- *Let X be a smooth cubic surface in $\mathbb{P}^3$ over a global field k s.t. $X(\mathbb{A}_k) \neq \emptyset$. If $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$, there exists an $\alpha \in \mathrm{Br}(X)[3]$ s.t. $X(\mathbb{A}_k)^{\alpha} = \emptyset$*
- *Let X be a smooth cubic surface in $\mathbb{P}^3$ over a local field F s.t. $X(F) \neq \emptyset$. Then, for each $\alpha \in \mathrm{Br}(X)$, the image of the evaluation map $\mathrm{ev}_\alpha : X(F) \to \mathrm{Br}(F)$ is a group coset.*

Fix $\alpha \in \mathrm{Br}(X)[3]$ as in the first bullet point. The image of $\mathrm{ev}_\alpha : X(F) \to \mathbb{Q}/\mathbb{Z}$ can only have size 1 or 3 (subset of $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$ which is a coset). Since $X(\mathbb{A}_k) \neq \emptyset$, we know

$$X(\mathbb{A}_k)^\alpha = \emptyset \implies \text{each } \mathrm{ev}_{\alpha_{k_v}} : X(k_v) \to \mathbb{Q}/\mathbb{Z} \text{ is not surjective}$$

so each evaluation map is constant. For $(P_v) \in X(\mathbb{A}_k) \subset X(\mathbb{A}_L)$, we have $(3 \nmid [L:k])$

$$\sum_w \mathrm{inv}_w(\mathrm{ev}_{\alpha_{L_w}}(P_v)) = [L:k] \sum_v \mathrm{inv}_v(\mathrm{ev}_\alpha(P_v)) \neq 0.$$

As element of the Brauer-Manin set will need to come from $X(\mathbb{A}_L)$, not $X(\mathbb{A}_k)$. Reduced to below local statement.

Proposition 4.1.9 (R.-Viray, 2021)**.** *Let X be a smooth cubic surface over a local field k with $X(k) \neq \emptyset$ and let $\alpha \in \mathrm{Br}\, X[3]$. If $\mathrm{ev}_\alpha : X(k) \to \mathrm{Br}\, k$ is constant, then for all finite extensions L/k, $\mathrm{ev}_{\alpha_L} : X(L) \to \mathrm{Br}\, L$ is constant.*

One possible approach is to understand $\mathrm{CH}_0(X_k)$. If $\mathrm{CH}_0(X_k)$ is generated by classes of k-rational points (e.g. true if there's good reduction), then the constant evaluation persists. Since α is 3-torsion, it suffices for $2\,\mathrm{CH}_0(X_k)$ to be generated by classes of k-rational points.

Colliot-Thélène improvement of Coray's argument. Using tools like large fields, R-density properties, and refined Bertini theorems, he was able to prove analogues of Coray's theorem on other del pezzo surfaces, and obtain new results for cubic surfaces.

Theorem 4.1.10 (CT, 2020)**.** *Let k be a char 0 field, and let $X \subset \mathbb{P}^3_k$ be a smooth cubic surface. If $X(k) \neq \emptyset$, then the group $\mathrm{CH}_0(X)$ is generated by classes of points of degrees 1 or 3*

Corollary 4.1.11 ((CT,2020) + ε(-,Viray))**.** *Let k be an infinite field, and let $X \subset \mathbb{P}^3_k$ be a smooth cubic surface. If $X(k) \neq \emptyset$, then the group $2\mathrm{Ch}_0(X)$ is generated by classes of k-rational points.*

Proof. Start w/ a degree 3 point P on X.

- Blow up X at two generic k-rational points R and S, different from Q. Let $\pi : Y \to X$ be the blowup map.

If I heard correctly, at some point Carlos said cubic surfaces w/ a k-rational point are unirational

Carlos explained more things in words, but I did not follow... ■

4.2 Andreas-Stephan Elsenhans: Point Counting on K3 surfaces

(joint w/ J. Jahnel)

Remark 4.2.1. Start w/ a couple of diagrams plotting

$$\frac{p+1-\#E(\mathbb{F}_p)}{\sqrt{p}}$$

for a couple of elliptic curves E. ∘

Let's relate this to chomology

Theorem 4.2.2 (Lefschetz trace)**.** *Let V be an n-dimensional proper variety over $\mathbb{Q}$ w/ good reduction at p. Then,*

$$\#V(\mathbb{F}_p) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\left(\operatorname{Frob}_p \mid \mathrm{H}^i_{\acute{e}t}(V_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)\right)$$

Also included stated of Weil conjectures, but slides are fast...

Definition 4.2.3. A **K3 Surface** is a simply connected algebraic surface having trivial canonical bundle. They have a 22-dimensional vector space of 2-dimensional cycles.

Recall 4.2.4. Every elliptic curve has a Weierstrass equation

K3 surfaces have a few different models

- degree 2 model: double cover of $\mathbb{P}^2$, ramified at a sextic curve
- degree 4 model: quartic in $\mathbb{P}^3$
- degree 6 model: complete intersection of quadric and cubic in $\mathbb{P}^4$
- degree 8 model: complete intersection of three quadrics in $\mathbb{P}^5$

As long as models have at worse ADE-singularities, the desingularization will still be a K3 surface

Note 4. Wrote down 6 explicit equations as double covers of $\mathbb{P}^2$ (ramified over union of 6 lines in general position, e.g. $W^2 = XYZ(X+Y+Z)(3X+5Y+7Z)(-5X+11Y-2Z)$

Proposition 4.2.5. *For the double cover $S' : w^2 = f_6(x,y,z)$ and an odd prime p, we have*

$$\#C'(\mathbb{F}_p) = 1 + p + p^2 + C_p \mod p,$$

where C_p the coefficient of $(XYZ)^{p-1}$ of $f_6^{(p-1)/2}$

Remark 4.2.6. David Harvey worked on meothods to compute $(C_p \mod p)_p$ and similar sequences as fast as possible. ∘

Corollary 4.2.7. *The Deligne-Weil theorem implies*

$$\left|\#S'_i(\mathbb{F}_p) - (p^2+p+1)\right| \leq 6p$$

for the singular models $S'_1, \ldots, S'_6$ written earlier (but not written in these notes. Oops)

Suffices to determine $\#S'_i(\mathbb{F}_p)$ modulo some integer $> 12p$. In fact, combining with mod p counts, suffices to determine it mod 16.

Gonna stop taking notes, because I can't type fast enough to also follow what's going on while I do it...

4.3 Ulrich Derenthal: Integral points on singular del Pezzo surfaces

(joint w/ Florian Wilsch)

Cubic surfaces are del Pezzo surfaces. Ulrich showed images of Clebsch's smooth cubic surface (27 real lines), including one where the rational points of bounded height were dotted in.

We want to talk about certain singular del Pezzo surfaces, e.g. an intersection of two quadrics in $\mathbb{P}^4$ such as

$$X = \left\{x_0^2 + x_0x_3 + x_2x_4 = x_1x_3 - x_2^2 = 0\right\} \subset \mathbb{P}^4_{\mathbb{Q}}.$$

This is a singular quartic del Pezzo (dP) w/ 3 lines

$$L_1 = \{x_0 = x_2 = x_3 = 0\}, \ L_2 = \{x_0 = x_1 = x_2 = 0\}, \text{ and } L_3 = \{x_1 + x_3 = x_1 = x_2 = 0\}.$$

This has 2 singularities $Q_1 = (0, 1, 0, 0, 0)$ and $Q_2 = (0, 0, 0, 0, 1)$ coming from computing partial derivatives.

Conjecture 4.3.1 (**Manin's Conjecture**). *Let X be a del Pezzo (w/ at wrose ADE singularities) with $X(\mathbb{Q}) \neq \emptyset$. Let V be the complement of the lines in X. Then,*

$$N_{V,H}(B) = \#\{x \in V(\mathbb{Q}) : H(x) \leq B\} \sim cB(\log B)^{\rho-1}$$

where ρ is the rank of the Picard group and H is an anti-canonical height function.

Theorem 4.3.2 (D. '05). *Above holds (with explicit c) for some (any?) rank 6 del Pezzo.*

(Unclear which surface(s) he proved this for. Maybe the X from above?)

Let's spend a bit of time thinking about integral points.

- $\mathbb{P}^2(\mathbb{Z}) = \mathbb{P}^2(\mathbb{Q})$
- $\mathbb{A}^2(\mathbb{Z}) = \mathbb{Z}^2$

  This is because $\mathbb{A}^2 = \mathbb{P}^2 \setminus \{x + 0 = 0\}$, so $(x_0 : x_1 : x_2)$ integral $\iff$ $x_0 \neq 0$ and in fact $x_0 \not\equiv 0 \pmod{p}$ for all p, so $x_0 \in \mathbb{Z}^\times$. So $(x_0 : x_1 : x_2)$ integral $\iff$ it has the form $(1 : x_1 : x_2)$ with $x_1, x_2 \in \mathbb{Z}$. Furthermore, $H(1 : x_1 : x_2) = \max\{1, |x_1|, |x_2|\}$. Note $N_{\mathbb{A}^2,H}(B) \sim 4B^2$.

Let $\mathcal{X}$ be an integral model of X, so $\mathcal{X} \subset \mathbb{P}^4_{\mathbb{Z}}$. Choose a boundary, e.g. $Z = \{Q_2\} = \{(0, 0, 0, 0, 1)\}$. Let $U = X \setminus Z$ with integral model $\mathcal{U} = \mathcal{X} \setminus \overline{Z}$. Then,

$$\mathcal{U}(\mathbb{Z}) = \{(x_0, \ldots, x_4) \in X(\mathbb{Q}) : \gcd(x_0, \ldots, x_3) = 1\}$$

(not singularity modulo any prime). A reasonable choice of height function here is

$$H(\underline{x}) = \max\{|x_0|, \ldots, |x_3|\}.$$

Theorem 4.3.3 (D.-Wilsch '21).

$$N_{\mathcal{U},V,H}(B) := \#\{x \in \mathcal{U}(\mathbb{Z}) \cap V(\mathbb{Q}) : H(\underline{x}) \leq B\} \sim \frac{1}{32} \prod_p \left(1 - \frac{1}{p}\right)^3 \left(1 + \frac{3}{p}\right) B(\log B)^4.$$

Similarly for $Z = \{Q_1\}, \{Q_1, Q_2\}, L_1, L_2, L_3$. The exponent, among other things, differs.

Manin's conjecture for rational points is known for

- complete intersections w/ $\dim X \geq (\deg X - 1)2^{\deg X} - 1$: using circle method
- certain classes of spherical varieties, equivariant compactifications of vector groups: using harmonic analysis on adelic points
- many del Pezzo surfaces, some higher-dimensional examples: mostly using universal torsors

Analogue for integral points is known for

- ... using circle method
- ... using haramonic analysis on adelic points
- ... using universal torsors

Note 5. I'm getting lost...

There's an integral version of Manin's conjecture that was written down, and is due to CL-T

Also definition of (graded) **Cox ring**

$$\operatorname{Cox} \widetilde{X} = \bigoplus_{\operatorname{Pic} X} \mathrm{H}^0(X, \mathscr{O}(D)).$$

Somehow knowing this is useful for counting points?

4.4 Maarten Derickx: Explicit descent using étale morhphisms between modular curves

(joint w/ Barinder Banwait)

Throughout the talk K is number field of degree d.

Definition 4.4.1. A rational prime p is an **isogeny prime** for K if there exists a k-rational degree p isogeny $\varphi : E \to E'$. It is a **torsion prime** for K is there is an elliptic curve E/K with $\#E(K)[p] > 1$

Note every torsion prime is an isogeny prime.

Theorem 4.4.2 (Mazur, '77 and '78)**.** $\operatorname{TorsPrimes}(\mathbb{Q}) = \{2, 3, 5, 7\}$ *and*
$\operatorname{IsogPrimes}(\mathbb{Q}) = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$.

Theorem 4.4.3 (Momose, '95)**.** *If $[K : \mathbb{Q}] = 2$ and K is not imaginary quadratic of class number 1, then there are only finitely many K-isogeny primes.*

(CM gives infinitely many isogenies over Hilbert class fields of imaginary quadratic fields)

Theorem 4.4.4 (Uniform Boundedness, Merel '96 + Oesterl'́9?)**.** $\max \operatorname{TorsionPrimes}(K) < \left(3^{d/2} + 1\right)^2$

If GRH holds and K does not contain the Hilbert class field an imaginary quadratic field, then

Theorem 4.4.5 (Momose '95, David '12, Larson-Vaintrob '14)**.** *The number of K-isogeny primes is finite, and there is a bound in terms of effectively computable constants.*

- $\max(\text{IsogPrimes}(\mathbb{Q}(\sqrt{5}))) \leq 5.65 \times 10^{126}$ (Banwait)

Theorem 4.4.6 (Banwait in deg 2, Bainait-D. in deg >2)**.** *There is an algorithm which computes a superset of* $\text{IsogPrimes}(K)$ *which sometimes allows one to compute* $\text{IsogPrimes}(K)$*, i.e.*

- $\text{IsogPrimes}(\mathbb{Q}(\sqrt{5})) = \text{IsogPrimes}(\mathbb{Q}) \cup \{23, 47\}$
- $\text{IsogPrimes}(\mathbb{Q}(\zeta_7 + \overline{\zeta}_7)) = \text{IsogPrimes}(\mathbb{Q})$

(still assuming GRH, used for good effective Chebotarev density bounds)

4.4.1 Reformulation of Momose's approach in terms of descent

Notation 4.4.7.

- Let Ω_K denote the set of places of K
- p a rational prime
- C/K a nice curve, smooth over $\mathscr{O}_K[1/p]$
- $H \subset \text{Aut}_K C$ with $H \cong \mathbb{Z}/m\mathbb{Z}$ cyclic of order prime to p (i.e. $p \nmid m$)
- $D := C/H$ and assume $f : C \to D$ étale over $\mathscr{O}_K[1/p]$
- $$\text{Sel}_C(K, H) := \left\{\tau \in \text{H}^1(K, H) \mid C^\tau(K_\mathfrak{q}) \neq \emptyset \text{ for all } \mathfrak{q} \in \Omega_K\right\} \subset \text{H}^1(\mathscr{O}_K[1/p], H).$$

Theorem 4.4.8 (Descent)**.**

$$D(K) = \bigsqcup_{\tau \in \text{Sel}_C(K,H)} f^\tau(C^\tau(K))$$

Example. Let $H_p = \mu_{12}(\mathbb{Z}/p\mathbb{Z}) \subset (\mathbb{Z}/p\mathbb{Z})^\times$ denote the 12th roots of unity. $(\mathbb{Z}/p\mathbb{Z})^\times$ acts on $X_1(p)$ through diamond operators (multiply order p point by element of $(\mathbb{Z}/p\mathbb{Z})^\times$), so can define $X_h(p) := X_1(p)/H_p$.

The map $f : X_h(p) \to X_0(p) \cong X_h(p)/((\mathbb{Z}/p\mathbb{Z})^\times/H_p)$ is étale over $\mathbb{Z}[1/p]$, so it is possible to use descent w.r.t. f to study $X_0(p)(K)$. △

Theorem 4.4.9 (Banwait-D., based on Momose)**.** *Suppose that K does not contain the hilbert class field of an imaginary quadratic field, then for $p \gg_K 0$:*

$$\text{Sel}_{X_h(p)}(K, (\mathbb{Z}/p\mathbb{Z})^\times/H_p) = \{1\} \text{ or } \left\{1, \chi_p^{(p+1)/4}\right\}.$$

If either $p \equiv 1 \mod 4$ or GRH holds, then $\left\{1, \chi_p^{(p+1)/4}\right\}$ does not occur.

(χ_p the cyclotomic character)

Corollary 4.4.10 (Momose '95 + Merel '96 + ε(Larson & Vaintrob '14))**.** *Assume GRH and that K does not contain the hilbert class field of an imaginary quadratic field, then* $\text{IsogPrimes}(K)$ *is finite.*

(use uniform boundedness, $X_1(p)$ has no points of degree 12d for $p \gg_d 0$)

4.4.2 Uniform bounds

Let K be a number field, $\varphi : E \to E'$ a degree p isogeny over K, and $G := \ker \varphi \subset E[p]$.

Definition 4.4.11. We define the **isogeny character**

$$\lambda_\varphi : \mathrm{Gal}(K) \to \mathrm{Aut}_{grp}\, G(\overline{K}) = \mathbb{F}_p^\times,$$

the isogeny character of φ. An isogeny prime p for K is called **p-unramified** if there exists a degree p isogeny whose character is unramified at all primes $\mathfrak{p} \mid \mathscr{O}_K p$.

We set $\mathrm{IsogPrimes}_{p\text{-unr}}(d) := \bigcup_{[K:\mathbb{Q}]=d} \mathrm{IsogPrimes}_{p\text{-unr}}(K)$.

Theorem 4.4.12 (Banwait - D.)**.** $\mathrm{IsogPrimes}_{p\text{-}unr}(d)$ *is finite for all integers* d

Since $\mathrm{TorsPrimes}(d) \subset \mathrm{IsogPrimes}_{p\text{-unr}}(d)$ (Galois action is trivial when map comes from quotienting by a degree p point), this generalizes uniform boundedness for torsion.

In terms of class field theory

- $\mathcal{I}_K^{(p)}$: fractional ideals of K coprime to p
- $\mathcal{R}_K^{(p)} \subset \mathcal{I}_K^{(p)}$: principal fractional ideals coprime to p
- $\mathrm{Hom}\left(\mathcal{I}_K^{(p)}, \mathbb{Z}/m\mathbb{Z}\right) \leftrightarrow \mathrm{H}^1(\mathscr{O}_K[1/p], \mathbb{Z}/m\mathbb{Z}) \subset \mathrm{Hom}(\mathrm{Gal}(K), \mathbb{Z}/m\mathbb{Z})$ by CFT
  (trivial Galois action above)
- Let L be the normal closure of K and let $\varepsilon = \sum_{\sigma \in \mathrm{Hom}(K,L)} a_\sigma \cdot \sigma$ w/ $a_\sigma \in \mathbb{Z}$. The **twisted norm** is

$$\begin{array}{rccc} N_\varepsilon : & K & \longrightarrow & L \\ & \alpha & \longmapsto & \displaystyle\prod_\sigma \sigma(\alpha)^{a_\sigma} \end{array}$$

  Lemma 4.4.13. *If* $p \nmid m$ *and* $\mu \in \mathrm{Hom}\left(\mathcal{I}_K^{(p)}, \mathbb{Z}/m\mathbb{Z}\right)$*, then every prime* $\mathfrak{p} \mid p\mathscr{O}_L$*, there exists* ε *and* $\iota : \mathbb{Z}/m\mathbb{Z} \hookrightarrow \mathbb{F}_\mathfrak{p}^\times$ *s.t. for all* $(\alpha) \in \mathcal{R}_K^{(p)}$*:*

$$\iota \circ \mu((\alpha)) \equiv N_\varepsilon(\alpha) \mod \mathfrak{p}.$$

- $\varphi : E \to E'$ a K-rational isogeny of degree p
- $x = (E, \varphi) \in X_0(p)(K)$
- $\eta_\varphi \in \mathrm{H}^1(\mathscr{O}_K[1/p], (\mathbb{Z}/p\mathbb{Z})^\times / H_p)$, the pullback of $f : X_h(p) \to X_0(p)$ along x
- $\mu_\varphi \in \mathrm{Hom}\left(\mathcal{I}_K^{(p)}, (\mathbb{Z}/p\mathbb{Z})^\times / H_p\right)$ correspond to η_φ
- $\iota_p : (\mathbb{Z}/p\mathbb{Z})^\times / H_p \to (\mathbb{Z}/p\mathbb{Z})^\times$ via $s \mapsto s^{12}$

  Proposition 4.4.14. $\lambda_\varphi^{12} = \iota_p \circ \mu_\varphi$ *and one can take* $\iota = \iota_p$ *and* $\varepsilon = \sum_\sigma a_\sigma \sigma$ *w/* $a_\sigma \in \{0, 4, 6, 8, 12\}$ *in earlier lemma.*

- Out of time...

4.5 Filip Najman: Quadratic points on bielliptic modular curves

(joint w/ Borna Vukorepa)

Question 4.5.1 (Motivating)**.** *What are the possible degrees of isogenies of non-CM elliptic curves over quadratic fields?*

Theorem 4.5.2 (Mazur '78)**.** *Let p be a prime. Then, $X_0(p)$ has a non-cuspidal rational point if and only if $p \in \{2, 3, 5, 7, 11, \dots\}$ (missed set cause I'm slow)*

(Later someone expanded theorem to composite levels)

The degree d points on $X_0(n)$, for all n, are not known for any $d > 1$. So current goal is results towards $d = 2$. Unlike in the case of $X_1(p)$, there are noncuspidal quadratic points on $X_0(p)$ for infinitely many p coming from CM elliptic curves. Even the problem of finding all n s.t. $X_0^+(n)(\mathbb{Q})$ contains points that are neither CM nor cusps is open. The set of such n has been conjectured to be finite by Elkies.

The quadratic CM points on $X_0(n)$ are known for all n. To find the (non-CM) quadratic points on $X_0(n)$ for all n, one has to

(1) Find an upper bound m such that for $n \geq m$, $X_0(n)$ has only cusps and CM points over all quadratic fields. This is currently not known.

(2) Determine the quadratic points on $X_0(n)$ for small n, ...

4.5.1 Hyperelliptic curves

$X : y^2 = f(x)$ a hyperelliptic curve with $f : X \to \mathbb{P}^1$ the hyperelliptic map. It has infinitely many quadratic points of the form $(x, \sqrt{f(x)})$ for $x \in \mathbb{Q}$. The reamining quadratic points are called **exceptional**. For almost all hyperelliptic $X_0(n)$, the hyperelliptic involustion ι iw w_d for some $d \mid n$ (sending E to d-isogenious curve). The non-rational obvious points satisfy $\iota(P) = \sigma(P)$, so it folloes that E is d-isogenous to E^σ. A **$\mathbb{Q}$-curve** is an EC isogenous to all of its Galois conjecates, so all obvious points correspond to $\mathbb{Q}$-curves.

missed something

Theorem 4.5.3 (Bruin, N. '15)**.** *Determined the quadratic points on all hyperelliptic $X_0(N)$ such that $J_0(n) := J(X_0(n))$ has rank 0 over $\mathbb{Q}$.*

Furthere results obtained by Ozman, Siksek (2019) and Box (2022?).

4.5.2 Bielliptic curves

A curve X has infinitely many quadratic points if there exists a map $X \to C$ of degree 2 where $C(\mathbb{Q})$ is infinite. This holds if $C \simeq \mathbb{P}^1$ or C an elliptic curve w/ positive rank.

Abramovich and Harris showed that the converse is also true: these are the only possible cases when X w/ $g(X) \geq 2$ can have infinitely many quadratic points.

Theorem 4.5.4 (Bars '99)**.** *Determined all the values of n for which $X_0(n)$ is bielliptic*

Question 4.5.5 (Mazur, '21)**.** *Can we describe all the quadratic points on all the remaining bielliptic curves?*

The reamining n are 60,69,83,92,95,119,62,79,89,94,101,131

N.-Vukorepa (202?): solved all these cases. All exeptional points are CM in these cases. Do this using 2 approaches

- Looking at the moduli interpretation and reducing the problem to rational points on several modular curves
- The Box-Siksek method, a combination of the Mordell-Weil sieve and relative symmetric Chabauty, with modifications

Looking at the moduli interpretation of quotients solves $n = 62, 69, 92, 94$. Take $n = 94$. Bruin and N. showed that all quadratic points on $X_0(47)$ are non-exceptional and correspond to $\mathbb{Q}$-curves of degree 47. As any elliptic curve w/ a subgroup of order 94 also has one of order 47, all quadratic points on $X_0(94)$ also correspond to degree 47 $\mathbb{Q}$-curves.

Want to take advantage of this, and ask to which modular curves do $\mathbb{Q}$-curves of degree 47 w/ a subgroup of order 2 correspond...

(Stopped taking notes)

4.6 Ari Shnidman: Sums of two cubes

(joint w/ L. Alpoge and M. Bhargava)

Theorem 4.6.1 (ABS)**.** *At least $\frac{1}{6}$ of all integers n are not the sum of two rational cubes*

(the truth should be exactly 1/2)

Before this, even showing a positive proportion was open. Conjecturally, 0% should be a sum of two integer cubes.

$x^3 + y^3 = n$ is an elliptic curve, birational (biholomorphic?) to $E_n : y^2 = x^3 - 432n^2$. Now, n is a sum of two rational cubes $\iff$ $\operatorname{rank} E_n$ is positive (except maybe $n = 1, 2$). The real theorem is about cubic twist families of elliptic curves.

Theorem 4.6.2. *Fix an integer $d \neq 0$ (e.g. $d = -432$). Reset notation and let*

$$E_n : y^2 = x^3 + dn^2.$$

Then,

- *The root number $\varepsilon(E_n)$ is equidistributed*
- $\operatorname{avg}_n \#\operatorname{Sel}_2(E_n) = 3$

  Moreover, if you restrict n to those with fixed root number (± 1), then the average is still 3.

Think of root number as being a locally constant function on the adeles. This is literally true if you restrict to squarefree numbers

To get the previous theorem from this, you really need to be able to average over a fixed root number (else e.g. could be 50% 2-Selmer rank 1 and 50% 2-Selmer rank 2).

Corollary 4.6.3. *Fix d, and define*

$$\mu_* := \liminf_{x \to \infty} \frac{\#\{n < X : \operatorname{rank} E_n = *\}}{\#\{n < X\}}$$

(a) $\mu_0 = 1/6$

(b) *Assuming the 2-converse conjecture, one gets* $\mu_1 \geq 5/12$.

Proof. Use the 2-parity conjecture (which is actually a theorem now) that says parity of root number is parity of 2-Selmer rank. ■

Conjecture 4.6.4 (**2-converse conjecture**). *For* $E/\mathbb{Q}$ *with* $E[2](\mathbb{Q}) = 0$, $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/\mathbb{Q}) = 1 \implies \mathrm{rank}\, E = 1$

Don't Wei-Yun have some result like this for function fields?

(would follow from BSD or even just from finiteness of Ш)

Remark 4.6.5. There's a p-converse conjecture for every p, and is known for many cases. ∘

Theorem 4.6.6 (in progress, ABS-Durungale (spelling?)). *At lest* $1/12$ *of* n *are a sum of 2 cubes*

(Sounds like they should be able to get as much as $5/12$ like this)

Remark 4.6.7. Average 3-Selmer in this family is ∞. 5-Selmer could help, but probably still wouldn't get to $1/2$. ∘

Remark 4.6.8. 0% of integers are representable by an irreducible binary cubic form, apparently ∘

Proof combines geometry-of-numbers and circle methods.

4.6.1 Bhargava-Ho hypercubes

(See paper by Bhargava and Ho)

Let F be any field. They give a bijection

$$\left\{(C, L, P) : C \text{ genus } 1, L \in \mathrm{Pic}^2(C), P \in \mathrm{Jac}(C)[3](F)\right\}_{/\simeq} \longleftrightarrow G(F)\backslash V(F)^{\text{non-deg}}$$

where $G = \mathrm{GL}_2^2$ and $V = F^2 \otimes \mathrm{Sym}^3(F^2)$ (pairs of binary cubic forms).

Example. Note $V \subset (F^2)^{\otimes 4} \simeq \mathrm{End}(F^2 \otimes F^2)$ (imagine 4-dimensional hypercube w/ elements of F at each vertex?) Given some a in here, get

$$\mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3 \xrightarrow{a^*} \mathbb{P}^3 \simeq \mathbb{P}\,\mathrm{Mat}_2(F)$$

The intersection C of $\mathbb{P}^1 \times \mathbb{P}^1$ and locus of matrices w/ zero determinant is the corresponding genus 1 curve. It will be a $(2,2)$-curve in $\mathbb{P}^1 \times \mathbb{P}^1$, so it comes w/ two degree 2 line bundles. It comes w/ more actually; get 4 independent line bundles of degree 2. Consider $P_i = L_i \otimes L_i^{-1} \in \mathrm{Jac}(C)(F)$; these have relation $P_1 + P_2 + P_3 = 0$. If $a \in F^2 \otimes \mathrm{Sym}^3 F_2$, then in fact $P_1 = P_2 = P_3 =: P$, so P is 3-torsion. △

Let $\widetilde{G} = \mathrm{SL}_2^2/\mu_2$ (group action by G factors through this), so $\widetilde{G} \curvearrowright V$. There are two invariants b_2, b_6 of degrees $2, 6$. If you have an element in $G(F)\backslash V(F)$, it's Jacobian will be the elliptic curve $E : y^2 + b_2xy + b_6y = x^3$ with $(0,0)$ the point of order 3. Set $b_2 = 0$ to get quadric $X \subset V$ (which is $\widetilde{G}$-invariant). Rewriting into short weierstrass form, looking at elliptic curve

$$y^2 = x^3 + 16b_6^2.$$

This is the sort of family we saw in the beginning ($d = 16$ and $n = b_6$. Such a curve will have a rational 3-torsion point (if and?) only if d is a square).

Let $L_n = \mathscr{O}_{E_n}(2\infty)$ and let

$$\theta(L_n) = \left\{(P, s) : P \in E_n[2], s : L_n \xrightarrow{\sim} t_P^* L_n\right\}$$

be the theta group. This sits in an exact sequence

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \theta(L_n) \longrightarrow E_n[2] \longrightarrow 0.$$

Keep in mind the sequence

$$\mathrm{H}^1(\mathbb{Q}, \theta(L_n)) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E_n[2]) \longrightarrow \mathrm{H}^2(\mathbb{Q}, \mathbb{G}_m)$$

and the $\mathrm{Sel}_2(E_n)$ lands in $\mathrm{H}^1(\mathbb{Q}, \theta(L_n))$. This H^1 of the theta group gives isoclasses of genus 1 curves (whose Jacobian is E_n) equipped w/ a degree 2 line bundle. This is furthermore $\widetilde{G}(\mathbb{Q})\backslash X(\mathbb{Q})_n$. The image of the Selmer group there lands in the space of orbits that have integral representatives. So now you're interested in counting lattice points in this region (apparently, Levent did some general work on this in his thesis).

Idea. Quadratic twisting does not change the θ group. All these cubic twist families are quadratic twists away from each other, so you want to reduce everything to this square d case.

5 Day 5 (4/1)

5.1 Abbey Bourdon: Towards a classification of sporadic j-invariants

These are the j-invariants of elliptic curves which give rise to sproadic/isolated points on modular curves.

Definition 5.1.1. Let C/K be a nice curve over a number field. A closed point $x \in C$ of degree d is sporadic if C has only finitely many points of degree $\leq d$.

Example. Any $\mathbb{Q}$-point on a curve of genus ≥ 2 is sporadic. △

Example (Debarre/Klassen ('94))**.** $n \geq 7$, $F_n : X^n + Y^n + Z^n/\mathbb{Q}$. There are only finitely many points of degree $\leq n - 2$. △

Definition 5.1.2. More generally, we say x is an **isolated point** if for

$$\Phi : C^{(d)} \longrightarrow \mathrm{Jac}(C),$$

there is no other point $y \in C^{(d)}(K)$ w/ $\Phi(x) = \Phi(y)$,[3] and there is no positive rank abelian variety $A \subset \mathrm{Jac}(C)$ s.t. $\Phi(x) + A \subset \mathrm{im}(\Phi)$.[4]

(both definitions so far as in paper by BELOV; conventions differ)

[3] If so, these would give a function with divisor $x - y$ which would give an infinite family of points including x

[4] This would given another infinite family of degree d points, parameterized by A, including x

Example. $X_0(28) : y^2 = x^8 + 14x^4 + 1$ with hyperelliptic map $f : X_0(28) \to \mathbb{P}^1, (x, y) \mapsto x$. This gives an infinite family of degree 2 points coming from $\mathbb{P}^1$ (preimages of rational points). Bruin/Najman (2013) found the points $(\pm\sqrt{-1}, 4), (\pm\sqrt{-1}, -4)$ not coming from the $\mathbb{P}^1$. These points are isolated, but not sporadic. Note $J_0(28)$ has rank 0. △

Remark 5.1.3. Say $g \geq 2$. Then,

$$C(K) \subset \{\text{sporadic points}\} \subset \{\text{isolated points}\}.$$

All 3 of these sets are finite. ∘

5.1.1 Sporadic/isolated points on $X_0(N)$,$X_1(N)$

Let's first mention some applications

(1) Classifying torsion subgroups of elliptic curves over all number fields of a fixed degree d

Such a classification is known for $d \leq 3$ (the $d = 3$ case came out in 2020, due to Derickx, Etropolsic (spelling?), van Hoeij, Morrow, Zureick-Brown)

For $d = 4$, we know the torsion subgroups that occur infinitely often

Open Question 5.1.4. *Are there any sporadic points of degree* 4 *on* $X_1(N)$*?*

(2) Characterizing quadratic points on $X_0(N)$

Open Question 5.1.5 (Mazur,...)**.** *Does* $X_0(N)$ *have no non-cuspidal, non-CM quadratic points for* N *sufficiently large?*

Remark 5.1.6. There are infinitely many quadratic points only if you have a degree 2 map to $\mathbb{P}^1$ or to a positive rank elliptic curve. ∘

Fact. We know which modular curves are hyperelliptic or bielliptic. For $N > 131$, any quadratic point is sporadic.

Remark 5.1.7. A quadratic point on $X_0(N)$ for $N \gg 0$ gives a sporadic point on $X_1(N)$ ∘

(3) Serre's uniformity conjecture

Conjecture 5.1.8 (**Serre uniformity**)**.** *There exists a constant*[5] C *s.t. for all non-CM elliptic curves* $E/\mathbb{Q}$*, the mod* ℓ *Galois representation of* E *is surjective for primes* $\ell > C$

(Technically, Serre asked this as a question, but did not conjecture it)

Remark 5.1.9. Say $p > 37$ prime and $E/\mathbb{Q}$ has $\rho_{E,p}$ not surjective. Work of many people then shows that $\operatorname{im} \rho_{E,p} \subset \mathrm{GL}_2(\mathbb{F}_p)$ is contained in $C_{ns}^+(p)$ the normalizer of the non-split Cartan. One can then show that there exists an elliptic curve E' in the $\overline{\mathbb{Q}}$-isogeny class of E which gives a sporadic point on $X_1(p^2)$ for sufficiently large[6] p (see e.g. B.-Najman, 2021). ∘

[5] It's believed $C = 37$ should work

[6] For every p, you get a point in $X_1(p^2)$. If $p \gg 0$, it will be sporadic

5.1.2 Sporadic j-invariants

Definition 5.1.10. Say $j \in X(1) \simeq \mathbb{P}^1$ is a **sporadic j-invariant** (resp. **isolated j-invariant**) if it is the image of some sporadic (resp. isolated) point on $X_1(n)$ for some $n \geq 1$.

(If I heard correct, a recent phd at Wesleyan wrote a thesis studying sporadic points on $X_0(n)$)

Example. $E : 126b1$ (LMFDB label) gives rise to a degree 3 sporadic point on $X_1(21)$ (Nojman, 2012). Hence, $j(E) = -3^2 \cdot 5^6/2^3$ is a sporadic j-invariant (note rational j-invariant, but degree 3 sporadic point). △

Theorem 5.1.11 (B., Ejcher, Liu, Odumodu, Viray 2019 = BELOV)**.** *Suppose Serre's uniformity conjecture holds. Then, there are only finitely many isolated j-invariants valued in $\mathbb{Q}$.*

Example (some isolated j-invariants)**.** $-3^2 \cdot 5^6/2^3, -7 \cdot 11^3$, all 13 CM j-invariants in $\mathbb{Q}$ △

(Apparently $X_0(13)$ has a non-modular automorphism sending a rational cusp to a sporadic (non-cuspidal) point)

Theorem 5.1.12 (B., Gill, Rouse, Watson '20)**.** *The only non-CM j-invariants in $\mathbb{Q}$ corresponding to an isolated point of odd degree on $X_1(N)$ (for any N) are*

$$-3^2 \cdot 5^6/2^3, 3^3 \cdot 13/2^2.$$

(the second comes from a degree 9 point on $X_1(28)$ which is isolated but not sporadic)

Open Question 5.1.13.

- *Know **Serre curves**/$\mathbb{Q}$ do not give rise to sporadic points[7] on $X_1(N)$. Can they give rise to isolated points?*

  Need only consider $X_1(24)$ due to arguments in BELOV '19

- *Isolated points coming from elliptic curve w/ a non-trivial p-isogeny/$\mathbb{Q}$.*[8]

  Apparently, the Galois reps of such curves are surjective for $p \gg 0$ (by Lemos?)

Transitioning to $\mathbb{Q}$-curves

Definition 5.1.14. A **$\mathbb{Q}$-curve** is an elliptic curve which is isogenous (over $\overline{\mathbb{Q}}$) to its Galois-conjugates

Example.

- CM elliptic curves are $\mathbb{Q}$-curves
- rational elliptic curves are $\mathbb{Q}$-curves
- Any elliptic curve w/ $j(E) \in \mathbb{Q}$ is a $\mathbb{Q}$-curve
- Anything isogenous (over $\overline{\mathbb{Q}}$) to the above is a $\mathbb{Q}$-curve
- There are more examples... △

Remark 5.1.15. $\mathbb{Q}$-curves are exactly the elliptic curves over number fields that are modular (quotients of $J_1(N)$)

Ribet proved this in 2004, assuming a conjecture of Serre which was later proven in 2009 (by Khare, Witenberger). ∘

I feel like I'm missing something. Is this true?

For this talk, think of $\mathbb{Q}$-curves as a generalization of elliptic curves w/ rational j-invariant.

Recall 5.1.16. Serre's uniformity conjecture $\overset{\text{BELOV}}{\Longrightarrow}$ only finitely many sporadic j-invariants in $\mathbb{Q}$.

Question 5.1.17. *Are there only finitely many non-CM $\mathbb{Q}$-curves giving rise to sporadic points (of any degree) on $X_1(N)$ (for any $N \geq 1$).*

Remark 5.1.18. There are infinitely many CM elliptic curves, and they all give rise to a sporadic point. ∘

Remark 5.1.19. An affirmative answer to the above question would imply Serre's uniformity conjecture (B., Najman). In fact, it's much stronger than what you would need to get Serre uniformity. ∘

Theorem 5.1.20 (B., Najman 2021)**.** *Suppose all non-CM $\mathbb{Q}$-curves giving rise to a sporadic point on $X_1(p^2)$ (for any prime p) lie in only finitely many $\overline{\mathbb{Q}}$-isogeny classes. Then, Serre's uniformity conjecture holds.*

Proof Sketch. Say $E/\mathbb{Q}$ is an elliptic curve w/ $\operatorname{im}\rho_{E,p} \leq C_{\text{ns}}^+(p)$. Note this is a group of size $2(p^2-1)$, so E has full p-torsion in an extension of this degree. This gives two independent p isogenies, so there will be an elliptic curve E' in E's $\overline{\mathbb{Q}}$-isogeny class with a p^2 isogeny. Now E' is a $\mathbb{Q}$-curve giving a point on $X_1(p^2)$ of degree $\leq 2p(p^2-1)$. This will be sporadic if $p \gg 0$. ■

Theorem 5.1.21 (B., Najman 2021)**.** *All non-CM $\mathbb{Q}$-curves giving rise to a sporadic point of odd degree on $X_1(N)$ for some $N \geq 1$ lie in the $\overline{\mathbb{Q}}$-isogeny class of the elliptic curve w/ j-invariant $-3^2 \cdot 5^6/2^3$.*

Let's finish by saying something about the connection to rational points.

Say $x \in X_1(N)$ is a sporadic point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve. One can show that $N = 2^a p^b$ with $p \in \{3, 5, 7, 11, 13\}$ or E is $\overline{\mathbb{Q}}$-isogenous to the elliptic curve w/ j-invariant $-3^2 \cdot 5^6/2^3$.

Example. Say $x \in X_1(54)$ ($54 = 2 \cdot 3^3$) sporadic of odd degree (assuming $j(x) \in \mathbb{Q}$). Have a degree 3 map $f : X_1(54) \to X_1(27)$. If $\deg(x) = 3\deg(f(x))$, then $f(x)$ is sporadic (BELOV). However, $f(x)$ cannot be sporadic by work of Rouse, Sutherland, Zureick-Brown (2021), so $\deg(x) = \deg(f(x))$ (can't have $\deg(x) = 2\deg(f(x))$ since $\deg(x)$ is odd). This implies there's a model $E/\mathbb{Q}$ for x so that $\mathbb{Q}(E[2]) \subset \mathbb{Q}(E[27])$. There is a modular curve for this! You can show it has no non-cuspidal rational points, so this case can't happen. △

5.2 Michael Stoll: Rational points on and BSD for a curve of genus 4

Long ago, on this very day, before Wiles, someone spread a rumor that Noam Elkies found a counterexample to FLT.

Let C be the closure in $\mathbb{P}^1 \times \mathbb{P}^1$ of

$$a^3b^2 + a^2b^3 - a^3b - ab^3 - a^2b - ab^2 + a^2 + 2ab + b^2 - a - b = 0$$

[7] Elliptic curves w/ adelic Galois representation as large as possible

[8] This will put you in a similar situation to the one in the BGRW '20 paper

This is a smooth projective curve of type $(3,3)$ and genus 4.

This came up in connection to arithmetic dynamics. It classifies numbers z such that there are c, c' s.t. z has period 3 under $f_c : x \mapsto x^2 + c$ and $f_{c'}(z)$ (but not z) has period 3 under $f_{c'}$

Knowing $C(\mathbb{Q})$ (and assuming "Poonen's conjecture") leads to a complete and explicit description of

$$\mathbb{Q} \ni z \mapsto \#\{c \in \mathbb{Q} : z \text{ is preperiodic under } f_c\} \in \mathbb{Z}_{\geq 0}.$$

Theorem 5.2.1. $C(\mathbb{Q}) = \{0, 1, \infty\} \times \{0, 1, \infty\} \in \mathbb{P}^1 \times \mathbb{P}^1$

The rest of the talk was going through the computational proof in Magma

6 List of Marginal Comments

Index