

Course Notes Template

Niven Achenjang

April 24, 2022

These are my course notes for “Class name” at School name. Each lecture will get its own “chapter.” These notes are live-texed or whatever, so there will likely to be some (but hopefully not too much) content missing from me typing more slowly than one lectures. They also, of course, reflect my understanding (or lack thereof) of the material, so they are far from perfect.¹ Finally, they contain many typos, but ideally not enough to distract from the mathematics. With all that taken care of, enjoy and happy mathing.

The instructor for this class is Prof name, and the course website can be found by clicking this link. Extra extra read all about it

Contents

1	Jordan Ellenberg (University of Wisconsin) and David Zureick-Brown (Emory University): Rational points: what’s new, what’s next	1
1.1	Ellenberg (6/14)	1
1.2	David Zureick-Brown (6/15)	3
1.2.1	Function Fields	5
1.3	DZB (6/16)	6
1.3.1	Stacky Bat-Man	6
1.4	Ellenberg (6/17): Examples and Problems	9
2	Jennifer Balakrishnan (Boston University): Chabauty–Coleman and Chabauty–Kim experiments	12
2.1	(2/14)	12
2.1.1	Working with higher genus curves	12
2.1.2	Strategy for computing rational points on curves	13
2.1.3	p -adic Line integration	14
3	List of Marginal Comments	15
	Index	16

List of Figures

¹In particular, if things seem confused/false at any point, this is me being confused, not the speaker

List of Tables

1 Jordan Ellenberg (University of Wisconsin) and David Zureick-Brown (Emory University): Rational points: what's new, what's next

1.1 Ellenberg (6/14)

Note 1. I was 10 minutes late. Whoops...

In the middle of quickly introducing discriminants of number fields.

Theorem 1.1 (Hermite). *There are only finitely many number fields L/\mathbb{Q} of degree d w/ $|D_{L/\mathbb{Q}}| < X$.*

This means the discriminant gives us a way to order number fields. How does one prove this theorem?

Proof Sketch. The primitive element theorem let's us write $L = \mathbb{Q}(\alpha)$ for some algebraic integer α , whose minimal polynomial is of the form

$$x^d + a_1x^{d-1} + \cdots + a_d,$$

where $a_i \in \mathbb{Z}$ is the i th symmetric polynomial of α and its Galois conjugates. Hermite shows that one can choose such an α with all $|\alpha|$ (archimedean absolute values) bounded, and thus all $|a_i|$ bounded, in terms of $|D_{L/\mathbb{Q}}|$.

Why can you do this? Use Minkowski's theorem. The point is that $|D_{L/\mathbb{Q}}|$ controls the covolume of the integer lattice $\mathcal{O}_L \hookrightarrow L \otimes_{\mathbb{Q}} \mathbb{R}$. Can use Minkowski's theorem to show that a lattice with bounded covolume has a vector in a small box (i.e. with all coordinates bounded).

Now, there are only finitely many possible values for $a_i \in \mathbb{Z}$ (since $|a_i|$ bounded), so there are only finitely many number fields with $|D_{L/\mathbb{Q}}| < X$. ■

We see that every number field of disc $< X$ is generated by a root of some $P(x) \in \mathbb{Z}[x]$ with coefficients bounded in terms of X .

Notation 1.2. Say $N_d(X, \mathbb{Q}) = \#$ number fields of degree d with $|D| < X$.

Hermite shows that $N_d(X, \mathbb{Q}) \ll X^{\frac{d+2}{4}}$. This is expected to be non-optimal.

Conjecture 1.3 (Folklore). $N_d(X, \mathbb{Q}) \sim c_d X$

There's a more refined conjecture due to Bhargava; he predicts the value of c_d if we restrict to extensions with Galois group S_d .

What's known?

- When $d = 2$, we're counting quadratic extensions, so $L/\mathbb{Q} = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$ and $D_{L/\mathbb{Q}}$ is roughly D (restrict to D squarefree). Hence, this amounts to counting square-free integers. The conjecture in this case is equivalent to

$$\#\text{squarefree integers in } [-X, X] \sim cX$$

This is true!

- For $d = 3$, this is due to Davenport-Heilbronn (1970)

- For $d = 4, 5$, this is due to Bhargava.
- $d = 6$ is still open, and proving this would be a big deal (not just incremental progress). There's a “fundamental wall” between $d = 5$ and $d = 6$.

How about upper bounds?

- E.-Venkatesh (2006): $N_d(X, \mathbb{Q}) < C_d X^{e^{c' \sqrt{\log d}}}$. Note that this exponent is smaller than any power of d , but is also bigger than 1.
- Couvaignes (spelling?) (2019): upper bound of order $X^{c \log^3 n}$
- Lemke-Oliver-Thorne (2020): $X^{c \log^2 n}$.

The approaches here are, in some sense, is based on Hermite. To see the connection, let's re-express Hermite's approach.

Start with an affine space V with an action of a finite group G (e.g. $G = S_d$).² Then we have a map $(V/G)(\mathbb{Q}) \rightarrow \{G\text{-extensions of } \mathbb{Q}\}$. This is given by $P \mapsto [\text{field of definition of } \pi^{-1}(P)]$.

Note 2. Is this talk the same as his ‘What's up in Arithmetic Statistics talk?’ in the Number Theory Web Seminar?

Strategy

- Show that every G -extension of $|\text{disc}| < X$ arises from a point of $(V/G)(\mathbb{Z})$ with height $< c(X)$.
- Count points on $V/G(\mathbb{Z})$ of height at most $c(X)$.

Example. In Hermite's case, $V = \mathbb{A}^d$ with S_d acting by permuting coordinates. In this case \mathbb{A}^d/S_d is again an affine space, whose coordinates are symmetric polynomials.

Note 3. Got distracted and missed the rest of the Hermite stuff. Whoops.

The basis idea of E-V (06) is to change the choice of V .

Example. Say $V = (\mathbb{A}^d)^r$ with S_d acting diagonally. It's less well-known, but equally classic, that the (‘multisymmetric’) functions on V/S_d are well understood. One counts points on it by choose N multisymmetric functions, i.e. a map

$$V/S_d \rightarrow \mathbb{A}^N,$$

(which will preserve low height points), and then counting points on \mathbb{A}^N . You need to have enough functions to make this map injective (or at least for it to have finite fibers). EV showed $N \sim 2^{2r}d$ works. Couvaignes made it work with $N \sim r^2d$. LO-Thorne got it down to $N \sim rd$ which is basically optimal ($\dim V = rd$).

Is there a way to count \mathbb{Z} -points on (V/G) more effectively than embedding in an affine space?

Let's end with a few points of philosophy.

²Need some assumptions of the action. Say the G -action is faithful

- Why guess $\sim cX^1$ (Malle’s conjecture)?

Think about the case of degree d extensions of $\mathbb{F}_q(t)$. These are the same things as degree d covers $C \xrightarrow{d} \mathbb{P}_{\mathbb{F}_q}^1$. These are the \mathbb{F}_q -rational points of a moduli space, called a Hurwitz space. In this case, $|\text{disc}| = q^n$ is (roughly?) saying cover has n branch points. The Hurwitz space of covers w/ n branch points and degree d has dimension n , so one guesses that it has q^n points over \mathbb{F}_q . This is very unjustified but often correctish. See e.g. E-V-Westerland for an example. Also see Lipnowski-Tsimerman (2018) for an example where this heuristic fails.

- Beyond discriminant: shapes of number fields

Let L/\mathbb{Q} be a number field. Then, \mathcal{O}_L is a lattice (it has a bilinear form $\langle \alpha, \beta \rangle = \text{Tr}(\alpha\beta)$) with covolume $\sim |D_{L/\mathbb{Q}}|$. What can we say about the ‘shape’ of this lattice in the space of all lattices? Is it equidistributed? This was worked out for $d = 3$ by Terr in PhD thesis, and for $d = 4, 5$ by Bhargava-H. in 2016. There’s some recent results for specific Galois groups by Harron, Harron-H, ... Also a 2019 paper by Marhilla-Soler, River-Guvea. They (this last paper?) show e.g. that for totally real $\#$ fields, shape is a complete invariant (can’t have two totally real number fields with isometric lattices).

Does this shape actually matter? Are we just adding invariants for no good reason? There was a conjecture by Rubests (spelling?) (c.a. 2000?) that $N_3(X; \mathbb{Q}) = c_3 X - c' X^{5/6} + o(X^{5/6})$. This was proved by Bhargava-Shanker-Tsimerman, by Tanisuchi-Thorne, and separately by Zhao (in function field case). The key idea is to separate cubic fields by shape, and the “missing $X^{5/6}$ ” are lattices so skew that they can’t occur.

What does any of this have to do with rational points?

Remark 1.4. A G -extension of a field K is a K -rational point on the classifying stack BG .

So this question of counting G -extension *is* a question of counting rational points.

Note that a vector bundle on BG is a representation V of G . The total space of the vector bundle/representation V is V/G . Let’s now rephrase Hermite’s strategy in the language of stacks:

To count points on a stack \mathcal{X} (“eeks”), choose a suitable vector bundle \mathcal{V} on \mathcal{X} with total space $\mathcal{Y} \rightarrow \mathcal{X}$, and then...

- (1) Show that every low-height point on \mathcal{X} comes from a low-height point on \mathcal{Y} (“wee”)
- (2) Count low-height points on \mathcal{Y} .

This is the same strategy (“method of the universal torsor”) often used for counting low-height points on schemes.

There’s still one thing missing from this unification.

Question 1.5. *What is a low-height point on a stack?*

1.2 David Zureick-Brown (6/15)

Today we want to talk about the Batyrev-Manin conjecture. Tomorrow we’ll see how this is similar to Malle’s conjecture.

Conjecture 1.6 (Lang-Vojta (spelling?)). *Say X is a variety of **general type** (i.e. K_X big³). Then*

³e.g. ample

$X(\mathbb{Q})$ is not dense in X .

Example. The Fermat surfaces $x^n + y^n = z^n + w^n$ (for $n \geq 5$) are of general type. Conjecturally, in this case, the only rational points are the ‘obvious’ ones (e.g. $(x, y) = (z, w)$). This is not known to hold for any n .

Remark 1.7. If X is rational (i.e. birational to \mathbb{P}^n) or **Fano** (i.e. $-K_X$ ample), then $X(\mathbb{Q}) \subset X(K)$ is dense.

Question:
What is K ?

Conjecture 1.8 (Batyrev-Manin). *Let X/\mathbb{Q} satisfy $X(\mathbb{Q})$ is dense. Consider some embedding $\varphi : X \hookrightarrow \mathbb{P}^N$ and let $\mathcal{L} = \varphi^{-1}\mathcal{O}(1)$. Pick an open $U \subset X$, and form the counting function*

$$N_{U, \mathcal{L}}(B) := \# \{P \in U(\mathbb{Q}) : \text{ht}(P) \leq B\}.$$

The conjecture is that $N_{U, \mathcal{L}}(B) \sim cB^a \log^b B$ for some a, b, c .

The formula for c is due to Perre.

Definition 1.9. Given $P = [x_0 : \dots : x_N] \in \mathbb{P}^n(\mathbb{Q})$ (written in reduced form). Then, the naive height of P is $\text{ht}(P) = \max\{|x_0|, \dots, |x_N|\}$.

Note 4. My laptop is dying and I’m away from an outlet, so I gotta move and lose a few minutes. Whoops... Lost like 10ish minutes I think. Guess later I’ll look at the recording and fill in what I missed...

Example. Let $X \subset \mathbb{P}_{\mathbb{Q}}^3$ be a (smooth) cubic surface (e.g. $X : x^2 + y^2 + z^3 + w^3 = 0$). Then X has 27 lines and is rational, $X \cong \text{Bl}_{p_1, \dots, p_6} \mathbb{P}^2$. Let U be the complement of the 27 lines.

Conjecture 1.10. $N_U(B) \sim cB \log^{\rho-1} B$, where $\rho = \text{rank Pic } X$.

Note that X has lines, so $N_X(B)$ will have extra points. One gets $N_X(B) \sim c'B^2$. These lines are what are called accumulating subvarieties.

In general, there will be some exceptional subvariety Z that you should throw away; it’s not always easy to figure out what this should be. People have made conjectures about how to find this Z in general, but then other people keep finding counterexamples to those more precise conjectures.

What are a, b, c ? Recall $X \hookrightarrow \mathbb{P}^n$ via some line bundle \mathcal{L} .

Definition 1.11. The **Fujita invariant** is

$$a(X, \mathcal{L}) := \min \left\{ t \in \mathbb{R} : K_X + tL \in \overline{\text{Eff}}'(X) \right\}$$

with $\overline{\text{Eff}}'(X)$ the ‘pseudo-effective cone.’ In practice, this is basically just requiring $K_X + tL \geq 0$. What is this pseudo-effective cone. Start with $\text{Eff} \subset \mathbb{R}^{\rho} \cong \frac{\text{Pic } \overline{X}}{\text{Pic } \overline{X}_{\text{tors}}} \otimes_{\mathbb{Z}} \mathbb{R}$ the cone generated by the effective divisors.

For b , we use $b(K, X, \mathcal{L}) = \text{codim of minimal face of } \overline{\text{Eff}}'(X) \text{ containing } K_X + aL$.

For c , see Perre’s paper.

Example. If $K_X \geq 0$, then $a = 0$. This holds, for example, if X is K3 or an abelian variety. In these cases, we expect the log term to dominate.

Example (Swinnerton-Dyer K3). $x^4 + 2y^4 = 1 + 4z^3$

Swinnerton-Dyer has conjecture only two solutions are $(\pm 1 : 0 : 0)$. Turns out there are more. The next smallest are

$$\left(\pm \frac{1484801}{1169407}, \pm \frac{1203120}{1169407}, \pm \frac{1157520}{1169407} \right).$$

We now expect there to be infinitely many solutions (from computing these a, b, c) with the number growing logarithmically with the height.

Example. Take $\varphi : \mathbb{P}^n \xrightarrow{\cong} \mathbb{P}^N$, so $\mathcal{L} = H$ is a hyperplane and $K_X = -(N+1)H$. Hence, $K_X + tL = -(N+1)H + tH \geq 0 \iff t \geq N+1$, so $a = N+1$.

Take $\mathbb{P}^1 \hookrightarrow \mathbb{P}^2$ with $\mathcal{L} = +2$ pts $= -K_X =: L$. Then, $K_X + tL = 2(t-1)$ pts $\geq 0 \iff t \geq 1$. Hence, $a = 1$ here.

Example. Say $X \subset \mathbb{P}^3$ a smooth cubic. “Honestly, the most fun thing you can do is compute things with the adjunction formula.” Adjunction here says

$$K_X = (K_{\mathbb{P}^3} + X)|_X = (-4H + 3H)|_X = -H|_X$$

so $L = -K_X$ here. We get that X is Fano and $a = 1$.

1.2.1 Function Fields

Say $K = \mathbb{F}_q(t)$ or $\mathbb{F}_p(C)$ (function field of some curve). How do we define height?

A point of $\mathbb{P}^n(\mathbb{F}_q(t))$ looks like (after clearing denominators and common factors)

$$[f_0(t) : \cdots : f_N(t)].$$

The naive height is $\text{ht}(P) := \max\{\deg f_0, \dots, \deg f_N\}$.

We can do better than this though. Think of \mathbb{P}_K^N as the generic fiber of

$$\begin{array}{c} \mathbb{P}^N \times \mathbb{P}^1 \\ \downarrow \\ \mathbb{P}^1. \end{array}$$

A K -rational point is now a section, and the image of that section is a curve.

Say we have a variety X over $K = \mathbb{F}_q(C)$ along with a model $\mathcal{X} \xrightarrow{\text{proper}} C$. Since \mathcal{X} is proper over C , a K -point $\text{spec } X \xrightarrow{x} \mathcal{X}$ extends to a section $\bar{x} : C \rightarrow \mathcal{X}$. Say $L \in \text{Pic } X$ is a line bundle, and extend to \mathcal{L} on \mathcal{X} . We define height as

$$\text{ht}_{\mathcal{L}}(x) = \deg(\bar{x}^* \mathcal{L}).$$

Why do line bundles extend? Think of a line bundle (with a section) as a divisor. Then extend the divisor and take \mathcal{O} of the resulting thing. This notion of height is purely geometric.

Recall the bijection $x \in \mathcal{X}(K) \leftrightarrow \text{map } C \rightarrow \mathcal{X}$. Can write down moduli space $C_d(\mathcal{X}, C)$ of degree d maps $C \rightarrow \mathcal{X}$. Can count \mathbb{F}_q -points on this (apply Weil conjectures). Working this out is where the definition of a comes from.

1.3 DZB (6/16)

1.3.1 Stacky Bat-Man

“Has the phrase ‘Stacky Bat-Man’ appeared in the literature?” (audience)

“There’s a lot of Batman literature.” (audience)

(joint work with Jordan Ellenberg and Matt Satriano (spelling?) that should appear on arxiv this summer)

Let $X \subset \mathbb{P}^N/K$ be a variety over a global field.

Conjecture 1.12 (BM). *There exists some non-empty open $U \subset X$ and explicit constants a, b, c such that the counting function is $N_U(B) \sim cB^a \log^b B$.*

(secretly, X above doesn’t really need to be projective or smooth)

On Monday, Jordan discussed a similar looking conjecture.

Conjecture 1.13 (Malle). *Let $G \leq S_n$ be a group, and fix a number field K . Then, there exists constant a, b, c s.t. the counting function $N_{G,K}(B) \sim cB^a \log^b B$.*

Above, $N_{G,K}(B)$ is G -extensions of K .

The idea is that these two conjectures should be specializations of the same, more general, conjecture. Let $BG = [\text{spec } \mathbb{Z}/G]$ (stack quotient). Also, let $*$ = $\text{spec } \mathbb{Z}$ be the terminal action. So we have $*$ \rightarrow BG with G -action on $*$. If you have $T \rightarrow BG$, then the pullback $P = T \times_{BG} * \rightarrow T$ inherits this G -action as well. For example, $BG(\mathbb{Q}) = \# \text{ fields}^4$ w/ Galois group G .

Conjecture 1.14 (Ellenberg-Satriano-ZB.). *Let \mathcal{X} be a proper Artin stack over a global field K w/ finite diagonal. Let $V \in \text{Vect}_{\mathcal{X}}$ be some vector bundle (need a positivity condition, e.g. Northcott). Then, there exists constant a, b, c s.t. $N_{\mathcal{X},V}(B) = cB^a \log^b B$.*

So far, they have an explicit conjecture for what a is. They have some idea for what b is, but not enough of one to make a specific conjecture. Less clear what c should be.

Note 5. I’m really bad at remembering to record discussions people have that weren’t formally part of the talk...

Let’s mention some interesting examples of stacks.

Example. $B\mu_2$ over \mathbb{F}_p with $p \neq 2$. Note that $B\mu_2(k(t))$ parametrizes hyperelliptic curves (or $k(t) \times k(t)$), so notion of stacky height should recover genus (more-or-less)

Example. Generalized Fermat surfaces $X : x^p + y^q + z^r = 0$. This has a (weighted) \mathbb{G}_m -action, so can form stack quotient $[(X \setminus 0)/\mathbb{G}_m]$. In p, q, r are coprime, this looks like a \mathbb{P}^1 with 3 stacky points with stabilizers μ_p, μ_q, μ_r .

⁴Secretly actually étale algebras

Example. Can look at $\mathcal{A}_g, \mathcal{M}_{1,1} \operatorname{Sym}^n \mathbb{P}^M = [(\mathbb{P}^M)^n / S_n]$, etc. Also weight projective stacks like $\mathbb{P}(a, b) = [(\mathbb{A}^2 \setminus 0) / \mathbb{G}_m]$ with \mathbb{G}_m acting by weights (a, b) ; people sometimes call these (American) 'footballs' (looks like \mathbb{P}^1 but w/ stacky points at 0 and ∞).

Here are some problems one might come across

- What does height mean?

Note, projective stacks are schemes, so there is no embedding $\mathcal{X} \hookrightarrow \mathbb{P}^N$. Alos, note that the coarse space loses information (e.g. the coarse space of BG is $*$)

since descent for schemes w/ an ample line bundle is effective, or something like this

- Need to look at vector bundles instead of line bundles

$\operatorname{Vect} BG \simeq \operatorname{Rep} G$, so $\operatorname{Pic} BG$ is torsion (characters of (finite group) G). Hence, heights $\operatorname{ht}_{\mathcal{L}}$ for line bundles can't be additive in \mathcal{L} .

- Properness is 'wonky'

If R is a dvr with fraction field K , the map $\mathcal{X}(R) \rightarrow \mathcal{X}(K)$ is not necessarily surjective, but "this is a feature, not a bug."

Example. Consider BG . Say we have

$$\begin{array}{ccc} P & \longrightarrow & * \\ \downarrow & \lrcorner & \downarrow \\ T & \longrightarrow & BG \end{array}$$

Take e.g. $T = \operatorname{spec} K$ and $P = \operatorname{spec} L$ a G -extension. We want to say this K -point won't necessarily extend to an \mathcal{O}_K -point. What \mathcal{O}_K -point would it extend to? You'd expect it's extend to $\operatorname{spec} \mathcal{O}_L$, but $\operatorname{spec} \mathcal{O}_L \rightarrow \operatorname{spec} \mathcal{O}_K$ is ramified (so not a G -torsor). Instead the K -point will extend to a \mathcal{C} -point where $\mathcal{C} := [\operatorname{spec} \mathcal{O}_L / G]$ (which lies above $\operatorname{spec} \mathcal{O}_K$ but below $\operatorname{spec} \mathcal{O}_L$).

TODO: Draw diagram?

We have half an hour left. In that time, we'd like to

- say what heights on stacks are
- say more about some example (e.g. $B\mu_2$)
- say what the explicit conjecture for the value of a should be

Foreshadow: the height on a stack will break into two pieces, a stable height satisfying additivity and also a 'sum of local heights' picking up ramification.

"Our approach is not axiomatic, but since projective space no longer helps – I had another meme..."

Recall 1.15. Say $K = \mathbb{F}_q(C)$. Recall yesterday we picked model $\mathcal{X} \rightarrow C$ of $X_0 \rightarrow \operatorname{spec} K$. Then, any K -point $\operatorname{spec} K \xrightarrow{x} X_0$ extends to a section $\bar{x} : C \rightarrow \mathcal{X}$, and we defined

$$\operatorname{ht}_{\mathcal{L}}(x) = \deg(\bar{x}^* \mathcal{L}).$$

We can do something similar even over \mathbb{Q} . Given $X_0 \rightarrow \operatorname{spec} \mathbb{Q}$, can extend to an integral model $\mathcal{X} \rightarrow \operatorname{spec} \mathbb{Z}$. A \mathbb{Q} -point $\operatorname{spec} \mathbb{Q} \xrightarrow{x} X_0$ will extend to a \mathbb{Z} -point $\operatorname{spec} \mathbb{Z} \xrightarrow{\bar{x}} \mathcal{X}$. Can then consider the

pullback $\bar{x}^*\mathcal{L}$ of a line bundle on \mathcal{X} . Sadly though, $\text{Pic spec } \mathbb{Z} = 0$. This can be fixed though using Arakelov theory (“metrized line bundle”). One end up with a theory of heights over \mathbb{Q} that’s exactly additive (instead of additive up to $O(1)$) like in the function field case.

Using an approach like this gets over a problem that there’s no embedding $\mathcal{X} \hookrightarrow \mathbb{P}^N$ when \mathcal{X} a stack (that’s not a scheme).

Let \mathcal{X} be a proper stack. Let C be a curve over \mathbb{F}_q or be $\text{spec } \mathcal{O}_K$. Consider diagram

$$\begin{array}{ccc} \mathcal{X}_0 & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow \\ \text{spec } K & \longrightarrow & C \end{array}$$

Fix a vector bundle V_0 on \mathcal{X}_0 w/ extension V to \mathcal{X} . Unfortunately, K -points on \mathcal{X}_0 do not automatically extend to C -points of \mathcal{X} (recall ramification example from before).

Theorem 1.16. *Given $x : \text{spec } K \rightarrow \mathcal{X}$ over C , there exists a stack \mathcal{C} with (birational?) coarse space $\pi : \mathcal{C} \rightarrow C$ and a factorization*

$$\begin{array}{ccccc} & & x & & \\ & \nearrow & & \searrow & \\ \text{spec } K & \longrightarrow & \mathcal{C} & \xrightarrow{\bar{x}} & \mathcal{X} \end{array}$$

over C . Here, \mathcal{C} is the relative normalization of x .

Note 6. There was some discussion on how one proves this, and issues that may arise, but I didn’t follow...

Definition 1.17. Given above theorem, we define the **height of a rational point w/ respect to a vector bundle on \mathcal{X}** as $\text{ht}_V(x) = -\deg(\pi_*\bar{x}^*V^\vee)$.

What’s up with this dual and minus and pushforward? “We want our heights to be Northcott, not Southcott” (sounds like this is the reason for the dual and minus sign, after working out some examples).

Example. Consider $B\mu_2$. Let $K = \mathbb{F}_q(\mathbb{P}^1)$. A $k(t)$ -point of $B\mu_2$ is a hyperelliptic curve $H \rightarrow \mathbb{P}^1$. Can fit inbetween the stack $\mathcal{C} = [H/\mu_2]$, so have Cartesian

$$\begin{array}{ccc} H & \longrightarrow & * \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\bar{x}} & B\mu_2 \end{array}$$

Note $\text{Pic } B\mu_2 \simeq \mathbb{Z}/2\mathbb{Z}$, say with generator \mathcal{L} . Note that $\deg(\bar{x}^*\mathcal{L}) = 0$ (it’s square is trivial). On the other hand, one can work out that

$$\mathcal{L} = \mathcal{O}\left(\sum \text{stacky points} - (g+1)\infty\right).$$

Pushing forward amounts to taking floors, so $\pi_*\mathcal{L} = \mathcal{O}(-(g+1)\infty)$. Thus,

$$\text{ht}_{\mathcal{L}} \bar{x} = \pm(g+1).$$

Hence, it’s picking up the genus.

TODO:
Make sure
I wrote this
down cor-
rectly

Let's end with the Fujita invariant in the stacky case. Say we have

$$\begin{array}{ccc} \mathfrak{C} & \xrightarrow{\bar{x}} & \mathfrak{X} \\ & \searrow \pi & \swarrow \\ & C & \end{array}$$

and also $x : C \rightarrow \mathfrak{X}$. Let $\text{edd}(x)$ be the “expected deformation dimension” which seems to be

$$\text{edd}(x) = \chi(L_{\bar{x}}^*[1]) = \chi(\bar{x}^*T_{\mathfrak{X}}) - \chi(T_{\mathfrak{C}}) = \deg(\pi_*\bar{x}^*T_{\mathfrak{X}}) - \deg \pi_*T_{\mathfrak{C}} + C = -\text{ht}_{K_{\mathfrak{X}}}(x) + \text{rDisc}x$$

with $\text{rDisc}(x)$ the ‘reduced discriminant’.

Recall 1.18. Classically, BM predicts

$$a = \min(t \in \mathbb{R} : K_X + tL \geq 0)$$

(more-or-less. Actually need to say the phrase ‘effective cone’ or whatever).

In the stacky situation, seems there's not good notion of ‘effective cone’. So instead, one predicts

$$a := \min\{t \in \mathbb{R} : f(x) := -\text{edd}(x) + t \text{ht}_V(x) \text{ is generically bounded below}\}.$$

Sounds like one can check that this restricts to the predicted value of a in both the BM and Malle conjectures.

1.4 Ellenberg (6/17): Examples and Problems

Recall from David's talk

Conjecture 1.19 (Malle). *#G-extensions L of a global field K with $|\text{Disc } L| < X$ is asymptotic to $c_{K,G} X^{a(G)} (\log X)^{b(G,K)}$.*

This is a question about rational points on BG with bounded height.

But wait: if $G = S_3$, do we mean

- L/K a cubic extension w/ Galois group S_3 ; or
- M/K a Galois sextic extension w/ Galois group S_3

Am I counting by $D_{L/K}$ or by $D_{M/K}$? These are different questions.

Example. Say we have $\text{spec } K \rightarrow B(S_3)$. Pulling back along $*$ gives $\text{spec } M \rightarrow \text{spec } K$ w/ an S_3 -action. So we can also recover $\text{spec } L = \text{spec } M / \langle \tau \rangle$ ($\tau \in S_3$ some transposition).

Remark 1.20. One should have $D_{L/K} = ab^2$ and $D_{M/K} = a^3b^4$ where

$$a = \prod_{p: \# \rho(I_p)=2} p \text{ and } b = \prod_{p: \# \rho(I_p)=3} p.$$

Above, $\rho : G_K \rightarrow S_3$ the natural map.

Davenport-Heilbronn counted cubic fields by $D_{L/K}$. Seems we have not yet counted cubics by $D_{M/K}$.

The L vs. M distinction comes down to the choice of vector bundle on BG with respect to which we count heights. Recall a vector bundle on BG is a representation of G .

Example. $V =$ regular rep of G corresponds to counting by discriminant of Galois extension $D_{M/K}$

Example. $V =$ permutation rep of G (i.e. $G \hookrightarrow S_n$), then counting by discriminant of the degree n extension arising from $G \hookrightarrow S_n$

Example. Varma, Altus, SHanker, Wilson (2017) count D_4 -extensions. In this current perspective, they count using the 2-dimensional rep V of D_4 . Their count has a nice constant (e.g. is has an Euler product representation) while a more classical count (by the analogue of $D_{L/K}$) had a nastier constant factor. So somehow some heights are better to count by than others.

Recall 1.21. The stacky height we defined is

$$-\deg \pi_* \bar{x}^* V^\vee \in \mathbb{R}.$$

Note that we can also define the “*vector bundle height*” by not taking degrees, $\pi_* \bar{x}^* V^\vee$, a vector bundle on C (which is $\text{spec } \mathcal{O}_K$ or a curve, e.g. $\text{spec } \mathbb{Z}$ or \mathbb{P}^1). Taking degrees throws out some information, potentially more than we wanted.

Example. A vector bundle on \mathbb{P}^1 is always a sum of line bundles: $\mathcal{O}(a_1) \oplus \cdots \oplus \mathcal{O}(a_r)$ with degree $\deg = \sum a_i$.

Example. A metrized vector bundle on $\text{spec } \mathbb{Z}$ is a lattice \mathbb{Z}^r equipped w/ a bilinear form.

When $\mathcal{X} = BG$, $G \hookrightarrow S_n$, and V is the permutation rep, this “vector bundle height” is simply the lattice \mathcal{O}_L equipped w/ the trace form. The covolume of this lattice is $\sqrt{|D_{L/K}|}$, up to simple factors.

Open Question 1.22. *How many cubic fields of disc $< X$ are there s.t. $\exists \alpha \in \mathcal{O}_L \setminus \mathbb{Z}$ w/ all arch. $|\alpha| < 0.000001 X^{1/2}$ (Bhargava-H 2016)? What if we want $|\alpha| < X^{0.4999}$ (open)?*

Open Question 1.23. *Say $\mathcal{X} = \mathbb{P}^2$ with $V = T_{\mathbb{P}^2}$. If $x \in \mathbb{P}^2(\mathbb{Q}) = (a : b : c)$, then the v.b. height of x w.r.t $T_{\mathbb{P}^2}$ is $(a : b : c)^\perp \subset \mathbb{Z}^3$. This has covolume $\sqrt{a^2 + b^2 + c^2} \sim \max(|a|, |b|, |c|)$.*

... I got distracted and missed the question itself.

See some work of Peyre and some work of Sawin (a paper with ‘freeness’ in title) for more along these lines.

Question 1.24. *How many iso classes of E/\mathbb{Q} such that E has a rational 5-isogeny and $\max(|A|^3, |B|^2) < X$, where $y^2 : x^3 + Ax + B$ is a min. Weierstrass form.*

This is usual called ‘naive height’, but maybe it’s not so naive. It turns out that this is the height of E as a point of the stack $X_0(5)$ w.r.t the Hodge bundle.

Answer (Bogges-Sanker 2020). $\Theta(x^{1/6} \log X)$

They also did it for $X_0(N)$ for $N = 2, 3, 4, 6, 8, 9, 12, 16, 18$. Follows up Harron-Snowden (2017) which asks for 5-torsion instead of 5-isogeny and gets $\sim X^{1/6}$.

Note that the moduli of elliptic curves w/ a 5-torsion point is a scheme, while $X_0(5)$ is a stack. This is where the difficulty lies.

If N is too big, then there will only be finitely many rational points (e.g. by Faltings)

Open Question 1.25. *What about $X_0(7)$?*

Sounds like this is the only case where $X_0(N)$ is rational not handled by Bogess-Sanker.

Here's another cool/recent result. $X_0(3)$ is particularly interesting (Pizzo-Pomerence-Voight 2019) $\sim cX^{1/2} + O(X^{1/3})$. The dominant term here comes just from curves with j -invariant 0. So here we see an accumulating subvariety which is just a 'point' (point in the coarse space).

Definition 1.26. Let $\text{sqf}(a)$ be the “squarefree part of a ,” the (smallest?) squarefree number m s.t. ma is a square.

Question 1.27. *How many pairs of coprime a, b such that*

$$[\text{sqf}(a)\text{sqf}(b)\text{sqf}(a-b)\max(a,b)]^{1/2} < X?$$

Can check that contribution of Pythagorean triples is $\sim X$. Contribution of a, b squarefree is $\sim X$. Le Boudec (2020) and Nasserden-Xiao (2020) both showed the answer is $\Theta(X \log^3 X)$.

Remark 1.28. This quantity they counted is the height of the point $(a : b)$ on the stacky curve \mathcal{X} which looks like \mathbb{P}^1 but where $0, 1, \infty$ are each a $B\mu_2$ (a $1/2$ -point).

Recall that the stacky conjecture does not (yet) predict a specific value of b , so a priori only expect that the answer lies between X^1 and $X^{1+\varepsilon}$. Hard to predict the value of 3 in the exponent of log before computing it.

Open Question 1.29. *Are there only finitely many 5-term coprime arithmetic progressions $a_1, a_2, \dots, a_5 \in \mathbb{Z}$ such that*

$$\text{sqf}(a_1 a_2 a_3 a_4 a_5) < \max(|a_i|)^{1-\delta}?$$

This is a Vojta-like statement.

Remark 1.30. You can't have 4 perfect squares in an arithmetic progression, so above value can't be 1.

2 Jennifer Balakrishnan (Boston University): Chabauty–Coleman and Chabauty–Kim experiments

2.1 (2/14)

Challenges in studying rational points on curves.

Theorem 2.1. *Let X be a smooth projective curve over \mathbb{Q} of genus at least 2. Then, the set $X(\mathbb{Q})$ is finite.*

How do we actually find $X(\mathbb{Q})$?

- Falting’s proof is not constructive
- Another proof due to Vojta is not constructive
- Recent work of Lawrence-Venkatesh give another proof which is not constructive
- The method of Chabauty-Coleman is effective, but does not always apply

Today and tomorrow we’ll see a few examples of Chabauty-Coleman

- Sometimes it can precisely compute $X(\mathbb{Q})$
- Other times, Chabauty-Coleman computes a finite set of points $X(\mathbb{Q}_p)_1$ strictly larger than $X(\mathbb{Q})$. What are the “extra” points? Are any of them defined over other number fields? Can we explain why these points show up in $X(\mathbb{Q}_p)_1$?
- We will carry out some experiments in **SageMath** and try to find some interesting new examples.

On Wednesday and Thursday, we’ll look at some aspects of the Chabauty-Kim method through a series of examples

- We’ll focus on quadratic Chabauty and look at examples for punctured elliptic curves, as well as genus 2 curves
- Some highlights: Bianchi’s quadratic Chabauty approach to a problem of Diophantus, computing $X_0(37)(\mathbb{Q}(i))$, rational points on other modular curves
- We’ll carry out computations in **SageMath** and try to construct new examples

Remark 2.2. There’s a (free) upgraded resource on a Cocalc project available for this week.

2.1.1 Working with higher genus curves

For curves X/\mathbb{Q} of genus ≥ 2 , $X(\mathbb{Q})$ is just a set, so to study rational points, it helps to associate X to other objects with more structure.

Fix a basepoint $b \in X(\mathbb{Q})$. Embed X into its Jacobian J via $P \mapsto [(P) - (b)]$. The Mordell-Weil theorem says $J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$. The rank r is important, but difficult to compute.

First example: triangles We say a **rational triangle** is one whose side lengths are rational numbers.

Question 2.3. *Does there exist a rational right triangle and a rational isosceles triangle that have the same perimeter and the same area?*

Feels very classical, but seemingly wasn't looked at before 2018.

By rescaling both given triangles, may assume their lengths are $(k(1+t^2), k(1-t^2), 2kt)$ and $((1+u^2)(1+u^2), 4u)$, respectively. Here, $0 < t, u < 1$ and $k > 0$ (think of isosceles triangle as two right triangle pushed together). By comparing perimeters and areas, and doing some algebra, problem turns out to amount to finding rational points on the genus 2 curve

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

Chabauty-Coleman applies here and tells us that $\#X(\mathbb{Q}) \leq 10$. One can search for some points naively and indeed find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^\pm.$$

Tracing back, one obtains

Theorem 2.4. *(377, 135, 352) and (366, 366, 132) are the side lengths of the unique pair, up to similitude, of a right triangle and isosceles triangle with same perimeter and area.*

What allowed CC to work in this example? The genus of the curve was less than the rank of the MW group of the Jacobian $J(\mathbb{Q})$.

2.1.2 Strategy for computing rational points on curves

The main idea is to associate another geometric object to X that will allow us to compute a larger (but still finite!) set of points containing $X(\mathbb{Q})$. Then one hopefully can use this set to determine $X(\mathbb{Q})$.

- This story starts with Chabauty-Coleman
- There are many variations on the CC method (by Bruin, Flynn, Siksek, Stoll, Wetherall, ...) that have also tackled a number of interesting curves in higher rank

Theorem 2.5 (Chabauty, '41). *Let X be a curve of genus $g \geq 2$ over \mathbb{Q} . Suppose the MW rank r of $J(\mathbb{Q})$ is less than g . Then, $X(\mathbb{Q})$ is finite.*

Coleman ('85) made Chabauty's theorem effective by re-interpreting this result in terms of p -adic line integrals of regular 1-forms. By counting zeros of such integral, Coleman gave bound $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2$ for good $p > 2g$.

Let $p > 2$ be a prime of good reduction for X . The map $H^0(J_{\mathbb{Q}_p}, \Omega^1) \rightarrow H^0(X_{\mathbb{Q}_p}, \Omega^1)$ induced by ι is an isomorphism of \mathbb{Q}_p -vector spaces. Suppose ω_J restricts to ω . Then for $Q, Q' \in X(\mathbb{Q}_p)$, we define

$$\int_Q^{Q'} \omega := \int_0^{[Q'-Q]} \omega_J$$

(note J is a p -adic Lie group). If $r < g$, there exists $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ such that

$$\int_b^P \omega = 0$$

for all $P \in X(\mathbb{Q})$. Thus by studying the zeros of $\int \omega$, we can find a finite set of p -adic points containing the rational points of X .

Remark 2.6. Can run Chabauty-Coleman at various primes p and combine data to extract $X(\mathbb{Q})$ (instead of a bigger set). Key phrase: Mordell-Weil sieve.

We have

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_1 := \left\{ z \in X(\mathbb{Q}_p) : \int_b^z \omega = 0 \right\}$$

for a p -adic line integral $\int_b^* \omega$, with $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$. We would like to compute an annihilating differential ω (or several if we can) and find its (or their) zero set.

2.1.3 p -adic Line integration

How does one make sense of p -adic line integration?

Can construct local ("tiny") integral easily (using local coordinates in a single residue disk), but extending to entire space is challenging. Coleman's solution is to use analytic continuation along Frobenius. This gives a nice theory. Implementations available in SageMath for hyperelliptic curves and Magma (Github) for smooth curves.

Here are some nice properties

- It is $\overline{\mathbb{Q}_p}$ linear in ω
- If P, Q reduce to the same point $\overline{P} \in X_{\mathbb{F}_p}(\overline{\mathbb{F}_p})$, then we call it a tiny integral. It can be evaluated by writing $\omega = \omega(t)dt$...
- $\int_P^a \omega + \int_R^S \omega = \int_P^S \omega + \int_R^Q \omega$, so can define $\int_D \omega$ for any degree zero divisor.
- If D principal, then $\int_D \omega = 0$.
- The integral is compatible with the action of $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.
- Fix $P_0 \in X(\overline{\mathbb{Q}_p})$. If $0 \neq \omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$,...

More on Chabauty-Coleman bounds






(1) Stoll: if $r < g$ and $p > 2r + 2$ is a good prime, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r$

(2) Stoll: if $p > 2$, then

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor.$$

(3) ...

3 List of Marginal Comments

	Question: What is K ?	4
	since descent for schemes w/ an ample line bundle is effective, or something like this	7
	TODO: Draw diagram?	7
	TODO: Make sure I wrote this down correctly	8
	If N is too big, then there will only be finitely many rational points (e.g. by Faltings)	10

Index

Fano, 4

Fujita invariant, 4

general type, 3

height of a rational point w/ respect to a vector

bundle on \mathcal{X} , 8

rational triangle, 13

Swinnerton-Dyer K3, 5