ELLENBERG/ZURICK-BROWN RTG WORKSHOP

These are notes taken live during the Ellenberg/Zurick-Brown Berkeley RTG Workshop in June 2021.¹

I. MONDAY: COUNTING NUMBER FIELDS

In arithmetic statistics one wants to count L/\mathbb{Q} number field (or global function field $L/\mathbb{F}_q(t)$) of degree d and discriminant $D_{L/\mathbb{Q}}$ as an ideal of \mathbb{Z} .

Theorem 1 (Hermite). There are only finitely many number fields of degree d and $|D_{L/\mathbb{O}}| < X$.

Sketch. Primitive element theorem: $L = \mathbb{Q}(\alpha)$ for $\alpha \in \mathcal{O}_L$ whose minimal polynomial is monic with \mathbb{Z} coefficients. Hermite shows one can choose such an α with all $|\alpha|$ bounded, and thus with all the $|a_i|$ (elementary symmetric polynomials) in terms of $|D_{L/\mathbb{Q}}|$. One can do this because the discriminant controls
the covolume of the integer lattice \mathcal{O}_L , and then use Minkowski's theorem to find an α in a small box. \Box

This gives an explicit bound on number fields with discriminant $\langle |X|$

$$N_d(X, \mathbb{Q}) < c + dX^{(d+2)/4}.$$

It is conjectured that in fact

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

If we restrict to S_n -extensions, Bhargava predicts the value of c_d .

What is known:

- d = 2. Then $L = \mathbb{Q}(\sqrt{m})/\mathbb{Q}$ the discriminant is roughly m. This is exactly true when m is square-free, so one proves the analytic fact that the number of square-free integers in [-X, X] is asymptotic to X.
- d = 3. Davenport-Heihroun (1970).
- d = 4, 5. Bhargava.

In this field, the fundamental wall seems to be 5 vs 6: to prove d = 6 would require a big new set of ideas. There is substantial progress on upper bounds.

- Ellenberg and Vakatesh (2006) obtained an upper bound of $X^{c\sqrt{\log d}}$.
- Couvaignes (2019) and then Lemke, Oliver, and Thorne (2020) improved this to $X^{c \log^2 d}$.

All three papers improve on Hermite's approach in the following way.

Take an affine space V with faithful (but not fixed-point-free) action of finite group G (here S_d). Then we have a map

$$(V/G)(\mathbb{Q}) \to \{G \text{-extensions of } \mathbb{Q}\}.$$

given by $P \mapsto$ field corresponding to $\pi^{-1}(P)$, where π is the structure projection $V \to V/G$. One shows that every G-extension of $|\operatorname{disc}| < X$ arises from a point of $(V/G)(\mathbb{Z})$ with height at most c(X), then counts points on $V/G(\mathbb{Z})$ of height at most c(X).

Hermite's proof applies this technique to $V = \mathbb{A}^d$, with the action of permuting coordinates. So the essence of the argument is that \mathbb{A}^d/S_d is also an affine space, generated by the elementary symmetric polynomials. So Hermite shows we can find a bounded point in this quotient affine space.

The idea of EV(06) is to let $V = (\mathbb{A}^d)^r$ with S_d acting diagonally by permutation of coordinates. Functions on the quotient V/S_d are called multisymmetric functions. One counts points on it by choosing Nmultisymmetric functions, i.e. a map $V/S_d \to \mathbb{A}^N$ and counting points on \mathbb{A}^N . You need to make N big enough to make this injective, or at least have finite fibers.

- In EV, one needs to take $N \sim 2^{2r} \cdot d$ in order to show injectivity.
- Caveignes improves this to $N \sim r^2 d$.
- LO/Thorne show injectivity with $N \sim rd$.

¹Notes by Connor Halleck-Dubé, UC Berkeley.

It is important that you not only minimize N but also the degree of the functions which generate the map.

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

This technique counts not only S_d -Galois extensions, but also all other degree d extensions. Three points of philosophy:

(1) The conjecture $N_d(X, \mathbb{Q}) \sim cX^1$ (Malle's) is motivated by the function field case. Degree d extensions of $\mathbb{F}_q(t)$ are covers of $\mathbb{P}^1_{\mathbb{F}_q}$ of degree d, which are the \mathbb{F}_q -rational points of a moduli space called a Hermite space.

In order to make this finite we need to bound the genus, which corresponds to bounding the discriminant. The discriminant of such a cover has norm q^n , where n is the number of branch points of the cover. It turns out the Hurwitz space of covers with n branch points and degree d has dimension n, so one heuristically guesses that it has q^n points over \mathbb{F}_q . This is unjustified but often close to correct. (EV 16). It fails horribly when counting abelian varieties in (Lipnowski-Tsiquessen 18), however.

(2) One can refine the discriminant with the notion of *shapes* of a number field. If L/\mathbb{Q} is a number field, then \mathcal{O}_L is a lattice with covolume $\sim |D_{L/\mathbb{Q}}|$ and bilinear form $(\alpha, \beta) = \text{Tr}(\alpha\beta)$.

What can we say about the shape of this lattice in the space of lattices? It is known to be equidistributed in d = 3 (Terr) and d = 4, 5 (Bhargava-H 16), and for specific Galois groups by some works of Harron et al.

Is the shape of the lattice (i.e. the lattice up to isometry) a complete invariant? Not in general because of some simple counterexamples, but (Mantilla-Soler, Rivera Guerra 2019) show for totally real number fields it *is* complete.

The shape actually does seem to be important in this picture. Roberts in 2000 on the basis of numerical evidence conjectured that

$$N_3(X, \mathbb{Q}) = c_3 X - c' X^{5/6} + o(X^{5/6}).$$

This has been proven by Bhargava-Shankar-Tsimerman and Tanisuchi-Thorne and Zhao in the function field case. The key idea is to separate cubic fields by shape. The "missing" $X^{5/6}$ are lattices whose shape is so skew that they cannot occur.

(3) What does counting number fields have to do with rational points? Clearly counting points on (V/G) was necessary for the story, but the connection is more fundamental. A *G*-extension of a field *K* is a *K*-rational point on the *classifying stack BG*. So this is a rational-point-counting question.

A vector bundle on BG is exactly a representation V of G, exactly as above. Its total space is V/G. So we can rephrase Hermite's strategy in abstract language: to count points on a stack \mathcal{X} , choose a suitable vector bundle V on \mathcal{X} , with total space $\mathcal{Y} \to \mathcal{X}$. Step 1: show that every low-height point on \mathcal{X} comes from a low-height point on \mathcal{Y} . Step 2: Count low-height points on \mathcal{Y} .

The strategy above then embeds \mathcal{Y} into something else (namely affine space) in order to accomplish Step 2.

In the case \mathcal{X} is a scheme, this is exactly the dominant technique (the "method of the dominant torsor") used to approach the Batyrev-Manin conjecture on the number of \mathbb{Q} -points on a variety X with bounded height.

For this perspective, one needs to develop a theory of heights on stacks. We think there is a good notion extending the classical definition, which allows a unification of Malle's conjecture and Batyrev-Manin conjecture as both being stacky-point-counting.

II. TUESDAY: BATYREV-MANIN CONJECTURES

The Lang-Vojta conjecture says: if X is a variety of general type (meaning that K_X is big, or if you don't know what that is, ample), then $X(\mathbb{Q})$ is not Zariski-dense.

We can think of Batyrev-Manin as a kind of opposite of Lang-Vojta. If X is rational (more generally Fano, meaning that $-K_X$ is ample), then the rational points are Zariski-dense. But we can ask for more, namely how quickly the number grows with the height.

If X/\mathbb{Q} does have a dense set of rational points, then take an embedding $\varphi : X \hookrightarrow \mathbb{P}^N$ defined by \mathcal{L} , and let $U \subseteq X$ a Zariski-open.

One can consider the counting function

$$\mathcal{N}_{U,\mathcal{L}}(B) := \#\{P \in U(\mathbb{Q}) \mid h(P) \le B\}$$

The Batyrev-Manin conjecture says that

$$N_{U\mathcal{L}}(B) \sim cB^a \log^b B$$

for some explicit a, b, c. The formula for c is due to Peure (?).

For our purposes, it suffices to define naive height.

Definition 1. For $P = [x_0 : \cdots : x_N] \in \mathbb{P}^N(\mathbb{Q})$, the height of P is defined

$$\operatorname{ht}(P) := \max\{|x_0|, \dots, |x_N|\}$$

More generally, for $P \in \mathbb{P}^N(K)$ of the same form,

$$ht(P) := \prod_{v} \max\{||x_0||_v, \dots, ||x_N||_v\}$$

We illustrate these a, b, c with a series of low-genus examples.

Example 2. If $X = \mathbb{P}^1$ (with the embedding the identity), then an elementary computation gives $N_X(B) \sim 2\frac{6}{\pi^2}B^2$. Note the formula for the probability of two integers to be coprime.

Theorem 3 (Schanuel). As $B \mapsto \infty$,

$$N_{\mathbb{P}^N}(B) \sim c_{K,N} B^{N+1}$$

where $c_{K,N}$ has an explicit expression.

Example 4. Again consider $\varphi : X = \mathbb{P}^1 \hookrightarrow \mathbb{P}^2$, this time with the anti-canonical conic embedding $[a:b] \mapsto [a^2:ab:b^2]$. So $N_{\mathbb{P}^1,-K_{\mathbb{P}^1}}(B) \sim cB$.

In general, we will see that Fano varieties with the anticanonical embedding have a = 1.

Example 5. Let $X \subseteq \mathbb{P}^3$ be a (smooth?) cubic surface over \mathbb{Q} , like for example $w^3 + x^3 + y^3 + z^3 = 0$. One has

$$N_X(B) \sim c^1 B^2$$
,

despite the fact that X is Fano, so we should be expecting the exponent of B to be 1. Why is this happening? Let Z be the locus of 27 lines on it, and U the complement, which is rational. The conjecture implies that

$$N_U(B) \sim cB \log^{s-1} B$$

where $s = \operatorname{rk}\operatorname{Pic} X$.

What this example shows is that the 27 lines are an exceptional locus, contributing more than they should to the point count. So the conjecture needs a caviat involving throwing away a certain exceptional "thin" subset.

The constants are themselves interesting geometric invariants defined in terms of the (pseudo-)effective cone. With $\varphi: X \hookrightarrow \mathbb{P}^N$ defined by L the constant a occurring in the conjecture is defined

$$a(X,L) := \min\{t \in \mathbb{R} : K_X + tL \in \overline{\mathrm{Eff}}^{\,\mathrm{r}}(X)\}$$

and the constant b (which depends on K, unlike a) is

$$b(K, X, L) := \text{codim of minimal face of } \overline{\text{Eff}}^{1}(X) \text{ containing } K_{X} + aL$$

There is also an explicit expression for c, see Peyre. Note that if $K_X \ge 0$, then a = 0 by definition. In the case of K3 surfaces or abelian varieties, one has a = 0.

Example 6. The Swinnerton-Dyer K3 surface is

$$x^4 + 2y^4 + 14z^4$$
.

It was conjectured for a long time that the only solutions were $[\pm 1:0:0]$. However a single huge solution was later found. This makes sense in the context of the conjecture: the conjecture suggests the number of points to grow logarithmically (to some power), so the heights of individual solutions should grow exponentially. We will probably never find the next solution, though we expect more.

Example 7. If we take $X = \mathbb{P}^N$ with L = H (i.e. the identity embedding) then $K_X = -(N+1)H$, so $K_X + tL \ge 0$ iff $t \ge N+1$ and we conclude a = N+1.

Example 8. Now take $\mathbb{P}^1 \hookrightarrow \mathbb{P}^2$ the anticanonical embedding. Then by definition $K_X + tL = (1-t)K_X \ge 0$ iff $t \ge 1$ so a = 1.

Example 9. Let $X \subseteq \mathbb{P}^3$ a cubic surface. What is the canonical bundle? We use the adjunction formula, which reads in this case

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

So cubic surfaces are Fano and the embedding is exactly the anticanonical one. By the same argument as the previous example, the invariant reads a = 1.

II.1. The Global Function Field case. Let $K = \mathbb{F}_q(t)$ or $\mathbb{F}_p(C)$ for some curve that isn't \mathbb{P}^1 (i.e. a finite extension of $\mathbb{F}_q(t)$). The naive height on \mathbb{P}^N is

$$\mathbb{P}^N(\mathbb{F}_q(t)) \ni [f_0/g_0 : \dots : f_N/g_N] = P.$$

Clearing denominators and common factors we define $ht(P) = max\{\deg f_0, \ldots, \deg f_N\}$.

We can do better, however. What is going on is that we are realizing $\mathbb{P}^N \to \operatorname{Spec} K$ as the generic fiber of some model, specifically $\mathbb{P}^N \times \mathbb{P}^1 \to \mathbb{P}^1$. A rational point defines a rational section of the structure map of the model, which extends to a regular section by properness.

In general, if X is a proper variety over $K = \mathbb{F}_q(C)$ and we take a model $\mathcal{X} \to C$, then a rational point on C defines such a section by taking the closure of the image (which lies on the generic fiber). In terms of line bundles, we take $L \in \operatorname{Pic} X$ and extend it to \mathcal{L} on \mathcal{X} . Then one can define the height as

$$\operatorname{ht}_{\mathscr{L}}(x) = \operatorname{deg} \overline{x}^{\star} \mathscr{L}.$$

The definition of a came from a moduli-theoretic interpretation. We have a bijective correspondence between $x \in \mathcal{X}(K) = X(K)$ and sections $C \to \mathcal{X}$ of the structure map. Then if we fix the degree of the sections, $C_d(\mathcal{X}, C)$ has a nice moduli space. The definition of the invariant a comes from doing analysis of this moduli space.

II.2. Working Group. Jordan said on Monday that the typical way of approaching Bat-Man problems is by replacing X with the total space of some vector bundle on X (actually, a G_m -torsor – we don't want the zero section). This is not so mysterious, as the following example shows.

Example 10. If $X = \mathbb{P}^1$, then take $V = \mathcal{O}(-1)$. The total space of V is approximately $\mathbb{A}^2 \setminus 0$ (kinda–this is the total space as a G_m -bundle. To count points on $\mathbb{P}^1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Z})$ of bounded height, we usually count $(\mathbb{A}^2 \setminus 0)(\mathbb{Z}) = \{(a, b) \in \mathbb{Z}^2 : \gcd(a, b) = 1\}$. On the other hand $\mathbb{P}^1(\mathbb{Z}) = \{[a : b] \in \mathbb{P}^1(\mathbb{Q}) : a, b \in \mathbb{Z}, \gcd(a, b) = 1\}$, so point-counting of bounded height is basically doing the same thing in \mathbb{A}^2 .

It often happens that for good enough X, there exists $Y \to X$ a $(G_m)^r$ -torsor (a torus torsor) with $r = \operatorname{rk}\operatorname{Pic} X$ such that the total space of Y is open in some \mathbb{A}^N or maybe some blowup of \mathbb{A}^N . This is the kind of strategy used for Batyrev-Manin.

Over a field with nontrivial class group, the picture of the example above is somewhat more complicated, because one may not take a global set of homogeneous coordinates which are all algebraic integers and relatively prime. This additional complexity translates to some fibers of $Y \to X$ being empty.

This doesn't happen for the cases we talked about on Monday: for example, given a finite extension of K, there actually is a polynomial with coefficients in \mathcal{O}_K giving rise to it. This is perhaps an incarnation of Hilbert 90.

The difference is fundamentally the difference between vector bundles and G_m^r -torsors. The former only has one rational form, the latter are classified by $H^1(\operatorname{Spec} K, G_m) = \operatorname{Pic}(\operatorname{Spec} \mathcal{O}_K)$.

Note that $\mathbb{A}^2 \setminus 0$ classifies surjections $\mathbb{O}^{\oplus 2} \to \mathbb{O}$ and \mathbb{P}^1 classifies line bundles L with surjections $\mathbb{O}^{\oplus 2} \to L$. The map we have described above is on the functor of points exactly the natural embedding of the former into the latter.

[Discussion I didn't understand about the classifying stack BG_m – decided the stack classifying $(L, \operatorname{Hom}(\Theta^{\oplus 2}, L))$ is \mathbb{A}^2/G_m .]

III. WEDNESDAY: STACKY BAT-MAN

Conjecture 1 (Batyrev-Manin). Let $X \subseteq \mathbb{P}^N/K$. There exists $U \subseteq X$ open and nonempty and constants a, b, c such that

$$N_U(B) \sim cB^a \log^b B.$$

Conjecture 2 (Malle). Let $G \subseteq S_n$ and K a number or global function field. Then there exists a, b, c such that

$$N_{G,K}(B) \sim cB^a \log^b B.$$

We interpret both of these as examples of the same conjecture about point-counting on stacks. Question: one doesn't really need projective in the first conjecture? Answer: No you don't, and you also don't need nonsingular.

Let $BG = [\operatorname{Spec} \mathbb{Z}/G]$. Its universal property is that if $\{\star\}$ is the terminal object (with trivial G-action) and $T \to BG$ is a map, then the G action lifts to the fiber product



such that the top map is equivariant.

The \mathbb{Q} -points of BG are étale algebras over \mathbb{Q} with Galois group G (generically, field extensions). It is the stackiest stack – basically a point, and everything interesting about it is stacky.

Conjecture 3 (E,S,Z-B). Let \mathcal{X} be a proper Artin stack over K with finite diagonal. Let $V \in \text{Vect } \mathcal{X}$. Then there exists a, b, c such that

$$N_{\mathcal{X},V}(B) = cB^a \log^b B.$$

Suggested reference: Geometric Consistency of Manin's Conjecture. Some examples other than BG.

Example 4. Over \mathbb{F}_p , $p \neq 2$ one has that $B\mu_2(k(t))$ classifies hyperelliptic cones.

If one takes $X : x^p + y^q + z^r = 0$ (a curve in weighted projective space) then there is a corresponding weighted-diagonal action of \mathbb{G}_m on X, and one can descend to the quotient $[X - 0/\mathbb{G}_m]$, which is a \mathbb{P}^1 with 3 stacky points when x, y, or z = 0 (nontrivial stabilizers).

Other examples this conjecture is interesting for: $A_g, \mathcal{M}_{1,1}, \operatorname{Sym}^n \mathbb{P}^m = [(\mathbb{P}^m)^n / S_n], \mathbb{P}(a, b).$ Problems:

- (1) What does height mean on stacks?
- (2) There does not exist an embedding $\mathcal{X} \hookrightarrow \mathbb{P}^N$.
- (3) The coarse space loses information, e.g. $BG \to \{\star\}$.
- (4) The vector bundles on BG are representations of G. This implies that $\operatorname{Pic} BG$ is torsion, and so $\operatorname{ht}_{\mathscr{L}}$ isn't additive in \mathscr{L} .
- (5) Properness is wonky: if $R \subseteq K$ is a DVR then the map $\mathcal{X}(R) \to \mathcal{X}(K)$ need not be surjective. For example,



If we have an \mathcal{O}_K -point, it does not necessarily extend to an \mathcal{O}_L -point because $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ is ramified. So instead we find that the point extends to a stacky curve \mathcal{C} living between $\operatorname{Spec} \mathcal{O}_L \to$ $\operatorname{Spec} \mathcal{O}_K$ which has stacky points at all ramification. III.1. Global Function Field. Everything is nicer for function fields. If $K = \mathbb{F}_q(C)$ for curve C and $\mathcal{X} \to C$ a (proper?) model. Then if



one defines height for a point x by pulling back our line bundle L along the corresponding section $C \to \mathcal{X}$ (the section extends by properness) and taking degree. One extends this to the number field case using the theory of metrized line bundles.

On the other hand, if \mathcal{X} is a stack and K is the function field of a curve C over \mathbb{F}_q or Spec \mathcal{O}_K , then given a diagram



and V a vector bundle on \mathcal{X} , the section corresponding to the point need NOT extend from the generic point to all

Theorem 5. There exists a birational map $\pi : \mathcal{C} \to \mathcal{C}$ to the coarse space from the relative normalization of the point $x : \operatorname{Spec} K \to \mathcal{X}$. So we have a commutative diagram



This gives the natural notion of height with respect to the vector bundle.

Definition 6. We define

$$\operatorname{ht}_V(x) := -\operatorname{deg} \pi_\star \overline{x}^\star V^\vee.$$

This is in particular independent of C chosen. In order to explain why pushforward along π , consider the following example.

Example 7. Consider $K = \mathbb{F}_q(t)$, $q \neq 2$ and $B\mu_2$. A hyperelliptic curve gives rise to a Cartesian diagram



with the top map equivariant for the μ_2 action, and $\mathcal{C} = [H/\mu_2]$ a stacky- \mathbb{P}^1 with stabilizers of μ_2 at the branch points of the hyperelliptic map. A line bundle on $B\mu_2$ is a 1-dimensional representation of μ_2 , i.e. a character mod 2, so we have $\operatorname{Pic} B\mu_2 \cong \mathbb{Z}/2$. Take \mathcal{L} the line bundle corresponding to the nontrivial character, so $\mathcal{L}^2 \cong \Theta$. But since \mathcal{L} and its pull-back to \mathcal{C} are both torsion, we have

$$\deg \overline{x}^{\star} \mathcal{L} = 0.$$

So just pulling back along \overline{x} is not enough to make this a reasonable notion of height – the stacky points are affecting our count. But can represent the line bundle by $\mathcal{L} = \mathcal{O}(\sum \text{stack-y points} - (g+1)\infty)$, and so when we pushforward under π , the contribution from the stacky points all vanishes and $\pi_*\mathcal{L} = \mathcal{O}(-(g+1)\infty)$.

III.2. Fujita Invariant. Given a stacky curve over a curve $\mathcal{X} \to C$ and a point on C defining a section $C \to \mathcal{X}$, we get an extended map \overline{x} as below.

$$\begin{array}{ccc} C & \xrightarrow{\overline{x}} & \mathcal{X} \\ & \searrow^{\pi} & \downarrow \\ & & C \end{array}$$

One can do a stacky-Riemann-Roch stype computation to determine that the "expected deformation dimension" edd(x) gives

$$\operatorname{edd}(x) = \chi(\overline{x}^{\star}T_{\mathcal{X}}) - \chi(T_{\mathcal{C}})$$

= deg($\pi_{\star}\overline{x}^{\star}T_{\mathcal{X}}$) - deg($\pi_{\star}T_{\mathcal{C}}$) + const
= - ht_{K_x}(x) + r Disc x

In order to generalize the condition $K_X + tL \ge 0$, we translate it to a numerical criterion: we want the corresponding intersection to be positive. So the right definition seems to be

 $a(V) := \min t \text{ s.t. } (-\operatorname{edd}(x) + t \operatorname{ht}_V(x)) \text{ is generally bounded below.}$

Then we have

$$c_{\varepsilon}' B^{a(V)} \le N(B) \le c_{\varepsilon} B^{a(V) + \varepsilon}$$

roughly as desired. [What happened to the $\log B$ term?]

III.3. Working Group Meeting. In the working group, Martin suggested that perhaps the of heights should be better understood as a function not on C or on \mathbb{P}^1 , but on $\mathcal{G}C$, the inertia stack. In the hyperelliptic example above, the inertia stack is $C \bigsqcup B\mu_2 \bigsqcup \cdots \bigsqcup B\mu_2$, an isolated stacky point for each stacky point on C. The height with respect to L the nontrivial character is then more naturally a function on $\mathcal{G}C$, as they defined it on the copy of C corresponding to the identity, and taking values of -1/2 on the isolated points.