

# Simons Meeting 2023 Notes

Niven Achenjang

July 2022

These are notes on talks given in “Simons Collaboration Meeting” which took place at Simons Foundation in NY. 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

<b>1 Jan 11</b>	<b>1</b>
1.1 Brendan Hassett (Brown University): Rationality and Arithmetic . . . . .	1
1.1.1 Guiding problem . . . . .	1
1.1.2 Small dimensions . . . . .	1
1.1.3 Three-folds . . . . .	2
1.1.4 Two quadrics $V_4 \subset \mathbb{P}^5$ . . . . .	3
1.1.5 $X_{18}$ example . . . . .	3
1.2 Wei Ho (IAS, Princeton, and UMich): Recent Progress in Arithmetic Statistics . . . . .	4
1.2.1 Part A . . . . .	4
1.2.2 Part B . . . . .	5
1.2.3 Combining w/ Circle Method . . . . .	5
1.2.4 $\mathbb{Q}$ -invariant method . . . . .	6
1.2.5 Higher moments . . . . .	6
1.2.6 Vinberg theory . . . . .	6
1.3 David Roe (MIT): Modular Curves and Finite Groups: Building Connections via Computations . . . . .	6
1.4 Robert Lemke Oliver (Tufts): Uniform exponent bounds on the number of primitive extensions of number fields . . . . .	6
1.5 Lightning Talks . . . . .	10
1.5.1 Alexander Betts (Harvard): Computing Local Heights for Quadratic Chabauty . .	10
1.5.2 Juanita Duque-Rosero: Triangular Modular Curves . . . . .	10

<b>2</b>	<b>Jan 12</b>	<b>11</b>
2.1	Wanlin Li (WashU): Ordinary and Basic Reductions of Abelian Varieties . . . . .	11
2.1.1	Newton polygon for abelian varieties . . . . .	12
2.1.2	Ordinary reductions . . . . .	13
2.1.3	Infinitely many basic primes . . . . .	13
2.2	Edgar Costa (MIT): Computing Isogeny Classes of Principally Polarized Abelian Surfaces Over the Rationals . . . . .	14
2.3	DZB . . . . .	14
<b>3</b>	<b>List of Marginal Comments</b>	<b>15</b>
	<b>Index</b>	<b>16</b>

## List of Figures

## List of Tables

# 1 Jan 11

## 1.1 Brendan Hassett (Brown University): Rationality and Arithmetic

Most results today are in algebraic or birational geometry, but they have connections to questions in arithmetic statistics.

Some of new results to be presented are joint with Yuri Tschinkel.

### 1.1.1 Guiding problem

Let  $X$  be a smooth and projective over a field  $k$  (usually  $\text{char } k = 0$ ). Assume that  $X$  is geometrically rational, i.e.  $\bar{X} = X_{\bar{k}}$  is a rational variety, i.e.  $\bar{k}(X) = \bar{k}(t_1, \dots, t_d)$ .

*Goal.* We would like to give criteria for when  $X$  is rational over  $k$ .

There are a few necessary conditions:

- (1)  $X(k) \neq \emptyset$

**Non-example.**  $X : x^2 + y^2 = -1$  is rational over  $\mathbb{C}$ , but not over  $\mathbb{R}$ . ▽

**Example.** If  $X : Q(x_0, \dots, x_{d+1}) = 0$  is given by a quadratic form, then

$$X(k) \neq \emptyset \implies X \text{ rational}/k$$

(project away from a fixed point to get birational map to  $\mathbb{P}^d$ ). △

- (2) Suppose  $k \hookrightarrow \mathbb{R}$ . Then, we must have  $X(\mathbb{R})$  connected (w/ Euclidean topology?)

- (3) There's a Chow group obstruction. Need

$$\text{deg} : \text{CH}_0(X) \xrightarrow{\sim} \mathbb{Z}.$$

In a rational variety, any two points can be joined by a line (or at least, a rational curve of some degree).

### 1.1.2 Small dimensions

**Recall 1.1.1.** We have the running assumption that  $X$  is always assumed geometrically rational. ⊙

Here are some results in small dimension cases

- $\dim(X) = 1$

$$X(k) \neq \emptyset \iff X \text{ rational}.$$

- $\dim(X) = 2$ . Need some 'elementary birational geometry'.

**Definition 1.1.2.** A surface  $X$  is **minimal** if it admits no pairwise disjoint collection of  $(-1)$ -curves defined over  $k$ . A  **$(-1)$ -curve** (over  $\bar{k}$ ) is a copy of  $\mathbb{P}^1 \simeq E \subset X$  with self-intersection  $E^2 = -1$ . ◇

If  $X$  is not minimal, you can blow-down any such collection. If you keep blowing things down like this, you'll eventually arrive at a minimal surface.

**Theorem 1.1.3** (Enriques-Manin-Tskavskikh (spelling?)). Assume  $X$  is geometrically rational over  $k$  and minimal. Then,  $X$  is rational over  $k$  if and only if  $X(k) \neq \emptyset$  and  $K_X^2 \geq 5$  ( $K_X$  the divisor class associated with  $\bigwedge^2 \Omega_X^1$ ).

**Non-example.** Cubic surfaces are never rational when minimal. ▽

This theorem “reduced rationality to Galois theory”. The main thing is to understand Galois action on the  $(-1)$ -curves over an algebraic closure.

If I'm not mistaken, these satisfy  $K_X^2 = 0$

### 1.1.3 Three-folds

There are a lot of three-folds. There are over 100 different classes of three-fold with negative canonical class, so we can't do all of them. Let's narrow our focus.

**Definition 1.1.4.** A variety is **Fano** if  $-K_X$  is ample. ◇

**Setup 1.1.5.** Let  $X$  be Fano of rank one, i.e.  $\text{Pic}(\overline{X}) \cong \mathbb{Z}$ .

The **index** of  $X$  is

$$\text{index}(X) = \text{divisibility of } K_X \text{ in } \text{Pic}.$$

Let's quickly recall the classification over  $\overline{k}$

(index 4) Only  $\mathbb{P}^3$  (★)

(index 3) Only quadratic hypersurface  $Q \subset \mathbb{P}^4$  (★)

(index 2)

- Complete intersection of two quadrics  $V_4 = \{Q_0 = Q_1 = 0\} \subset \mathbb{P}^5$
- intersection of Grassmannian with codim 3 subspace  $V_5 = \{\text{Gr}(2, 5) \cap \text{codim 3 linear subspace}\} \subset \mathbb{P}^6$  (★)

(index 1)

- $X_{12} = \{\text{OGr}(5, 10) \cap \text{codim 7 linear subspace}\} \subset \mathbb{P}^8$  (★)
- $X_{10} = \{\text{LGr}(3, 6) \cap \text{codim 3 linear subspace}\} \subset \mathbb{P}^{10}$
- $X_{18} = \{\text{G}_2\text{Grassmannian} \cap \text{codim 2 subspace}\} \subset \mathbb{P}^{11}$
- $X_{22} = \{\text{won't say here}\} \subset \mathbb{P}^{13}$  (★)

(Above, only talking about geometrically rational examples)

Let's first mention the ‘easy’ cases, by which we mean the ones where  $X(k) \neq \emptyset \implies X$  rational. These are the ones with a star (★) next to them.

### 1.1.4 Two quadrics $V_4 \subset \mathbb{P}^5$

Let's see a connection to arithmetic geometry. However, we'll first need a bit for geometry.

- (1)  $U_4 \subset Q_t$  is contained in a pencil of quadrics, e.g.  $Q_t = t_0 Q_0 + t_1 Q_1$ . These are generically of full rank, but with 6 members  $b_1, \dots, b_6 \in \mathbb{P}_t^1(\bar{k})$  of rank five.

*Remark 1.1.6.* We have 6 marked points on a  $\mathbb{P}^1$  and talk of degree 2 things, so maybe there should be a genus 2 curve lurking in the background.  $\circ$

Let  $F_2(G_4)$  be the space of maximal isotropic subspace. The Stein factorization of  $F_2(G_4) \rightarrow \mathbb{P}_t^1$  looks like

$$F_2(G_4) \longrightarrow C \xrightarrow{2} \mathbb{P}_t^1$$

with first map an étale  $\mathbb{P}^3$ -bundle and second map of degree 2 branched at  $b_1, \dots, b_6$ . An maximal isotropic subspace can be intersected with  $V_4$  (a maximal isotropic in quadric will give a conic in the other, or something), and so get an identification  $\text{conics}(V_4) \simeq F_2(G_4)$ .

- (2)  $\text{lines}(V_4)$  form (read: is isomorphic to) a principal homogeneous space  $P$  for the Jacobian of  $C$ . Furthermore,  $2[P] = [\text{Pic}^1(C)]$ , so  $P$  is a square-root of  $\text{Pic}^1(C)$  (in the Weil-Chatelet group).

**Theorem 1.1.7** (HT, Benast Wittenborg (spelling?)).  $V_4$  is rational if and only if  $[P] = 0$  in the Weil-Châtelet group, i.e. iff  $V_4$  admits a line  $\ell$  over  $k$ .

This is somehow reminiscent of work of Bhargava-Gross-Wang who use these sorts of constructions to produce cohomological obstructions to local-global on genus 2 curves.

*A bit about the proof.* ( $\Leftarrow$ ) Given a line  $\ell \subset X$ , projection from that  $\ell$  gives a birational map  $\pi_\ell : X \dashrightarrow \mathbb{P}^3$ .

( $\Rightarrow$ ) If  $X$  is rational, then  $P \simeq \text{Pic}^e(D)$  for  $D$  a curve blown up. A priori expect  $[P]$  to have order 4 (since  $\text{Pic}^2(C)$  has a rational point), but  $\text{Pic}^e(D)$  can only have order 1 or 2. This will create some tension which one can exploit to get a proof.  $\blacksquare$

### 1.1.5 $X_{18}$ example

Let  $G_2$  denote the exceptional Lie group, with Lie algebra  $\mathfrak{g}_2$ . Consider the projectivized adjoint representation  $\mathbb{P}(\mathfrak{g}_2) \simeq \mathbb{P}^{13}$ . In here, there is a closed orbit  $\mathcal{Z}$  (a  $G_2$  Grassmannian) contained in a hypersurface  $H$  of degree 6,

$$\mathcal{Z} \subset H \subset \mathbb{P}(\mathfrak{g}_2) \cong \mathbb{P}^{13}.$$

One has  $\dim(\mathcal{Z}) = 5$  and  $\deg(\mathcal{Z}) = 18$ . Recall that  $X_{18} = \mathbb{P}^{11} \cap \mathcal{Z}$ .

Now,  $\text{conics}(X_{18})$  is a PHG  $P$  for  $\text{Jac}(C)$  for some genus 2 curve  $C$ . Furthermore,  $\text{Lines}(X_{18}) \simeq$  genus ten curve. Looking at the intermediate Jacobian of  $X_{18}$  gives an embedding  $\text{Lines}(X_{18}) \hookrightarrow P'$ , a PHS for  $\text{Jac}(C)$  such that  $2[P'] = [P]$ . If I heard correctly,  $[P']$  will have order dividing 18.

**Theorem 1.1.8.** Say  $X_{18}$  degree 18 Fano 3-fold over  $k$ . Then,  $X_{18}$  is rational/ $k$  if and only if both

- (1)  $X_{18}(k) \neq \emptyset$   
(2)  $P = 0$ , i.e.  $X_{18}$  has a conic over the ground field

**Question 1.1.9.** *Is there an arithmetic statistics application of this? What's the fiber product of this result with Bhargava-Gross-Wang?*

## 1.2 Wei Ho (IAS, Princeton, and UMich): Recent Progress in Arithmetic Statistics

There's a lot of work (including much done by people here). To keep things reasonable, we'll only look at one particular direction and recent advances in it.

Today we talk about the “parameterize and count” method that's gotten a lot of use in recent decades (but goes back to Gauss and others). We'll start with an overview of the general method, in two parts.

(Part A) Get a “nice” description of moduli spaces. We want a description that we can really get our hands on, i.e. a parameterization of geometric/arithmetic/algebraic objects by orbits or representations.

(Part B) Count certain lattice points in regions of this space. Often involves some sieving.

(Part A is more algebraic, Part B more analytic)

### 1.2.1 Part A

What has worked in many cases has roughly been to describe the moduli stack of objects we care about as a quotient  $[V/G]$  with  $G$  a group and  $V$  a  $G$ -rep. More concretely, you may want the orbits  $V(\mathbb{Q})/G(\mathbb{Q})$  to correspond to  $\mathbb{Q}$ -objects and/or  $V(\mathbb{Z})/G(\mathbb{Z})$  to correspond to  $\mathbb{Z}$ -objects. Ideally, the  $G$ -invariants of  $V$  should correspond to some (natural) invariants of objects.

**Warning 1.2.1.** Part of the restriction of this method is that we've had to deal with representations which have simple invariant rings. •

How do you find these representations? It's a mix of things. One source is classical algebraic/geometric constructions which can be written in this language.

**Example.** Look at (integer) binary cubic forms up to linear transformations (up to (twisted action of)  $\mathrm{GL}_2(\mathbb{Z})$ ). These correspond to cubic rings over  $\mathbb{Z}$  (up to isomorphism). Can think of binary cubic forms as the representation  $\mathrm{Sym}^3(2)$ .

A binary cubic form cuts out a degree 3 subscheme of  $\mathbb{P}^1$  which gives a cubic ring (you don't get more information from the choice of embedding since the pullback of (1) will be the canonical sheaf it sounds). This associate matches up discriminates.

Davenport-Heilbronn exploited this correspondence to count cubic rings. △

Sounds like Melanie has a paper about looking at what binary  $n$ -ic forms parameterize. Sounds like we don't know how to parameterize all degree  $n$  rings in general, but Bjorn does have a paper on the moduli stack of degree  $n$  algebras (though w/o giving a presentation as a quotient associated to a group representation).

**Example.** Can look at pairs of ternary quad forms, i.e. at  $2 \otimes \mathrm{Sym}^2(3)$ . This turns out to give quartic rings.

Geometrically, a pair of ternary quadratic forms will be two conics in  $\mathbb{P}^2$  which intersect in a degree 4 subscheme.

By class field theory, these objects are (roughly) related to 2-torsion class group elements in cubic rings. To see the underlying cubic ring, we have this pencil of conics, and on this pencil, there are 3 degenerate conics (so get a degree 3 subscheme of  $\mathbb{P}^1$  parameterizing degenerate members of the pencil).  $\triangle$

### 1.2.2 Part B

First problem is to relate  $V(\mathbb{Q})/G(\mathbb{Q})$  to  $V(\mathbb{Z})/G(\mathbb{Z})$  (so only finitely many such things in a bounded region). This is often difficult.

Then, you want to count some lattice points in a fundamental domain for  $G(\mathbb{Z}) \curvearrowright V(\mathbb{R})$ . The first step here is to find a fundamental domain for  $G(\mathbb{Z}) \curvearrowright V(\mathbb{R})$ . So far, this is generally done in two steps

- Find fundamental domain for  $G(\mathbb{Z}) \curvearrowright G(\mathbb{R})$
- Find fundamental set for  $\mathbb{R}^\times \times G(\mathbb{R}) \curvearrowright V(\mathbb{R})$

Part of the reason for this is that early examples had  $G$  and  $V$  looking very similar (e.g. only one open orbit), so the first of the above was basically all you needed.

When doing these counts, can run into trouble if fundamental domain has a “cusp” (image a thing tail whose number of lattice points is poorly approximated by its volume). One innovation of Bhargava’s is to address this by “averaging.”

Another issue is that of reducible vs. irreducible orbits. Often times if many coefficients in  $V$  are 0, the corresponding orbit will be reducible, and you’ll want to ignore these. Very often, it turns out that the cusps have few irreducible points and the main body has few reducible points. Thus, to count irreducible points, can often ignore cusp and focus on main body.

This still leaves the problem of local conditions. These are generally handled by a sieve. The uniformity estimates coming up here can be hard.

To use this sort of thing to get a theorem about some sort of average, you might have to divide.

**Example** (Bhargava). The average size of  $\text{Cl}_K[2^\infty]$  for cubic fields  $K$  is

$$\begin{cases} 5/4 & \text{if totally real} \\ 3/2 & \text{otherwise.} \end{cases}$$

$\triangle$

Assuming  
I read the  
board cor-  
rectly

### 1.2.3 Combining w/ Circle Method

This started perhaps in Sam Ruth’s thesis. Levent Alpöge’s thesis and subsequent work has build on this.

Say you have a  $G$ -rep  $V$ . The idea is to count on  $(G\text{-invariant quadrics in } V)/G$ , i.e. pick some degree 2  $G$ -invariant and set it equal to 0. The circle method will let you count integral points on the main body of the quadric, and then you use separate arguments to say you can essentially ignore the cusps. Some applications

- (Saipy-Want, up to spelling) square-free values of  $\beta\alpha^4 + \alpha\beta^2$ .
- (Alpöge-Bhargava-Shnidman) sum of 2 cubes

Sounds like this is related to computing a 2-Selmer average in a certain family of elliptic curves.

- (Same authors) positive proposition of cubic fields are not monogenic, but not for local rings

Sounds like this is related to comparing a 2-Selmer average to a 3-Selmer average in a certain family of elliptic curves (in fact, the same family alluded to above).

#### 1.2.4 $\mathbb{Q}$ -invariant method

Tries to get around hardness of uniformity estimates by taking the representation you care about and embedding it into a larger representation. Used e.g. in Shankar-Shankar-Wang Counting elliptic curves by conductor (as well as at least 3 other papers, include at least 1 by H. et al.).

*Note 1.* Couldn't read what came next... Something about average size of  $\text{Cl}_K[2^\infty]$  for number fields vs. monogenic number fields (of fixed degree)

#### 1.2.5 Higher moments

These are hard to find parameterizations for. Need to parameterize e.g. two Selmer elements for the same elliptic curve.

#### 1.2.6 Vinberg theory

Ideas of Jack Thorn, B. Romona, and Jef Laga. Worked out a more uniform way of producing parameterizations and doing counts starting from a (simply laced) Dynkin diagram.

### 1.3 David Roe (MIT): Modular Curves and Finite Groups: Building Connections via Computations

Talking about two projects, both of which involved huge numbers of collaborators.

Not taking notes here, but will include a link to [alpha.lmfdb.org](http://alpha.lmfdb.org).

### 1.4 Robert Lemke Oliver (Tufts): Uniform exponent bounds on the number of primitive extensions of number fields

**Notation 1.4.1.** For any  $X \geq 1$ , let

$$\mathcal{F}(X) := \{K/\mathbb{Q} : |\text{Disc } K| \leq X\}.$$

**Theorem 1.4.2** (Hermite-Minkowski).  $\mathcal{F}(X)$  is finite for every  $X \geq 1$

**Question 1.4.3.** What is  $\#\mathcal{F}(X)$  as  $X \rightarrow \infty$

**Theorem 1.4.4** (Minkowski). There is an absolute constant  $c > 1$  such that  $|\text{Disc}(K)| \geq c^{[K:\mathbb{Q}]}$

There are refinements due e.g. to Serre, Stark, Odlyzko. Also, if  $K \in \mathcal{F}(X)$ , then  $[K : \mathbb{Q}] = O(\log X)$ .

Upshot: If  $\mathcal{F}_n(X) := \{K \in \mathcal{F}(X) : [K : \mathbb{Q}] = n\}$ , then  $\mathcal{F}(X) = \bigcup_{n \leq c' \log X} \mathcal{F}_n(X)$ .

**Question 1.4.5.** Given  $n$ , how does  $\#\mathcal{F}_n(X)$  behave as  $X \rightarrow \infty$ ?

**Conjecture 1.4.6** (Folklore; Linnik, Davenport?). There is a constant  $c_n > 0$  such that  $\#\mathcal{F}_n(X) \sim c_n X$  as  $X \rightarrow \infty$ .



(Often attributed to Linnik. Maybe early appeared in unpublished lecture notes of Davenport) This is known if

- $n = 2$  (Classical)
- $n = 3$  (Davenport-Heilbronn)
- $n = 4$  (Bhargava; Cohen-Diaz y Diaz-Olivier)
- $n = 5$  (Bhargava)
- $n \geq 6$  (Open)

Note that the conjecture in particular implies  $\#\mathcal{F}_n(X) = O_n(X)$ . Is this weaker conjecture known?

- Schmidt:  $\#\mathcal{F}_n(X) = O_n\left(X^{\frac{n+2}{4}}\right)$
- Ellenberg-Venkatesh:  $\#\mathcal{F}_n(X) = O_n\left(X^{\exp(c\sqrt{\log n})}\right)$
- Couveignes:  $\#\mathcal{F}_n(X) = O_n(X^{c(\log n)^3})$
- Lo-Thorn:  $\#\mathcal{F}_n(X) = O_n(X^{c(\log n)^2})$  (Best known)

None gives

**Conjecture 1.4.7** (“Uniform exponent conjecture”). *There is  $C \geq 1$  such that  $\#\mathcal{F}_n(X) = O_n(X^C)$  for every  $n \geq 6$*

For which families of fields can we prove the uniform exponent conjecture?

- We will stratify based on Galois groups of fields
- We’ll work over a number field, bounding relative extensions  
(We do so uniformly; hidden in this talk for simplicity)
- Reduce the general problem to that of bounding almost simple, primitive extensions
- We prove the strongest known bounds on almost all such families
- These bounds resolve the uniform exponent conjecture for families w/ Galois groups solvable, of Lie type w/ bounded rank, or sporadic.

Let’s take a second to be precise how we think about “Galois groups of non-Galois extensions.” Let  $K/k$  be a (possibly non-Galois) extension of number fields with degree  $n$ , and let  $\tilde{K}/k$  be the normal closure of  $K/k$ . There are  $n$  embeddings  $K \hookrightarrow \tilde{K}$  over  $k$ , on which  $\text{Gal}(\tilde{K}/k)$  acts faithfully and transitively. This gives an embedding  $\pi : \text{Gal}(\tilde{K}/k) \hookrightarrow S_n$  that’s canonical up to conjugation. The image  $\text{im}(\pi)$  is a transitive subgroup  $G \subset S_n$ .

**Definition 1.4.8.** We say  $K/k$  is a  $G$ -extension if  $\text{im}(\pi) \simeq_{\text{perm}} G$ , and write

$$\mathcal{F}_{n,k}(X; G) := \{K/k \text{ a } G\text{-extension} : |\text{Disc}(K/\mathbb{Q})| \leq X\}.$$

When  $k = \mathbb{Q}$ , we drop it from the above notation. ◇

**Example.**  $\mathcal{F}_3(X) = \mathcal{F}_3(X; C_3) \cup \mathcal{F}_3(X; S_3)$ .  $\triangle$

**Question 1.4.9.** *What can we say about bounds on  $\#\mathcal{F}_n(X; G)$ ? Can we resolve the uniform exponent conjecture for some family of  $G$ ?*

In recent work on van der Waerden's conjecture, Bhargava made use of the “trivial” inequality

$$\#\mathcal{F}_n(X; G) \leq \#\mathcal{F}_n(X) = O_n\left(X^{c(\log n)^2}\right)$$

for primitive groups  $G \neq S_n, A_n$ .

**Definition 1.4.10.**  $G$  is **primitive** if it preserves no nontrivial partition of  $\{1, \dots, n\}$ . Equivalently, any  $G$ -extension  $K/k$  has no proper subextensions.  $\diamond$

**Question 1.4.11** (Bhargava). *For primitive  $G \neq S_n, A_n$ , are there better bounds than  $\#\mathcal{F}_n(X; G) = O_n(X^{c(\log n)^2})$ ?*

Note that (almost) simple groups are primitive, and the most common simple groups are those of Lie type.

**Theorem 1.4.12.** *There is an absolute constant  $C > 0$  such that if  $G$  is any finite almost simple classical group of Lie type with rank  $m$  (e.g.  $\mathrm{PSL}_{m+1}(\mathbb{F}_q)$ ), then  $\#\mathcal{F}_n(X; G) = O_n(X^{Cm})$ .*

(This statement holds for any permutation representation of these groups. It's most interesting for the minimal degree permutation representation.)

This is completely explicit, e.g.

$$\#\mathcal{F}_{q+1}(X; \mathrm{PSL}_2(\mathbb{F}_q)) = O_q(X^{4.5})$$

for any prime power  $q$ .

This theorem resolves the uniform exponent conjecture for such  $G$  as  $q \rightarrow \infty$  with  $m$  fixed. The worth case is  $m \rightarrow \infty$  with  $q$  fixed. This yields  $\#\mathcal{F}_n(X; G) = O_n(X^{c \log n})$  which still improves the earlier bound.

Let's look at the example for solvable groups.

**Theorem 1.4.13.** *If  $G$  is solvable, then  $\#\mathcal{F}_n(X; G) = O_n(X^{14.5})$ .*

**Corollary 1.4.14.** *The number of monic irreducible polynomials  $w$ /coeff's  $\leq H$  and solvable Galois group is  $O\left(H^{\frac{29}{31}n + \frac{294}{961}}\right)$ .*

The proof does not use class field theory in any way. Class field theory by itself does not give  $X^{O(1)}$  in general.

The method could maybe give  $\#\mathcal{F}_n(X; G) \stackrel{?}{=} O_n(X^5)$ .

**Question 1.4.15.** *Can this be combined with CFT to go further?*

A final example: Monstrous extensions.

**Theorem 1.4.16.** *Let  $\mathbb{M}$  be the Fischer-Griess monster group in its minimal degree  $n \approx 9.7 \cdot 10^{19}$  permutation representation. Then,*

$$\#\mathcal{F}_n(X; \mathbb{M}) = O(X^{8.5}).$$

Previous best bound (LO-Thorne):  $\#\mathcal{F}_n(X; \mathbb{M}) = O(X^{1462})$ .

These three examples can be put into a general framework, but it's probably more instructive to consider the idea of the proof next.

Connections w/ geometry of numbers: Schmidt's theorem

**Theorem 1.4.17** (Schmidt). *For any  $n \geq 2$ ,  $\#\mathcal{F}_n(X) = O_n(X^{(n+2)/4})$ .*

*Proof Sketch.*

- Any  $K \in \mathcal{F}_n(X)$  has some (nonzero)  $\alpha \in \mathcal{O}_K$  w/  $\text{Tr}_{K/\mathbb{Q}} \alpha = 0$  and  $|\alpha|_v \ll X^{\frac{1}{2n-2}}$  for all  $v \mid \infty$ .
- The minimal polynomial  $f_\alpha(x) = x^n + a_2x^{n-2} + \dots + a_n$  satisfies  $|a_i| \ll_n X^{\frac{i}{2n-2}}$ .
- As  $K$  and  $\alpha$  vary, there are  $O_n\left(X^{\frac{i}{2n-2}}\right)$  choices in  $\mathbb{Z}$  for the coefficient  $a_i$ .
- Multiplying the number of choices gives Schmidt's bound. ■

To improve this (idea of Ellenberg-Venkatesh), coefficients  $a_i$  of  $f_\alpha(x)$  are invariants of its roots  $\alpha_1, \dots, \alpha_n$ . There are more invariants of small degree attached to  $r$ -tuples of integers in  $\mathcal{O}_K$ .

**Theorem 1.4.18** ( $r = 2$ , LO-Thorne). *The first  $2n$  "mixed traces"*

$$\text{Tr}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \dots + \alpha_n^i \beta_n^j, \quad i + j \leq 2\sqrt{n}$$

*are algebraically independent.*

(Missed stuff because slide talks are fast...)

General setup is to look at mixed traces of  $r$ -tuples, say of degree  $d$ .

**Theorem 1.4.19** (LO-Thorne). *If there are at least  $rn$  "mixed traces"  $\text{Tr}(\alpha_1^{i_1} \dots \alpha_r^{i_r})$  of degree  $d$ , then there is a set of size  $rn$  that is algebraically independent. If so, then  $\#\mathcal{F}_n(X) = O_n(X^{rd})$ .*

Optimize parameters w/  $r, d \approx \log n$  to get result.

How to incorporate Galois structure? If  $G \neq S_n, A_n$  is primitive, then  $G$  is very small, so should already have lots of small invariants even when  $r = 1$ .

**Theorem 1.4.20** (Simplified version). *Suppose  $G \subset S_n$  is transitive and that there are  $n$  algebraically independent  $G$ -invariant polynomials in  $\mathbb{Z}[\alpha_1, \dots, \alpha_n]$  w/ degree at most  $d$ . Then,  $\#\mathcal{F}_n(X; G) = O(X^d)$ .*

**Theorem 1.4.21.** *If  $G$  is primitive and almost simple\*, then there is a set of  $n$  algebraically independent  $G$ -invariants in  $\mathbb{Z}[\alpha_1, \dots, \alpha_n]$  of degree at most  $C^{\frac{\log|G|}{\log n}}$  for some absolute  $C > 0$ .*

*Remark 1.4.22.* Orbit-stabilizer suggests  $O\left(\frac{\log|G|}{\log n}\right)$  is natural bound. ◦

**Example.**  $G = C_p$  cyclic of prime order  $p$ . Then,  $\log|G|/\log n = \log p/\log p = 1$ .

For  $i \leq p$ , let  $f_i := (\alpha_1^2 \alpha_i)^G$  ( $G$ -trace, sum of monomials in  $G$ -orbit). These are algebraically independent. Consider matrix of partials

$$\left( \frac{\partial f_i}{\partial \alpha_j} \right)_{i,j=1}^p.$$

If  $\det \neq 0$ , then the  $f_i$  are algebraically independent. If you write out the matrix explicitly, you'll see an  $\alpha_1^2$  in every diagonal entry, but every other entry is at most linear in  $\alpha_1$ . Thus, can't get cancellation, so determinant is non-zero. △

The key ingredient about is that the stabilizer of 1 (of  $\alpha_1$ ) is trivial.

A **base** of  $G$  is a smallest set of points whose intersection of stabilizers is trivial. We define  $\text{base}(G)$  to be the order of a base.

**Example.**  $\text{base}(C_p) = 1$  and  $\text{base}(S_n) = n - 1$ .  $\triangle$

**Theorem 1.4.23.** *Any  $G$  has a set of  $n$  algebraically independent invariants of degree at most  $\frac{1}{2}(\text{base}(G) + 1)(\text{base}(G) + 2)$ .*

**Theorem 1.4.24** (“Pyber’s conjecture”; Duyan-Halasi-Maroti). *If  $G$  is primitive, then  $\text{base}(G) = O(\log |G| / \log n)$ .*

Base is frequently bounded for primitive groups.

**Slogan.** Primitive groups are usually small.

(Some more stuff I missed)

The above essentially handles (almost?) simple groups. What about primitive groups? These are classified by a theorem of O’Nan-Scott. They come in 5 types I won’t bother writing down. I will mention that one type is groups of diagonal, product, or twisted wreath types; these have much smaller faithful representations and one gets  $\#\mathcal{F}_n(X; G) = O_n(X^{C(\log n)^2/\sqrt{n}})$ .

Imprimitive groups are always subgroups of wreath products of primitive groups.

## 1.5 Lightning Talks

Each talk gets 10 minutes. Try not to interrupt. There will be a 2 minute period for a lightning question. At the end, the speakers will gather in a “cloud” for the “lightning” where you can come up to ask questions.

### 1.5.1 Alexander Betts (Harvard): Computing Local Heights for Quadratic Chabauty

(joint w/ Juanita Duque-Rosero, Sachi Hashimoto, and Pim Spelier)

Motivating question: How do we compute rational points on curves in practice?

Let  $X/\mathbb{Q}$  be a smooth projective curve of genus  $g \geq 2$  and  $b \in X(\mathbb{Q})$  a basepoint. To every trace zero correspondence  $Z \subset X \times X$ , one has an associated  $p$ -adic (Coleman-Gross) height function

$$h_Z : X(\mathbb{Q}) \longrightarrow \mathbb{Q}_p,$$

...

It’s very quickly become clear that these talks are too fast to take notes on...

### 1.5.2 Juanita Duque-Rosero: Triangular Modular Curves

## 2 Jan 12

### 2.1 Wanlin Li (WashU): Ordinary and Basic Reductions of Abelian Varieties

(joint w/ Farfain, Mantovan, Pries, Tang and w/ Mantovan, Pries, Tang) [both up to spelling]

Let's begin by recalling the difference between ordinary and supersingular elliptic curves. Say  $E/\mathbb{F}_q$  is an elliptic curve. Then,

$$\#E(\mathbb{F}_q) + 1 + q - a,$$

where  $a$  is the trace of Frobenius on the ground field. We say  $E$  is **ordinary** if  $p \nmid a$  while  $E$  is **supersingular** if  $p \mid a$ .

Can ask, how many elliptic curves are supersingular? Can make sense of this question even over  $\overline{\mathbb{F}}_p$ . In the  $j$ -line  $\mathbb{A}_j^1$ , there's a dense open of  $j$ -invariants of ordinary curves, but only finitely many (in fact,  $\approx p/12$ ) supersingular  $j$ -invariants. From the moduli perspective, supersingular curves are rare.

Let's look from a reduction perspective. Say  $E/L$  an elliptic curve over a number field. Among the primes of  $L$ , how many have ordinary/supersingular reduction?

**Answer** (CM case). If  $E$  is CM, we have a complete answer, following from work of Shimura-Taniyama (1961). Let  $v$  be a prime of  $L$  above a rational prime  $p$ . Say  $E$  has CM by an order in  $\mathbb{Q}(\sqrt{-d})$ . Then,  $E$  has ordinary reduction at  $v$  exactly when  $p$  splits in  $\mathbb{Q}(\sqrt{-d})$ . This tells us that, over  $L(\sqrt{-d})$ , the ordinary primes have density 1. ★

**Answer** (non-CM case). First knowledge in this direction comes from a theorem of Serre.

**Theorem 2.1.1** (Serre, 1977). *For  $E$  non-CM, the density of ordinary primes is 1.*

**Theorem 2.1.2** (Elkies, 1987 + 1989). *When  $L \hookrightarrow \mathbb{R}$ ,  $E$  has infinitely many supersingular primes.* ★

The goal today is to generalize these two theorems to higher dimensional abelian varieties.

**Example.** Can look at Jacobians of the family

$$C_t : y^5 = x(x-1)(x-t)$$

of genus 4 curves (compare above to Legendre family). Note that the moduli point of this curve is determined by the “ $j$ -function”

$$j_0(t) := \frac{(t^2 - t + 1)^2}{t^2(t-1)^2}. \quad \triangle$$

**Theorem 2.1.3** (CLMPT). *For any  $C/L$  with equation  $y^5 = x(x-1)(x-t)$  over  $\overline{L}$ , if its Jacobian has no CM, then the set of  $\mu$ -ordinary primes has density 1. Over  $L(\zeta_5)$ , then its set of ordinary primes had density 1.*

**Remark 2.1.4.** By no CM above, we mean  $\text{End}_{\mathbb{Q}}^0 \text{Jac}(C) \cong \mathbb{Q}(\zeta_5)$ . ○

**Theorem 2.1.5** (LMPT). *Consider a (smooth, proper) curve  $C : y^5 = x(x-1)(x-t)$  in this family. Impose the local conditions*

- $j_0(t) \in \mathbb{Q} \cap [0, 27/4]$ .

- $C$  has bad reduction at 5.

Then,  $\text{Jac}(C)$  has infinitely many non  $\mu$ -ordinary primes.

**Question 2.1.6** (Audience). *Would one expect the theorems of Serre and Elkies to be true for any abelian variety over any number field?*

**Answer.** Serre conjectured there's always a positive density of ordinary primes. We know less about supersingular primes. ★

**Question 2.1.7** (Audience). *Would we expect there to be an abelian variety where the number of supersingular primes is finite but not nonzero?*

**Answer** (Paraphrased; lots of people said things, I may be misrepresenting them). Sounds like every abelian variety is expected to have non-ordinary primes, and the number of such should be infinite. However, if you strictly mean supersingular, then it's less clear. ★

### 2.1.1 Newton polygon for abelian varieties

Let  $A/\mathbb{F}_q$  be an abelian variety. Its **Newton polygon** is the Newton polygon of the characteristic polynomial of Frobenius. You can think of this as a multiset of  $v_q(\lambda_i)$ , the  $q$ -adic valuations of Frobenius eigenvalues  $\lambda_1, \dots, \lambda_{2g}$ . These Newton polygons all taken together form a poset which gives a stratification of  $\mathcal{A}_{g, \overline{\mathbb{F}}_p}$  (Oort, 2001).

**Definition 2.1.8.** We say  $A$  is **ordinary** if  $v_q(\lambda_1) = \dots = v_q(\lambda_g) = 0$  (the other half have valuation 1).  $A$  is **supersingular** if  $v_q(\lambda_i) = 1/2$  for all  $i$ . ◇

**Example.** Say  $g = 2$ , so  $\dim \mathcal{A}_2 = 3$ . Wanlin proceeded to draw a picture of  $\mathcal{A}_2$  along with its Oort stratification. △

Say  $C : y^5 = x(x-1)(x-t)$  from our favorite family satisfies  $\text{End}_{\mathbb{Q}}^0 \text{Jac}(C) \cong \mathbb{Q}(\zeta_5)$ . Consider automorphism  $(x, y) \mapsto (x, \zeta_5 y)$ . The Torelli image of this family lies in a PEL-type Shimura subvariety  $S \subset \mathcal{A}_4$  ( $\mathcal{A}_4$  has 8 Newton polygons). From the work of Niehmann-Wedhorn (spelling) in 2013, we know the Newton strata of  $S$ . For each  $p \neq 5$ ,  $S_{\overline{\mathbb{F}}_p}$  only has two Newton strata.

*Remark 2.1.9.* The family under consideration is special in that its Jacobians are parameterized by a Shimura curve. ○

**Definition 2.1.10.** A member of the family is  **$\mu$ -ordinary** if it belongs to the open Newton stratum of  $S$ . It's **basic** if it belongs to the other stratum. ◇

**Fact.** If  $p \equiv 1 \pmod{5}$ , then  $\mu$ -ordinary is ordinary. Basic had Newton polygon  $\text{ord}^2 \oplus \text{ss}^2$ , i.e has  $(0, 0, 1, 1, 1/2, 1/2, 1/2, 1/2)$ .

If  $p \equiv 2, 3, 4 \pmod{5}$ , then  $\mu$ -ordinary is not ordinary and basic is supersingular.  $\mu$ -ordinary is  $(1/4, 1/4, 1/4, 1/4, 3/4, 3/4, 3/4, 3/4)$  when  $p \equiv 2, 3 \pmod{5}$  and is  $\text{ord}^2 \oplus \text{ss}^2$  if  $p \equiv 4 \pmod{5}$ .

*Remark 2.1.11.* When you base change to include  $\zeta_5$  in your field, the primes which are not  $1 \pmod{5}$  become density zero, so can be ignored. ○

### 2.1.2 Ordinary reductions

**Conjecture 2.1.12** (Serre). *For any  $A/L$ , the set of ordinary primes has positive density.*

**Theorem 2.1.13** (Katz 1982, Sawin 2016). *Say  $g = 2$ . They resolve Serre's conjecture w/ explicit density.*

(This uses work of Fité-Kedlaya-Rutger-Sutherland 2016)

For  $g \geq 3$ , this are yet to be resolved

- Pink (1998) Certain  $A$  w/  $\text{End}_{\overline{\mathbb{Q}}} A \cong \mathbb{Z}$
- Fité (2021) Certain  $A$  w/ non-trivial  $\text{End}_{\overline{\mathbb{Q}}} A$
- CLMPT Certain  $A$  w/ non-trivial  $\text{End}_{\overline{\mathbb{Q}}}^0 A \cong F$ , a CM field w/ action have signature  $(1, n-1)$  at one place, definite at other places.

*Note 2.* Got distracted for a moment, and when I snapped back to, I heard, "... and this is also the general strategy for our case." Sounds like I missed something important...

### 2.1.3 Infinitely many basic primes

Consider the curve  $C : y^5 = x(x-1)(x-t)$  ( $t$  fixed) with  $j$ -invariant  $j_C \in \mathbb{Q} \cap [0, 27/4]$  and  $C \bmod 5$  (?) is singular with reduction looking like a nodal union of 2 genus 2 curves.

To produce supersingular primes, idea is to produce CM curves whose reduction mod  $p$  agrees with the reduction of  $C$  (or  $\text{Jac}(C)$ ?) mod  $p$ . Since we know when CM curves have supersingular reduction, this makes things tractable. To get infinitely many such primes, construct the CM curve s.t. it has non-SS reduction at all such primes produced thus far.

**Construct CM cycles** Consider  $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})/\mathbb{Q}$  Choose  $\lambda \in F_0 = \mathbb{Q}(\sqrt{5})$  which is totally real. Let  $E$  be the compositum of  $\mathbb{Q}(\zeta_5)$  and  $\mathbb{Q}(\sqrt{-\lambda})$ . Then,  $\text{Jac}(C_\lambda)$  has CM by  $E$ . The point of this family is that we can determine exactly when such a Jacobian has basic reduction. It comes from Legendre associated to the quadratic extension  $F_0(\sqrt{-\lambda})/F_0$ . In particular, if  $p$  is non-split, then  $C_\lambda \bmod p$  is basic.

**Real CM points in  $S$**  This  $S$  turns out to be a triangular modular curve, in fact

$$S(\mathbb{C}) \cong \Delta(2, 3, 10) \backslash \mathcal{H}.$$

A fundamental domain looks like (two copies of?) a triangle, say with vertices  $P, Q, R$ . I can't really type and keep up with the description at this point, but Wanlin can identify the CM points (and their  $j_0$ -invariants) in this fundamental domain.

Sounds like the archimedean local condition  $j \in [0, 27/4]$  comes from them having a better understanding of one side of this triangle than the others. Also, sounds like all CM curves have supersingular reduction at 5, so they require  $C$  to have bad reduction there to make sure it doesn't collide with a (supersingular) CM curve.

## 2.2 Edgar Costa (MIT): Computing Isogeny Classes of Principally Polarized Abelian Surfaces Over the Rationals

(joint w/ Raymond van Bommel, Shiva Chidambaram, and Jean Kieffer)

An **isogeny** between two abelian varieties is a surjective homomorphism  $\varphi : A \rightarrow B$  with  $\# \ker \varphi < \infty$ . The **isogeny class** is obtained by taking quotients by finite rational subgroups. Two abelian varieties in the same isogeny class share many properties, e.g.

- $L$ -function
- Mordell-Weil rank
- Endomorphism algebra  $\text{End}(A) \otimes \mathbb{Q}$

A natural way to represent an isogeny class is by its irreducible isogeny graph. What shape can these take?

Can explore isogeny graphs of elliptic curves in the LMFDB

- all degrees of irreducible isogenies are primes
- Not all primes show up

Mazur:  $\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$

- the largest isogeny graph has size 8
- Not many graphs show up. Ignoring degrees, only 10 of them

(Chiloyan-Lozano-Robledo 2021) these are all the graphs

Little is known away from elliptic curves over  $\mathbb{Q}$ . LMFDB has genus 2 curves w/ small minimal absolute discriminant. These are grouped by isogeny class of their Jacobian. However, the isogeny classes are known to not be complete.

**Problem 2.1.** *Given an abelian surface  $A$ , compute its isogeny class. Actually, given a principally polarized abelian surface, compute all other principally polarized abelian surfaces in its isogeny class.*

- (1) List irreducible isogeny types
- (2) List the possible degrees for each type
- (3) Search for all isogenies of a given type and degree
- (4) Reapply as needed

Irreducible isogeny types depend on  $\dim A$  and  $\text{End}(A)^\dagger$  (ring fixed by Rosatti involution). There is a bijection

... (Too much on this slide to write it all down in real time) ...

At this point, I'm gonna stop taking notes, and just listen...

## 2.3 DZB

Slides on his website.

First few slides went by fast, so I'll just listen and not take notes...






Question:  
why?

Answer:  
Consider  
composition  
with dual  
isogeny.

TODO: Add  
link



### 3 List of Marginal Comments

	If I'm not mistaken, these satisfy $K_X^2 = 0$ . . . . .	2
	Assuming I read the board correctly . . . . .	5
	Question: why? . . . . .	14
	Answer: Consider composition with dual isogeny. . . . .	14
	TODO: Add link . . . . .	14

# Index

$\mu$ -ordinary, 12

(-1)-curve, 1

base, 10

basic, 12

Fano, 2

index, 2

isogeny, 14

isogeny class, 14

minimal, 1

Newton polygon, 12

ordinary, 11, 12

primitive, 8

supersingular, 11, 12

Uniform exponent conjecture, 7