AWS 2023: Special Point Problems

Jacob Tsimerman

January 26, 2023

Contents

1 Lecture #1: Roots of Unity and Langs Conjecture

1.1 Problem formulation and motivation

We begin by discussing at length the prototypical special point problems, Lang's conjecture. The context for this conjecture is that we shall be working in $(\mathbb{C}^\times)^n$ and we shall be interested in points all of whose co-ordinates are roots of unity. We could call these *special points*, but they already have a name: they are the torsion points if we think of $(\mathbb{C}^\times)^n$ as (the complex points of) an algebraic group.

The basic question we are trying to answer is: *What kinds of polynomials have 'many' solutions in torsion points?*

There are of course lots of examples one can cook up stemming from the fact that products of roots of unity are roots of unity. Thus, $x^m y^n - 1$ is an example for any non-zero pair of integers (m, n). In other words, any polynomials which express a multiplicative relations constitute an example.

One could think of this as yet another instance of trying to relate multiplication and addition to each other: The torsion points are defined purely multiplicatively and without reason to think otherwise, we view additive relations to be 'coincidental'. Now this is not to say that these never happen: In fact, for any finite set of torsion points one can come up with arbitrarily many polynomial relations they all satisfy. However, an easy heuristic is that while coincidences can happen, they should be rare, and in this case we take that to mean 'finite'. The basic instance of Lang's conjecture is therefore the following:

Conjecture 1.1 (Lang for $n = 2$)**.** *Let $f(x, y) \in \mathbb{C}[x, y, x^{-1}, y^{-1}]$[1] be an irreducible polynomial. If $f(x, y) = 0$ has infinitely many zeroes in roots of unity, then up to a unit f is equal to $x^m y^n - \eta$ for some relatively prime pair of integers (m, n) and a roof of unity η.*

In higher dimensions a couple of things change: First, it becomes way more convenient to use the language of algebraic varieties then systems of polynomial equations, so we make a slight adjustment in looking for varieties which contain many torsion points. Secondly, we have to be wary of the following situation: You could have a surface $S \subset (\mathbb{C}^\times)^3$ which has no 'multiplicative structure', but which contains for instance the diagonal curve $C = \{(x, y, z) \mid x = y = z\}$. Then S will contain infinitely many torsion points stemming from C, but this is not really expressing anything about S. Thus, we change the statement from containing infinitely many torsion points to containing a *Zariski-Dense* set of torsion points (Recall that the Zariski topology is a very coarse topology in which the only closed sets are closed subvarieties, and so the Zariski-closure of a set is the smallest subvariety which contains it).

We are now almost ready to formulate Langs conjecture. What we are missing is a precise statement for what a 'multiplicative' variety should be in high dimensions. Luckily, the group structure of $(\mathbb{C}^\times)^n$ provides such an answer:

Definition 1.1.

1. A closed subvariety $T \subset (\mathbb{C}^\times)^n$ is a *subtorus* if it is an irreducible subvariety which is also a subgroup: I.e. an irreducible group subvariety.
2. A closed subvariety $V \subset (\mathbb{C}^\times)^n$ is a *torus coset* is it is of the form zT where T is a subtorus and $z \in (\mathbb{C}^\times)^n$
3. A closed subvariety $V \subset (\mathbb{C}^\times)^n$ is a *torsion coset* is it is of the form zT where T is a subtorus and $z \in (\mathbb{C}^\times)^n$ is a torsion point.

Here are some exercise to get you used to these structures:

Exercise 1.2.

1. Prove a torus coset is a torsion coset iff it contains a torsion point
2. Prove that a torsion coset contains a Zariski-dense set of torsion points.
3. We can identify $\mathbb{Z}^n \cong \mathrm{Hom}\big((\mathbb{C}^\times)^n, \mathbb{C}^\times\big)$ with the set of Monomials by sending $(a_1, \ldots, a_n) \to \prod_{i=1}^{n} x_i^{a_i}$. Every subgroup $G \subset \mathbb{Z}^n$ defines an algebraic subgroup $T_G \subset (\mathbb{C}^\times)^n)$ by setting
$$T_G := \{z \mid \forall g \in G, g(z) = 1\}.$$
Prove that T_G is a subtorus iff G is saturated in $\mathbb{Z}^n$ (i.e. $\mathbb{Z}^n/G$ is torsion free) and that all subtori arise uniquely in this way.

[1] Note that as we are working in $\mathbb{C}^\times$ is is natural to work with Laurent polynomials.

4. Find a natural bijection between torsion cosets, and pairs (G, f) where $G \subset \mathbb{Z}^n$ is a subgroup, and $f \in \mathrm{Hom}((\mathbb{Z}^n/G)_{tor}, \mathbb{C}^\times)$.

We can now finally formulate Langs conjecture:

Conjecture 1.2. *Let $V \subset (\mathbb{C}^\times)^n$ be an irreducible subvariety, and suppose that that torsion points in V are Zariski-dense. Then V is a torsion coset.*

1.2 Galois orbits and Bezouts theorem

The first observation we make is that though Conjecture 1.2 is formulated for complex varieties, it is immediately reducible to the case of varieties defined over number fields. This is the case simply because all the roots of unity, and hence the torsion points, are defined over $\overline{\mathbb{Q}}$ and thus so is their Zariski closure V. Therefore, V is defined over a number field K. From now on we implicitly make this assumption.

One way in which this setting is the easiest is the precise control we have on the Galois action on roots of unity. Recall the following:

For each n, let $\zeta_n \in \overline{\mathbb{Q}}$ be a primitive $n'th$ root of unity and for convenience assume that $\zeta_{mn}^m = \zeta_n$. Let $\mathbb{Q}_{\mathrm{cyc}} := \bigcup_n \mathbb{Q}(\zeta_n)$ be the Cyclomotic field. Then

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

where $a \leftrightarrow \sigma_a$ acts via $\sigma_a(\zeta_n) = \zeta_n^a$. Taking the inverse limit this gives us an isomorphism

$$\hat{\mathbb{Z}}^\times \cong \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}).$$

The basic role played by the Galois group is the following observation: *If a variety V contains a torsion point, it must contain all of its Galois conjugates as well.* This makes the assumption much stronger because we can then try to make the following sorts of arguments:

- It is hard to contain too many torsion points of the same order.
- The torsion points 'repel' each other, so once you contain one it is hard to contain others.
- The torsion points have some kind of transcendental complex or p-adic structure, so our variety 'looks linear' from a certain point of view.

In this case, we have the following basic asymptotic estimates

Proposition 1.3. *Let K be a fixed number field and $\vec{\eta} = (\eta_1, \ldots, \eta_n) \in (\mathbb{C}^\times)^n$ be a torsion point of order m. Then*

1. $\#\mathrm{Gal}(\overline{\mathbb{Q}}/K) \cdot \vec{\eta} \geq \varphi(m) \cdot [K : \mathbb{Q}]^{-1}$
2. *There is a prime number p of size $O(\log m)$ such that $(\vec{\eta})^{p^{[K:\mathbb{Q}]!}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/K) \cdot \vec{\eta}$*

Proof. For the first part, first note that the statement is an exact equality if $K = \mathbb{Q}$ by the description given above. In the case where $K \neq \mathbb{Q}$ the statement follows from the fact that $\mathrm{Gal}(\overline{\mathbb{Q}}/K) < \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a subgroup of index $[K : \mathbb{Q}]$.

For the second part, we note that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is surjecitve onto $(\mathbb{Z}/m\mathbb{Z})^\times$, and so contains the element $\overline{p}$ whenever $(p, m) = 1$. It is elementary that such a prime number p exists of size $O(\log m)$ (Ex: Prove this using the prime number theorem). It is now sufficient to note that the $[K : \mathbb{Q}]!$ power of any element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ lies in $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. □

We can now give our first proof of Lang's conjecture:

Proof. of Conj 1.2: We first give the proof for the case where $n = 2$. So suppose that $C \subset (\mathbb{C}^\times)^2$ is an irreducible curve, which contains infinitely many torsion points. As above, we can assume that C is defined over a number field K. Let C be a degree d curve, when considered as a subset of $\mathbb{P}^2$ in the natural way.

Let $z \in C$ be a torsion point of exact order m. By Proposition 1.3, for large m we may find an integer N of size $(\log m)^{O(1)}$ and relatively prime to N such that $z^N \in G_K \cdot z$ and is therefore also on C.

Lemma 1.4. *Let $[N]C$ be the irreducible curve obtained by pushing forward C along the multiplication by N map. For large enough m, we have $C = [N]C$.*

Proof. Note that $z^N \in [N]C$, and that by construction $z^N \in G_K \cdot z$. Therefore, z is also in $[N]C$ (note that the curve $[N]C$ is also defined over K). It follows that $G_K z \subset C \cap [N]C$. Now assume for the sake of contradiction that $C \neq [N]C$ and we derive a contradiction by comparing a lower and upper bound for $\#(C \cap [N]C)$:

- **Upper bound:** The degree of $[N]C$ can be computed by intersecting with a generic line L. Thus

  $$\deg[N]C = \#([N]C \cap L) \leq C \cap [N]^*L \leq dN$$

  where the final inequality follows by Bezouts theorem. Thus, we conclude that

  $$\#(C \cap [N]C) \leq \deg C \deg[N]C \leq d^2 N.$$

- **Lower Bound** On the other hand, we know that the intersection contain $G_K \cdot z$ and thus by Proposition 1.3 we have

  $$\#(C \cap [N]C) \geq \#G_K \cdot z \geq [K : \mathbb{Q}]^{-1} \varphi(m)$$

We now get a contradiction by observing that $\varphi(m) = m^{1+O(1)}$ which grows faster than $(\log m)^{O(1)}$. □

We now complete the proof using the following lemma:

Lemma 1.5. *Suppose that $C \subset (\mathbb{C}^\times)^2$ is an irreducible curve such that $C = [N]C$ for some positive integer $N > 1$. Then C is a torsion coset.*

Proof. If C is a fiber than the statement is clear so we assume this is not the case. Pick a root of unity $a \in \mathbb{C}$ such that $\pi_1^{-1}(a) \cap C$ is non-empty, and consists of smooth points of C. Then by replacing N by one of its powers we may assume that $a^N = a$. Then there are only finitely many points in $C \cap \pi_1^{-1}(a)$ which must be mapped to each other by the N'th power map. By replacing N by one of its powers and changing b we may again assume that $b^N = b$. Next, replacing C by $(a,b)^{-1} \cdot C$ we may assume that $\mathrm{Id} = (1,1) \in C$ and is a smooth point.

We consider the analytic germ of C around Id. Consider the inverse image D of C around $(0,0)$ under the exponential map $(z,w) \to (e^z, e^w)$. This is a local isomorphism, and C being locally invariant under the N'th power map means D is invariant under $(z,w) \to (Nz, Nw)$. We may write the defining equation for D as a power series in z, w, and the invariance condition means that the power series is homogenous. Moreover, since D is smooth by assumption it must be linear, and thus D is the germ of a line.

As an alternative argument, one may notice that $M \cdot D$ looks more and more linear as $M \to \infty$, as we are 'zooming further and further in'. Thus $D = N^i D$ for any i which becomes linear as $i \to \infty$ and therefore D is a line.

Exercise 1.6. Flesh this out into a complete proof!

Hence C is locally analytically defined by $x = y^\alpha$ for some complex number α. Since C is algebraic it follows that α must be rational and the lemma is proved.

□

□

1.2.1 Generalization to higher dimensions

We explain how to generalize this proof to the case of $V \subset (\mathbb{C}^\times)^n$. The ideas are the same, but the geometric book-keeping can add some complexity, and one must also take into account that V might contain positive dimensional torsion cosets.

The reason the proof doesn't immediately generalize is that now there are more options other than $V = [N]V$ and $V \cap [N]V$ is finite. The intersection could be of intermediate dimensions. Before proceeding we list a very useful generalization of Bezout's theorem due to Fulton[10, Theorem 12.3]:

Theorem 1.7. *Let $V_1, \ldots, V_n$ be irreducible subvarieties of projective space of degrees $d_1, \ldots, d_n$. Let $W_1, \ldots, W_k$ be the irreducible components of $\bigcap_{i=1}^n V_i$. Then*

$$\sum_{i=1}^k \deg W_i \leq \prod_{j=1}^n d_j.$$

Note that this is not a strict generalization as written, as we have not included intersection multiplicities. Fulton in fact does this, but their definition is complicated and the above is sufficient for all our purposes.

The prototypical case we now consider is the following:

We suppose that $V \subset (\mathbb{C}^\times)^3$ is an irreducible surface which contains a Zariski-dense set of Torsion points.

Now suppose that V contains an m-torsion point z. By picking an appropriate $N = (\log m)^{O(1)}$ as before we conclude that $V \cap [N]V$ also contains z. Now there are three options.

1. $V = [N]V$. In this case we run the same argument as before to conclude that V is a torsion coset.

   Exercise 1.8. Run this argument!

2. $V \cap [N]V$ is a union of curves $C_1, \dots, C_s$. In this case Bezouts theorem tells us that the sum of the degree of the C_i is at most $\deg V \deg[N]V \leq N^3 \deg V^2$. Wlog $z \in C_1$. We now repeat the argument and consider $C_1 \cap [N]C_1$

   (a) $C_1 \neq [N]C_1$. In this case we get a contradiction using Fultongs generalized Bezouts theorem 1.7.

   (b) $C_1 = [N]C_1$. We now conclude as before that C_1 is a torus coset.

Thus only the last case remains to be addressed, and the situation we find ourselves in is that all the roots of unity in V, with finitely many exceptions, and contained in 1-dimensional torsion cosets. Now if the cosets were all cosets of the same torus we would easily reduce the dimension and conclude by induction. The issue is how to deal with torsion cosets of distinct tori. The most robust way of dealing with this case in modern terms is either through equidistribution (which we shall discuss in the next section) or through o-minimality (which Jonatha Pila will go into in great detail). Here, we explain how we can finish the proof using the same method as before. In fact, we prove the following more general theorem

Proposition 1.9. *Let $V \subset (\mathbb{C}^\times)^n$ be a degree d irreducible variety. Then there are only finitely many torsion cosets of dimension d contained in V.*

Proof. Assume not for the sake of contradiction, and write these cosets as $g_iT_i \subset V$ where g_i is a torsion point and T_i is a torus. It will be important for us to note that all subtori of $(\mathbb{C}^\times)^n$ are defined over $\mathbb{Q}$ (In general, subtori of split tori are split).

We shall run the same argument as before, but we let m_i denote the order of the image $\overline{g_i}$ of g_i in the quotient space $(\mathbb{C}^\times)^n/T_i$. We first that the m_i are bounded.

Note that the latter is isomorphic as a $\mathbb{Q}$-algebraic group to $(\mathbb{C})^r$ for some r. As V is defined over K, it must contain the entire Galois orbit of g_iT_i, and the number of cosets of T_i is precisely the Galois orbit of $\overline{g_i}$. By Proposition 1.3 this is at least of size $[K : \mathbb{Q}]^{-1}\varphi(m_i)$. Moreover, since T_i is a subgroup, by the same proposition we may find an $N > 1$ with $N = (\log m_i)^{O(1)}$ such that all of these cosets are also contained in $[N]V$. We now define V_k iteratively as $V_0 = V$, $V_{i+1} \subset V_i \cap [N]V_i$ is the irreducible component containing as many of the cosets in $G_k \cdot (g_iT_i)$ as possible. The dimension can drop by 1 at most n times, and so after n steps we obtain $V_n = [N]V_n$. Thus as before V_n is a torsion coset, and thus it must be maximal by our assumptions.

An easy estimate using Theorem 1.7 gives

$$\deg(V_i) \leq \deg V N^{n2^i} d^{2^i}$$

, which also bounds the number of components in our intersections, and thus by induction shows that V_n contains at least a fraction of $\frac{1}{N^{n2^{n+1}} d^{2^{n+1}}}$ of all the torsion cosets. But in fact it only contains 1 - itself! By our assumption $N = {m_i}^{o(1)}$, and this gives a contradiction if m_i is unbounded.

We may thus assume that the m_i are bounded. And in fact, replacing V by $[M]V$ for M the LCM of all the torsion orders, we may assume that the m_i are all 1. Thus all the maximal-dimensional torsion cosets in V are actual tori. However, for any torus T_i we have $T_i = [2]T_i$.Thus the Zariski closure W of all the T_i is stable under the squaring-map, and thus all of its irreducible components are stable under the $[2^t]$ map for a large enough t. Thus they must be torsion cosets, and by maximality must be the T_i themselves. As the number of components is alwys finite, there are only finitely many such T_i to begin with.

□

1.3 Equidistribution: Bilu's Theorem

Equidistribution is by now a common approach to such questions, often involving sophisticated techniques related to dynamics and ergodic theory. Here, however, we can give an elementary example of its usage. We recall that given a compact Hausdorff space X we let $M(X)$ denote the space of all Borel measures. We give this space the weak-* topology, meaning that a sequence $\mu_i \in M(X)$ converges to μ iff for all continuous functions f on X we have $\int f d\mu_i \to \int f d\mu$. It is well known that the weak-* topology is compact.

We shall study the Galois orbits of torsion points in $(\mathbb{S}^1)^n \subset (\mathbb{C}^\times)^n$ and their distributions.

Definition 1.10. For $x \in \mathbb{C}$ we let δ_x denote the delta measure supported on x. For $\alpha \in \overline{\mathbb{Q}}$, we define $\mu_\alpha := \frac{1}{m}\sum_{i-1}^{m} \delta_{\alpha_i}$ where $\{\alpha_1, \ldots, \alpha_n\}$ are the conjugates of α.

Note that a more uniform way to express μ_α is as $\int_{G_\mathbb{Q}} \delta_{g\alpha} dg$ where $G_\mathbb{Q}$ is given its Haar measure.

Lemma 1.11. *Let $\mu_m := \mu_{\zeta_m}$ where ζ_n is a primitive n'th root of unity. Then $\mu_m \to \mu$ where μ is the Haar measure on $\mathbb{S}^1$.*

Proof. By the Stone-Weierstrass theorem, it is enough to check convergence on the functions $t \to t^k$ for $k \in \mathbb{Z}$. We thus compute, for $k \geq 1$, that

$$\begin{aligned}\int t^k d\mu_m &= \frac{1}{\varphi(n)} \sum_{\substack{(d,m)=1 \\ 1\leq d \leq m}} \zeta_m^{dk} \\ &= \frac{1}{\varphi(m)} \sum_{a|m} \mu(a) \sum_{1\leq c \leq \frac{m}{a}} \zeta_m^{cak} \\ &= \frac{1}{\varphi(m)} \sum_{a|m} \mu(a) \frac{m}{a} \delta(m \mid ak) \\ &= \frac{1}{\varphi(m)} \sum_{\substack{a|m \\ m|ak}} \mu(a) \frac{m}{a} \\ &= \frac{1}{\varphi(m)} \sum_{b|\frac{m}{\gcd(m,k)}} \mu(b \gcd(m,k)) \frac{m}{\gcd(m,k)b} \\ &= O(\frac{k^2}{\varphi(m)})\end{aligned}$$

Now note that for k fixed and m large this goes to 0, which establishes the claim. The case of negative k follows as the functions t^k and t^{-k} are complex conjugates.

□

We now generalize this to n-dimensions. first we generalize our definitions from before:

Definition 1.12. For $x \in \mathbb{C}^n$ we let δ_x denote the delta measure supported on x. For $\alpha \in \overline{\overline{\mathbb{Q}}}^n$, we define $\mu_\alpha := \frac{1}{m} \sum_{i-1}^m \delta_{\alpha_i}$ where $\{\alpha_1, \ldots, \alpha_n\}$ are the conjugates of α.

Lemma 1.13. *Let $x(i) \in \mathbb{C}^n$ be a sequence of torsion points such that or any proper algebraic subgroup $H \subset \mathbb{C}^n$, only finitely many of the $x(i)$ lie in H. Then $\mu_{x(i)} \to \mu^n$ where μ is the Haar measure on $\mathbb{S}^1$.*

Proof. We again apply the Stone-Weirestrass theorem to conclude that it is enough to check equidistribution on $f_{\vec{k}} : (t_1, \ldots, t_n) \to \prod_i t_i^{k_i}$ where $k_i \in \mathbb{Z}$. The case of $\vec{k} = 0$ is clear so assume this is not the case. Now consider the map $f_{\vec{k}} : \mathbb{S}^n \to \mathbb{S}^1$ given by $(t_1, \ldots, t_n) \to \prod_i t_i^{k_i}$. Then $f_{\vec{k}}$ preserves the Galois action, and hence $f_{\vec{k},*}\mu_{x(i)} = \mu_{\mu_{\varphi(x(i))}(x(i))}$. Now by assumption the sequence $\varphi(x(i))$ has only finitely many elements of a fixed order, and thus by lemma 1.11 we conclude that $\mu_{\mu_{\varphi(x(i))}(x(i))} \to \mu$. It follows that

$$\int f_{\vec{k}} d\mu_{x(i)} = \int t df_{\vec{k},*}\mu_{x(i)} = \int t d\mu_{\mu_{\varphi(x(i))}(x(i))} \to \int t d\mu = 0$$

□

From this general form of Bilus lemma, it is easy to give the following proof of Lang's conjecture:

Proof. of Conj 1.2

Suppose $V \subset (\mathbb{C}^\times)^n$ is an irreducible variety with a Zariski-dense set of torsion points. If V is contained in a proper algebraic subgroupthen some coset of V is contained in a proper sub-torus and we can proceed by induction on n. Thus we assume that V is not contained in any proper torsion-coset.

Now as before V is defined over some number field K, and we let $W := \bigcup_{\sigma: K \to \mathbb{C}} \sigma(V)$. Then W is an algebraic variety defined over $\mathbb{Q}$ and V is one of its components. Moreover torsion points are also Zariski dense in W.

As such, we may consider a sequence $x(i)$ of torsion points in W, every subset of which is Zariski dense (To do this, we simply enumerate the algebraic subvarieties of W and pick $x(i)$ to be outside the first i of the). Then $x(i)$ satisfies the assumptions of Lemma 1.13, and so $\mu_{x(i)}$ converges to Haar measure on $(\mathbb{S}^1)^n$. Since W is closed it follows that $(\mathbb{S}^1)^n \subset W$. But it is elemetary that $(\mathbb{S}^1)^n$ is Zariski dense in $\mathbb{C}^n$ and hence $W = \mathbb{C}^n$, and thus $V = \mathbb{C}^n$ also.

□

Remark 1.14.

1. It is possible to prove analogues of 1.11 and 1.13 by considering Galois conjugates over a fixed number field K instead of $\mathbb{Q}$ (Ex: do this!). This avoides the need to form W in the proof above.

2. Bilu actually proved his lemma not just for torsion points but for points of small height. The idea is the same but now things are more complicated for a number of reasons, not least of which is that our points aren't contained in $\mathbb{S}^1$ even though the limiting measure is supported on it. Thus one has to worry about some members of the Galois orbit being very large or very small, causing 'escape of mass' phenomena. In fact Bilu uses an energy-minimization argument to prove his theorem instead of the moments approach we took here.

3. Note that Lemma 1.13 can be viewed as an equidisribution version of Lang's conjecture, which is sunbstantially stronger. This can also be formulated for the Manin-Mumford and André-oort conjectures. This is known in the former, but remains wide open in most instances of the latter.

1.4 Zhang's proof: defining equations

We sketch another proof of Zhang which generalizes this theorem to points of small height. For details, [5, §4], and for background [5, §1][2]

Recall that the height of a rational number $\frac{m}{n}$ with $\gcd(m,n) = 1$ is $h(\frac{m}{n}) := \log\max(|m|,|n|)$. One may generalize this to a height function $h : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$. We give a quick definition here and some properties:

- Let $|\cdot|_p$ be a fixed p-adic norm on $\overline{\mathbb{Q}}$ such that $|p| = 1$. Set $\log^+ x := \max(0, \log x)$. Then we set
$$h(\alpha) := \int_{G_{\mathbb{Q}}} \sum_v \log^+ |\sigma(\alpha)|_v d\sigma$$

[2] The reference also contains a detailed discussion of the unit equation and the Mordell-Lang conjecture, both deeply connected to what we are discussing.

where the sum is over all primes as well as the archimedean place. Note that we set $h(0) = 0$.

- $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + O(1)$
- $h(\alpha\beta) \leq h(\alpha) + h(\beta)$
- $h(x) = 0$ iff x is a root of unity.
- $$h(\alpha) = h(\alpha^{-1}) = \int_{G_{\mathbb{Q}}} \sum_v - \log^- |\sigma(\alpha)|_v d\sigma$$

  where $\log^- x := \min(0, \log x)$

Zhang proved a generalization of Conjecture 1.2 for points of small height instead of just torsion points. The key is the following proposition [5, Lemma 4.2.8]

Theorem 1.15. *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with integer coefficients and $\alpha \in \overline{\mathbb{Q}}^n$ such that $f(\alpha) = 0$. There there is a constant $c > 0$, such that if $h(\alpha) < \frac{c}{p}$ for a prime p such that $p \gg_f 1$ then $f(\alpha^p) = 0$..*

Proof. Suppose that $f(\alpha) \neq 0$. Then on the one hand, using the assumptions and the elementary properties of heights above we conclude that $h(f(\alpha)^p) = O_{f,c}(1)$. One the other hand, $f(\alpha)^p - f(\alpha^p)$ has coefficients divisible by p, so whenever $\sigma(\alpha)$ is an algebraic integer it follows that $\log |f(\sigma(\alpha)^p)|_p \leq -\log p + p \deg(f) \sum_{i=1}^n \log^+ |\alpha_i|$. Summing we see that

$$\int_{G_{\mathbb{Q}}} \log^{-1} |f(\sigma(\alpha)^p)|_p d\sigma \leq -\log p + p \deg(f) h(\alpha)$$

From which we conclude that $h(f(\alpha^p)) \geq \log p + O_f(1)$. □

Armed with this Theorem, one may provide an alternative proof - technically without using any Galois lower bound orbits!, though they are very much around the corner - that if a variety contains a point of sufficiently small height, than so does its image under the p'th power map. One then proceeds as before.

2 Lecture #2: Elliptic curves, Galois Representations and Class Groups

2.1 Elliptic Curves

2.1.1 Definition

an Elliptic curve E is a smooth, projective, connected algebraic curve of genus one, on which there is a specified point. This can be defined either over a field or one may also work in families $\varphi : \mathcal{E} \to S$, in which case we interpert the point as a section $f : S \to \mathcal{E}$ and we call $(\mathcal{E}, \varphi)$ an *elliptic curve over S*.

There is a canonical Abelian group variety structure on E with the marked point O as the origin. The simplest way to understand this structure is as such: $A + B + C = 0$ iff there is a non-constant rational function f on E whose associated divisor is $3O - (A + B + C)$. In other words, f has a triple pole at O and zeroes at A, B and C.

2.1.2 Complex Elliptic Curves

Over the complex numbers there is a uniformization of Elliptic curves. Namely, the complex points of every Elliptic curve may be written as

$$E(\mathbb{C}) \cong \mathbb{C}/L$$

for some discrete, rank 2 integral lattice $L \subset \mathbb{C}$. Note that such a presentation is not unique: the lattice L may be scaled by any complex number.

More canonically, elliptic curves have a 1-dimensional space of global regular differentials ω, and given any point $z \in E(\mathbb{C})$ one may form the complex number $\int_0^z \omega$. Now this is only well defined up to a choice of path γ from 0 to z, and any two paths differ by a homology class $H_1(E, \mathbb{Z})$. We thus get a well defined map

$$E(\mathbb{C}) \cong H^0(,\Omega^1_E)^\vee / H_1(E, \mathbb{Z})$$

which turns out to be an isomorphism.

2.1.3 Torsion Structure and the Tate module

If E is a complex elliptic curve, then it is easy to see by the uniformization $E(\mathbb{C}) \cong \mathbb{C}/L$ that $E(\mathbb{C})[n] \cong \frac{1}{n}L/L \cong (\mathbb{Z}/n\mathbb{Z})^2$. It turns out that for any field k of characteristic relatively prime to p, we have $E(\overline{k})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

in particular, for any prime ℓ relatively prime to the characteristic of k, we may form $T_\ell E := \varinjlim E(\overline{k})[\ell^n]$ where the transition maps are given by multiplication by ℓ. As a profinite group, $T_\ell E \cong \mathbb{Z}_\ell^2$. We call $T_\ell E$ the *ℓ-adic Tate module* of E.

We get a far richer structure if k is not algebraically closed, because then we get an induced Galois of G_k on $T_\ell E$. Studying these families of representations as ℓ varies gives a lot of information.

2.1.4 Complex Multiplication

For a complex elliptic curve E, consider the endomorphism ring $\mathrm{End}(E)$. Writing $E(\mathbb{C}) \cong \mathbb{C}/L$ it follows easily that

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha L = L$$

is either $\mathbb{Z}$, or a quadratic ring over $\mathbb{Z}$. We call the elliptic curves where $\mathrm{End}(E)$ is a quadratic ring *CM elliptic curves* and say that E has *complex multuplication*

Such Curves are crucially important to the study of number theory. We hae the following important lemma to start:

Lemma 2.1. *CM elliptic curves are defined over $\overline{\mathbb{Q}}$:.*

Proof. First, note that the property of having complex multiplication is algebraic, and hence Galois-invariant.

Moreover, it is easy to see that there are only countably many such elliptic curves up to isomorphism, since L must be (up to scale) spanned by 1 and a quadratic irrational, of which there are only countably many.

Finally, recall that Elliptic curves are classified up to isomorphism by their j-invariant. Thus their j-invariant is a complex number with a countable orbit under $\mathrm{Aut}(\mathbb{C})$. However, $\mathrm{Aut}(\mathbb{C})$ acts transitively on transcendental elements, and the claim follows.

□

The Galois action on Elliptic curves with CM is also extremely easy to understand. For a quadratic order $R \subset K$ there is a class group $Cl(R)$ consisting of invertible fractional ideals modulo principal ideas. This is a finite abelian group, and there is a natural abelian extension K_R of K such that $\mathrm{Gal}(K_R/K) \cong Cl(R)$. Note that there is a natural action of $Cl(R)$ on the set of CM elliptic curves with endomorphism ring R given as follows:

$$J \cdot E := E \otimes_R J.$$

Exercise 2.2. Prove that this gives a well defined action, and moreover that this action is simply transitive.

We have the following theorem (see [16] for a thorough exposition to this theory).

Theorem 2.3. *CM elliptic curves with Endomorphism ring R are all Galois conjugate and defined over K_R. Moreover, they form a torsor under* $\mathrm{Gal}(K_R/K)$ *compatible with the natural action of $Cl(R)$.*

We have the all-important Brauer-Siegel Theorem which will be responsible for 'large Galois orbits' in this context:

Theorem 2.4. $|Cl(R)| = (R)^{\frac{1}{2}+o(1)}$.

Proof. This is very much not a proof but one uses the class number formula, and this reduces the question to obtaining estimates for the Dedekind zeta function residue at $s = 1$. □

Exercise 2.5.

- Prove that if E does not have complex multiplication, then all irreducible algebraic subbgroups of E^n are isomorphism to E^m, and naturally in bijection with vector subspaces of $\mathbb{Q}^m$.
- If E has CM by a quadratic order in a quadratic field K, prove that irreducible algebraic subbgroups of E^n are naturally in bijection with K-vector subspaces of K^n, and are isogenous to E^m.

2.2 Manin-Mumford Conjecture

Definition 2.6. We may define torsion cosets of E^n in exactly the same way as for $\mathbb{G}_m^n$: as xH where $x \in E^n$ is a torsion point and $H \subset E^n_{\overline{k}}$ is an irreducible algebraic subgroup.

We have the following analogue of 1.2

Theorem 2.7. *Let $E/\mathbb{C}$ be an elliptic curve, an let $V \subset E^n$ be an irreducible algebraic variety. Then V contains finitely many maximal torsion cosets.*

This theorem was first proven by Raynaud for curves [25] and then in the general case [26]. Raynauds brilliant proof used the observation that the Frobenius map on Abelian varieties is inseparable, which imposes algebraic mod p^2 conditions on torsion points mod p. This observation alone suffices to handle prime-to-p torsion, and combined with large Galois orbits to facilitate a complete proof that works for all torsion orders.

We shall not give Raynauds proofs, but instead explain below how to generalize the proofs using intersection theory and Equidistribution, as well as the proof given by Pila-Zannier:

2.2.1 Reduction from $\mathbb{C}$ to $\overline{\mathbb{Q}}$

To get large Galois orbits one needs a large Galois action, and in particular for the elliptic curve to be defined over a number field. Here we explain how to reduce to that case. We thus assume the Manin-Mumford conjecture 2.7 for $\overline{\mathbb{Q}}$ Elliptic curves.

Suppose that E is a complex elliptic curve. If E has CM then E can be defined over $\overline{\mathbb{Q}}$, and so we assume that this is not the case. By taking the finitely generated subring $\iota : R \hookleftarrow \mathbb{C}$ containing all the defining equations for E and for V (in some projective embedding, say) we obtain an elliptic curve $\mathcal{E}$ over R, and a closed subvariety $\mathcal{V} \subset \mathcal{E}$, whose base-change to $\mathbb{C}$ via ι is (E, V). We may think of i as a generic complex-valued point of R. Note that $X = R \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$ is a scheme of finite type over $\overline{\mathbb{Q}}$, and by replacing X by its reduced subscheme we may obtain an elliptic curve $\mathcal{E}$ over a $\overline{\mathbb{Q}}$-variety X with a specialization via ι to E.

Now we fix a simply concected disc $\Delta X(\mathbb{C})$ which contains the point ι, and note that analytically locally, we have a trivialization $\varphi : \mathcal{E}^n_\Delta(\mathbb{C}) \cong \Delta \times (\mathbb{S}^1)^{2n}$. Now let $S \subset (\mathbb{S}^1)^{2n}$ denote the image of all the torsion points contained in V. Since ι is a generic in X, it follows that the $\overline{\mathbb{Q}}$-Zariski closure of $S \subset \mathcal{V}_\iota$ contains all of $\Delta \times S$. Thus we have that $\Delta \times S \subset \mathcal{V}$.

We let $M \subset (\mathbb{S}^1)^{2n}$ denote the smallest union of **real-analytic** -torsion cosets which contain S. Now for any $\overline{\mathbb{Q}}$-point $b \in X(\overline{\mathbb{Q}})$ we are assuming Theorem 2.7 holds, which means that $\{b\} \times S \subset \varphi(\mathcal{V}_b)$ is contained in a finite union of algebraic torsion cosets. Since algebraic torsion cosets are also real-analytic torsion cosets, it follows that $\{b\} \times M \subset \varphi(\mathcal{V}_b)$. Since the set of $\overline{\mathbb{Q}}$ points is topologically dense in X, we conclude that $\Delta \times M \subset \varphi(\mathcal{V})$, and in particular that $M \subset \varphi(V)$.

It follows that all the torsion points in V are contained in a finite union of real-analytic torsion cosets M_V. Now it is easy to show that the Zariski-closure of a subgroup of $E^n(\mathbb{C})$ is an algebraic subgroup of E^n, and hence the same is true for a torsion coset. Thus the Zariski-closure M_V^{zar} is a finite union of torsion cosets which is contained in V and contains all torsion points of V. The claim is thus proved. (Note that the proof shows $M_V^{\mathrm{zar}} = M_V$).

Remark 2.8. These kind of reduction arguments have been used by Bombieri-Masser-Zannier on Zilber-Pink questions as well, but they are often more challenging then the above. In particular, we got really lucky in the above that the torsion points are defined uniformly over all of X. Often, one has to worry about only being defined over an open set, and those open sets shrinking as one considers more and more points.

2.2.2 Large Galois Orbits

We need to establish that Galois orbits of torsion points are large. One may profitably rephrase this statement in the following way: The image of the galois representation $\rho_E : G_K \to \mathbf{GL}_2(\mathbb{Z})$ is large, and in particular has large orbits. Now it depends what one wants from this result. Work of Masser[17] - later greatly extended by Masser-Wẅustholz as we shall see in lecture 3- allows one a lower bound of the following form:

Theorem 2.9. *Let E/K be an Elliptic curve. If $x \in E(\overline{\mathbb{Q}})$ is an order-N torsion point, then $[K(x) : X] \gg_E N^\delta$ for some fixed $\delta > 0$.*

This proof is based on Transcendence techniques and we shall say no more about it here. The result is sufficent for the Pila-Zannier method to work, as all one needs is a polynomial bound.

In this instance, however, it is possible to do much better, using a theorem of Serre[27]:

Theorem 2.10. *[Serre's Open Image Theorem]*

Let E/K be an elliptic curve.

1. *If E does not have complex multiplication, then $\rho_E(G_k)$ is an open subgroup of $\mathbf{GL}_2(\mathbb{Z})$, and in particular finite index.*
2. *If E has CM by a quadratic field $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong L$, then $\rho_E(G_k)$ is a finite index subgroup of $\mathcal{O}_L^\times$.*

In particular, $\rho_E(G_k)$ contains a finite index subgroup of the scalar group $^\times$.

Theorem 2.10 is incredibly deep, with the second part being a consequence of the theory of complex multiplication and the first part being a hard-fought theorem of Serre. The advantage of this is it allows us to prove equidistribution results, as we shall see in the next section.

2.2.3 Equidistribution Results

We borrow the notation for δ_x of §1.3. Motivated by Theorem 2.10 we shall consider the following setup. Let $G \subset (\hat{\mathbb{Z}})^\times$ be a finite index subgroup. For $\alpha \in E^n_{tor}$ we let $\mu_\alpha := \int_G \delta_{g\alpha} dg$. Note that as topological group, $E(\mathbb{C}) \cong (\mathbb{S}^1)^2$, so this setup is very similar to what we encountered with Bilu's lemma, with the onyl different being that we consider G instead of all of $(\hat{\mathbb{Z}})^\times$.

Lemma 2.11. *Let $x(i) \in (\mathbb{S}^1)^n$ be a sequence of torsion points such that or any proper lie subgroup $H \subset (\mathbb{S}^1)$, only finitely many of the $x(i)$ lie in H. Then $\mu_{x(i)} \to \mu^n$ where μ is the Haar measure on $\mathbb{S}^1$.*

Proof. The reduction to the 1-dimensional case works the same as in 1.13, and so it is sufficient to consider the case of $n = 1$. In this case, let N be the order of $x \in \mathbb{S}^1$. Then let $\chi_1, \dots, \mathrm{ch}_r$ be the Dirichlet characters $\mod N$ which vanish on the image of G, where r is bounded by the index of G and therefore uniformly bounded. Then to check convergence on the moments $t \to t^k$ for $k \in \mathbb{Z}$ it is suffices to bound Gauss sums of the form

$$\frac{1}{\varphi(N)} \sum_{a \mod N} \chi(a) e^{\frac{2\pi i a}{N}}.$$

It is well known that the absolute value of this sum is bounded by $\frac{\sqrt{N}}{\varphi(N)}$ which converges to 0. The proof is therefore complete. □

This is almost enough to make the induction in the equidistribution claim hold up. The problem is that there are lie subroups of $(\mathbb{C})^n$ which are not algebraic. Thus, we need to upgrade lemma 2.11 to take into account the algebraic structure of E:

Lemma 2.12. *Let $x(i) \in E^n$ be a sequence of torsion points such that for any proper algebraic subgroup $H \subset E^n$, only finitely many of the $x(i)$ lie in H. Then $\mu_{x(i)} \to \mu^{2n}$ where μ is the Haar measure on $\mathbb{S}^1$.*

Proof. Let $x(i)$ be a sequence of torsion points and let H be the smallest lie subgroup of $E(\mathbb{C})^n$ containing them all. We wish to show that H must be algebraic. By increasing the base field of definition (or multipliying all the torsion points by an appropriate scalar) we may assume that H is connected.

We wish to use the extra Galois image (besides the center) provided by Theorem 2.10. Since the CM case gives a lower galois image we shall only tackle that case, with the non-CM case being more straightforward (and in fact following in the exact same way). As such, let $K = \mathrm{End}_{\mathbb{C}}(E)$. By Theorem 2.10 the group G from Lemma 2.12 contains a finite index subgroup $U \subset (\widehat{\mathcal{O}_K})^\times$.

Now we may identify $E(\mathbb{C})_{tor} \cong (K/L)^n$ for a lattice L in K. Therefore we may identify $E(\mathbb{C})_{tor}^\vee \subset (\hat{M})^n$ where

$$M = \{k \in K \mid \mathrm{tr}(kL) \subset \mathbb{Z}\}$$

and the pairing is simply

$$(a, b) \to e^{2\pi i\, \mathrm{tr}(ab)} \in \mathbb{S}^1.$$

Now let H be cut out by the integral sublattice $R \subset K$. Let $T \subset (\hat{M})^n$ be the set of all characters which vanish on all of the $x(i)$. Note that $R = T \cap \mathcal{O}_K$ and that T is a $\hat{Z}$-module. Since the $x(i)$ are invariant by U, it follows that $T = TU$. Therefore, T is a module under $\hat{\mathbb{Z}}[U] \subset \widehat{\mathcal{O}_K}$. It is straightforward to see that $\hat{\mathbb{Z}}[U]$ is finite index in $\widehat{\mathcal{O}_K}$ and therefore contains an order $S \subset \mathcal{O}_K$. Therefore R is invariant under S. Since H is connected it follows that R is saturated, and thus R is invariant under $\mathrm{End}_{\mathbb{C}}(E)$.

Finally, we now claim that H is algebraic. Indeed, since is invariant under $\mathrm{End}_{\mathbb{C}}(E)$ it follows that H may be cut out by an appropriate submodule of $\mathrm{Hom}(E^n, E)$, which completes the proof.

□

Exercise 2.13. Complete the proof by showing that for any number field K and any finite index subgroup $U \subset (\widehat{\mathcal{O}_K})^\times$, that $\hat{\mathbb{Z}}[U]$ is finite index in $\widehat{\mathcal{O}_K}$.

2.3 Moduli of Elliptic Curves $Y(1)$

2.3.1 Construction using Complex uniformization

We may use the complex uniformization of Elliptic curves to write down an analytic moduli space for them. Indeed, it suffices to classify rank 2 lattices up to scale!

To do this, we start by picking two elements (z, w) to span the lattice $L \subset \mathbb{C}$. The only condition is that (z, w) are independent over $\mathbb{R}$, which we shall manually remove in a minute. Now there are two things to worry about:

- Since we are only counting lattices up to scale, we should mod out by $(z, w) \sim (\alpha z, \alpha w)$ for $\alpha \in \mathbb{C}^\times$.
- We are in fact specifying a lattice with a basis, when we only want to remember the lattice. There is a natural action of $\mathrm{Gl}_2(\mathbb{Z})$ on $\mathbb{C}^2$ which permutes all possible bases, so we should mod out by that as well.

Now the actions of $\mathrm{Gl}_2(\mathbb{Z})$ and $\mathbb{C}^\times$ commute so we may quotient out by either order. Quotienting by $\mathbb{C}^2$ first gets us to $\mathbb{P}^1(\mathbb{C}) = (\mathbb{C}^2 - \{0\})/\mathbb{C}^\times$, and remembering that (z, w) should be linearly independent over $\mathbb{R}$ gets us to $\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$.

We thus get a coarse moduli space

$$Y(1) := \mathrm{Gl}_2(\mathbb{Z}) \backslash (\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})).$$

We may write

$$\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R}) = \mathbb{H}^1 \cup \mathbb{H}^1_-$$

as the union of the upper and lower half-planes, and as $\mathrm{Gl}_2(\mathbb{Z})$ acts transitively on the set, we have the equivalent (and more familiar presentation

$$Y(1) \cong \mathrm{Sl}_2(\mathbb{Z}) \backslash \mathbb{H}^1.$$

Remarkably, $Y(1)$ has a canonical structure of an algberaic variety. This can most easily be described by defining the j-function to be algebraic. In fact, ignoring the orbifold structure this gives us an analytic isomorphism $j : Y(1) \cong \mathbb{C}$.

Remark 2.14.

1. We may understand the action of $\mathrm{Sl}_2(\mathbb{Z})$ explicitly quite easily. Indeed, a point $z \in \mathbb{H}^1$ corresponds to the $\mathbb{C}^\times$-equivalence class of $(z, 1) \in \mathbb{C}^2$. An element $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on $(1, z)$ via

$$g \cdot (z, 1) = (az + b, cz + d) \sim \left(\frac{az + b}{cz + d}, 1 \right)$$

which recovers the action.

2. Technically $Y(1)$ - even complex analytically - is only a coarse moduli space because of the orbifold points $i, \omega = e^{\frac{2}{3}}$. For this reason when making arguments one often works with $Y(N)$ instead - the moduli space of Elliptic curves with 'full level N-structure' for some small N such as 3 or 6. Howeve, we shall mostly ignore these issues.

3. The Algebraic structure of $Y(1)$ in fact allows us to think of it as the algebraic moduli space of ellitic curves, which means we have a meaningful action of $\mathrm{Aut}(\mathbb{C})$ on $Y(1)$ such that $\sigma[E] = [\sigma(E)]$, where $\sigma(E)$ is the elliptic curve obtained by applying σ to the coefficients of a defining equation of E (Or in moe canonical scheme-theoretic language, by post-composing the structure map $E \to \mathbb{C}$ with σ^{-1}.

Exercise 2.15. Prove that a point $z \in \mathbb{H}^1$ corresponds to a CM elliptic curve in $Y(1)$ iff z is a quadratic irrational. I.e. $[\mathbb{Q}(z) : \mathbb{Q}] = 2$.

2.3.2 Hecke Operators

Recall the following definition:

Definition 2.16. An *isogeny* between elliptic curves E, E' is a non-constant finite map $\varphi : E \to E'$ which sends O_E to $O_{E'}$. Such a map is known to be a group homomorphism. We say that E, E' are *isogenous* if thee is an isogeny between them. It is known that if there is a map $\varphi : E \to E'$ then there is a dual map $\varphi^\vee : E' \to E$ of the same degree such that $\varphi \circ \varphi' = \times \deg \varphi$. Therefore isogeny is an equivalence relation.

We say that an isogeny is *primitive* if its kernely is cyclic. If 2 elliptic curves are isogenous they are so via a primitive isogeny.

Given an elliptic curve E and an integer n, there are finitely many Elliptic curves isogenous to E via a primitive isogeny of degree n. In terms of the uniformization of $Y(1)$ it is straightforward to describe the relation: $E \cong \mathbb{C}/\langle 1, z\rangle$ and thus all the curves we are looking for are of the form $\mathbb{C}/L$ where $L \subset \langle 1, z\rangle$ is an index n-sublattice with cyclic quotient.

We may find these in the following way: Let

$$T_n := \mathrm{Sl}_2(\mathbb{Z})\backslash\mathrm{Sl}_2(\mathbb{Z})\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)\mathrm{Sl}_2(\mathbb{Z})$$

be a set of left cosets of $\mathrm{Sl}_2(\mathbb{Z})$. Then $T_n z$ is the desired set. We call T_n the n'th Hecke operator.

We may think of T_n as a correspondence on $Y(1)$, and may think of it as a curve $T_n \subset Y(1)^2$. Note that the degree of T_n is $d(n)$-the sum of divisors function of n.

2.3.3 Andr-Oort conjecture, $n = 2$

We are now read to state Andrés Theorem: [1]

Theorem 2.17. *Let $C \subset Y(1)^2$ be an irreducible curve containing an infinite set of CM points: points both of whose co-ordinates are CM. Then C is a Hecke correspondence T_n, or a fiber over a CM point.*

Proof. If C is a fiber than the proof is clear so we assume this is not the case. Since CM points are defined over $\overline{\mathbb{Q}}$, so is C. We make a simplifying assumption that C is in fact defined over $\mathbb{Q}$, and leave it to the reader to remove this assumption as an exercise.

We first have the following reduction:

Lemma 2.18. *Let (z_i, w_i) be an infinite sequence of CM points in C. Then the ratio of the discriminants of the CM orders $f(z_i)/f(w_i)$ take on finitely many values.*

Proof. The key idea is that the fields $\mathbb{Q}(z_i), \mathbb{Q}(w_i)$ have to almost agree, in the sense that $[\mathbb{Q}(z_i, w_i) : \mathbb{Q}(z_i)] = O(1)$ and $[\mathbb{Q}(z_i, w_i) : \mathbb{Q}(w_i)] = O(1)$, since z_i, w_i satisfy a polynomial relation. But now by using the theory of complex multiplication one may precisely understand the Galois groups in terms of class groups of orders, and prove that these are all quite distinct unless the CM orders are essentially the same. For details, see [3, §3] □

By applying a suitable Hecke operator we may in fact assume that all the CM points have the same CM order for both co-ordinates, and we do this from now on.

The key fact we need about CM points are the following:

1. The set of CM elliptic curves with endomorphism ring R_D of discriminant D lies in a single Galois orbit
2. The CM points of discriminant $-D$ with highest j-invariant correspond to the invertible ideals in R_D of smallest norm: If $I = \langle m, a + b\sqrt{-D} \subset R_D$ is such that $I \cap \mathbb{Z} = m\mathbb{Z}$, and I is not divisible by any integer greater than 1, then the corresponding points in $Y(1)$ is $z_{[}I] = \frac{a+b\sqrt{-D}}{m}$ has j-invariant of size $\sim e^{2\pi\frac{b}{m}\sqrt{D}}$.
3. We have $(z_{[R_D]}, z_{[I]}) \in T_{(Nm(I)}$.

Now since C contains infinitely many CM points it contains infinitely points of the form $(z_{[R_D]}, w_D)$ for w_D a CM point corresponding to R_D. Now note that $z_{[R_D]} \to \infty$ where ∞ denotes the added point on $X(1)$. We now have two cases to consider:

1. $\mathbf{w}_D \not\to \infty$

   Then by picking a subsequence we may assume that $(z_{[R_D]}, w_D) \to (\infty, x)$ for some point $x \in Y(1)$. We show this is impossible. The reason is that in local co-ordinate j^{-1}, we have $|j^{-1}(z_{R_D}) - j^{-1}(\infty)| = O(e^{\frac{-\sqrt{D}}{2}})$. Therefore there must exist some constant $c > 0$ such that $|j(w_D) - j(x)| = O(e^{-c\sqrt{D}})$. Switching co-ordinates to the fundmaental domain in $\mathbb{H}^1$ we have that $\log|w_D - x| =\ll -\sqrt{D}$. Now $j(x)$ is algebraic, and w_D is a quadratic irrational. Using Transcendence theory, D.Masser[19, I 1.1] proved that

   $$\log|w_D - x| \gg -h(w_D)^3 \gg -|\log D|^3.$$

   These two inequalities are incompatible for large D which completes the proof.

2. $\mathbf{w}_D \not\to \infty$

   In this case we argue similarly, but now the conclusion is that $\log|j(w_D)| \geq q\sqrt{D} + O(1)$ for some fixed $q \in \mathbb{Q}$. By the above analysis this means that $(z_{[R_D]}, w_D) \in T_n$ for some n which is uniformly bounded. But now we have infinitely many points on $C \cap T_n$ for some n, and therefore we must have that $C = T_n$ as desired.

□

2.3.4 Edixhovens conditional proof on GRH

B.Edixhoven made a substantial amount of progress on André-oort by introducting a beautiful idea using Bezouts theorem to conditionally solve re-prove the $Y(1)^2$ case. In fact, we have already seen this idea carried out in detail in the case of Langs conjecture in the first lecture. How does it work in this context?

1. To begin with, one reduces as before to the case where the CM points have CM by the same ring in both co-ordinates.

2. The key observation is that if p is a split prime in R_D, then we get a corresponding frobenius element σ_p in the Galois group, and $(z, \sigma_p(z)) \in T_p$ whenever z has CM by R_D.

3. We now apply Bezout's theorem to $C \cap (T_p \times T_p)(C)$.

   - If $C \subset (T_p \times T_p)(C)$ one concludes using (elementary) functional transcendence that C is a Hecke curve.
   - Else, we know that $C \cap (T_p \times T_p)(C)$ contans and entire Galois orbit of CM points and thus is of size at least $\sim Cl(R_D)$.
   - On the other hand, the upper bound by Bezouts theorem gives somethinf of size $O(p^2)$.

   Now, by theorems 2.3 and 2.4, the size of $CL(R_D)$ is roughly $\sqrt(D)$. On the other hand, if GRH is true then we can find small split primes p (of size a power of $\log D$ in fact). This gives us our desired contradiction.

We see that the use of GRH is purely to get small split primes, without which the argument families. Now, how small do we need our primes? Well in this case it turns out anything less than $D^{\frac{1}{4}-\epsilon}$ would suffice, which is just on the border of what's achievable (though still just short of being doable, I believe)! However, for higher dimensions and in other Shimura varieties one needs much better estimates, tending to an arbitrarily small power of the Discriminant, which are extremely out of reach for the moment.

Remark 2.19. One may of course ask for an equidistribution version of the Andre-Oort conjecture for $Y(1)^2$. There has been much work on this and was proven under the GRH[15], but an unconditional proof is still open.

2.3.5 Higher-Dimensional Case

To formulate an analogue of Theorem 2.17 for $Y(1)^n$ we need to give an analogue of the notion of a torsion coset. In particular, we need to understand which varieties do in fact have a zariski-dense set of CM points. We are motivated by the following observation: If $x \in \mathbb{H}^1$ is a CM point, and $g \in \mathrm{Gl}_2(\mathbb{Q})$ then so is gx. in other words, *anything isogenous to a CM point is also CM.* This motivates the followig definitions

Definition 2.20. 1. A *special point* $x \in Y(1)^n$ is a point all of whose co-ordinates are CM. We may also call x itself a CM point.

2. A *special subvariety* $Z \in Y(1)^n$ is an irreducible variety which is an irreducible component of a variety Z' defined by relations of the following two types:

   - A co-ordinate z_i is fixed to be a CM point
   - Two of the co-ordinates z_i, z_j are satisfy the relation $(z_i, z_j) \in T_n$ for some positive integer n.

   In other words, Z is defined by taking an irreducible component of then intersection of pullbacks of Hecke curves and CM points under projections to $Y(1)^2$ and $Y(1)$ respectively. We say that Z is *Strongly Special* if no co-ordinates of Z are fixed to be CM points. These are the special varieties that do not 'deform' in a family.

Remark 2.21. 1. There is a more 'intrinsic' definition of special varieties as components of Shimura subvarietes, or more fundamentally in the language of Hodge theory as subvarieties defined by restricting the Mumford-Tate groups. We shall encounter these somewhat in the next 2 lectures, but we believe we have given the most down-to-earth definition in this simple case.

Armed with this definition, we may give the André-Oort conjecture for $Y(1)^n$.

Theorem 2.22. *Let $V \subset Y(1)^n$ be an irreducible algebraic subvariety. Then V contains finitely many maximal special subvarieties.*

Remark 2.23. This theorem was first proven conditionally under GRH by Edixhoven[9], and was first proven unconditionally by J.Pila [23].

We now present Edixhovens argument, and we simplify by considering the special case of $n = 3$, where the essential case is $\dim V = 2$. Now the same arguments as for the $n = 2$ case can be modified to prove that if V contains a Zariski-dense set of special points than it contains a Zariski-dense set of special curves.

Reduction to the strongly special setup

Suppose V contains infinitely many special curves which are not strongly special. Then they are, wlog, of the form $C_i \times P_i \subset Y(1)^2$ where C_i are Hecke correspondences and the P_i are CM points. Now by the Galois theory arguemts we already used, the Galois conjugates of the P_i grow, so we are in one of the following 2 cases:

- The P_i are a fixed set of points. Then it is easy to show that V is a fiber of the P_i.
- The P_i vary, in which case for large enough i, it must be the case that V contains $C_i \times Y(1)$ and thus be equal to it.

Therefore, we may assume that V contains an infinite set of strongly special curves. There is the following beautiful characterization result of Edixhoven:

Proposition 2.24. *Let $C \subset Y(1)^3$ be a special curve which projects dominantly onto every co-ordinate. Then there are positive integers (n_1, n_2, n_3) such that C is a connected component of the moduli of complex Elliptic curves E together with subgroups $G_i \subset E(\mathbb{C})$ with $G_i \cong \mathbb{Z}/n_i\mathbb{Z}$ which have no pair-wise intersection. Moreover, the embedding into $Y(1)^3$ is given by $([E], G_1, G_2, G_3) \to (E/G_1, E/G_2, E/G_3)$. Finally, the number of connected components of $Y(n_1, n_2, n_3)$ is at most $4^{\gcd(n_1,n_2,n_3)}$, and they all have the same degree projections to all 3 co-ordinates.*

Proof. Since the projection of C onto every pair of co-ordinates is special, it must be a Hecke correspondence. Hence, over the generic point of C the elliptic curves $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ are all isogenous. We first claim that there exists an ellptic curve $\mathcal{E}$ with finite cyclic subgroups $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ that are disjoint except for the identity, such that $\mathcal{E}/\mathcal{G}_i \cong \mathcal{E}_i$. Since the $\mathcal{E}_i$ do not have CM this comes down to the following linear algebra fact:

Lemma 2.25. *Let V be a rank 2 rational vector spaces, and L_1, L_2, L_3 be 3 lattices in V. Then there exists a lattice $L \subset V$ and elements $q_1, q_2, q_3 \in \mathbb{Q}^\times$ such that $q_iL_i \supset L$, the quotients L/q_iL_i are cyclic, and the pairwise intersections of q_iL_i are equal to L. Moreover such an L is unique up to scale.*

Proof. This lemma is easily seen to follow from the analogous one over $\mathbb{Z}_p$ for all primes p, so we tensor with $\mathbb{Z}_p$ to make V a $\mathbb{Q}_p$ vector space, and L_i are $\mathbb{Z}_p$-lattices.

We now consider the set T of $\mathbb{Z}_p$-lattices up to scale. T has a natural graph structure where we connect two lattices A, B if we may scale them such that $A \subset B, B/A \cong \mathbb{Z}/p\mathbb{Z}$. This is easily seen to be symmetric, as then $pB \subset A, A/pB \cong \mathbb{Z}/p\mathbb{Z}$. Moreover, it is well-known that this makes T a connected tree, and in fact T is $(p+1)$-regular.

Now given the three points $[L_1], [L_2], [L_3]$ in the tree T there is a unique 'center', a point $[L]$ such that the paths from $[L]$ to the other 3 lattices are disjoint. This is true in any connected tree! Then scaling we may assume that $L_i \supset L$ and the quotients are all cyclic. The fact about the paths being disjoint exactly translates to the pair-wise intersections being L, which proves the claim.

□

The lemma proves the existence of the groups $\mathcal{G}_i$ as desired. The only thing that remains to prove is the claims about the connected components of the moduli space. This follows from considering the action of the monodromy group $\mathrm{Sl}_2(\mathbb{Z})$. In particular, trivializing the cohomology of $H^1(\mathcal{E}, \mathbb{Z})$ the group $\mathrm{Sl}_2(\mathbb{Z})$ acts on the tree T of sublattices up to scale. By using Strong approximation, we see that $\mathrm{Sl}_2(\mathbb{Z})$ surjects onto $\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$ for any n. Thus, the relevant linear algebra fact is the following:

Lemma 2.26. *The action of $\mathbf{SL}_2(\mathbb{Z}_p)$ on T has at most 4 orbits on the set of triples $([L_1], [L_2], [L_3])$ with predetermined distances (n_1, n_2, n_3) to the fixed lattice $[L]$, with disjoint paths from $[L]$. Moreover, these orbits have the same size constant-size fibers over each pair of vertices, in any pair of co-ordinates.*

Proof. First, note that if we take the path fro $[L]$ to $[L_i]$ and elongate it to a further vertex v, we may recover $[L_i]$ from v by walking along the path from $[L]$ to v n_i steps. Thus, by picking an $N \geq \max(n_1, n_2, n_3)$ and picking further vertices from $[L]$ we may assume $n_1 = n_2 = n_3 = N$. Now lattices a fixed distance N away from $[L]$ are naturally in bijection with $\mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z})$. We thus need understand the action of $\mathrm{Sl}_2(\mathbb{Z}/p^n\mathbb{Z})$ on points in $\mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z})$ reducing to different points in $\mathbb{P}^1(_p)$. First note that the action on pairs is transitive, which proves the second claim. To understand the number of orbits, first move two of the vertices to $(0,1)$ and $(1,0)$. The third vertex then becomes an elment of $(\mathbb{Z}/p^N\mathbb{Z})^\times$, and the stabilizer is the diagonal torus which acts by squares. The claim now follows $\mathbb{Z}/p^N\mathbb{Z}$ has at most 4 square classes. □

Exercise 2.27. Prove the relevant graph-theoretic facts about T:

1. Prove that for any two $\mathbb{Z}_p$-lattices L, W there is a unique integer power q of p such that $qL \subset W$ and the quotient qL/W is cyclic. Call $|\log_p q|$ the distance from L to W, denoted $d([L],[W])$.

2. Prove $d([L],[W]) = d([W],[L])$

3. Suppose $d([L],[W]) = n > 0$. Prove that $[W]$ has exactly 1 neighbor $[W']$ such that $d([L],[W']) = n-1$ and for the other neighbors $[W'']$ we have $d([L],[W'']) = n+1$.

4. Prove that T has no cycles, and is therefore a tree.

5. Prove that in any connected tree, for any 3 vertices $a, b, c \in T$ there is a unique vertex $d \in T$ such that the paths from d to a, b, c have no vertices in common (except maybe the endpoints).

6. Finally, suppose that A, B, C are lattices and $A \subset B, C$ with cyclic quotients. Prove that $B \cap C = A$ iff the paths from $[A]$ to $[B], [C]$ are disjoint (except for endpoints).

□

Corollary 2.28. *Let $C \subset Y(1)^3$ be a strongly special curve. If all three projections $C \to \pi_{i,j}(C)$ have degree $O(1)$ then there are finitely many options for C.*

Proof. We use the notation in the previous lemma. If $n_1 \geq n_2, n_3$ the n the degree of the projection onto the first co-ordinate is at least

$$\prod_{p^r || n_1} \frac{(p-1)p^{r-1}}{4}$$

which clearly tends to infinity. □

We can now finish the proof:

Proposition 2.29. *Suppose that $V \subset Y(1)^3$ is an irreducible surface with dominant projection onto each co-ordinates, and suppose that it contains infinitely many special curves dominant on all 3 factors. Then S is the pullback of a Hecke correspondence from a projection onto some pair of co-ordinates.*

Proof. Suppose V has dominant projection onto all pairs of co-ordinates. Let $C \subset V$ be a special curve. Then its projection onto its image in $Y(1)^2$ is bounded by the degree of the projection of S onto the corresponding $Y(1)^2$. Thus all special curves in

$Y(1)$ have bounded degrees of all 3 projects, and thus by the above corollary 2.28 there are only finitely many of them. This is a contradiction, and therefore $V = V_0 \times Y(1)$ for some curve V_0. Now it is easy to see that V_0 must be special which completes the proof. □

3 Lecture #3: Abelian Varieties, their moduli, and the Masser-Wüstholz theorem

3.1 Background

3.1.1 Definitions and Basic Properties

Definition 3.1. An abelian variety A over a field k is an irreducible, projective algebraic group variety over k.

Abelian varieties are the higher-dimensional generalization of elliptic curves, and are important for many reasons. In the context of special point problems, one can either consider them as the ambient space, or consider their moduli which is the prototypical Shimura Variety $\mathcal{A}_g$.

We define Abelian subvarieties, Torsion Cosets, and isogenies exactly analogously as before.

3.1.2 Dual Abelian Variety and Polarizations

Given an Abelian variety A over k there is a dual abelian variety $A^\vee$, such that there is a natural isomorphism $A \cong (A^\vee)^\vee$. The easiest way to define $A^\vee$ is as $\text{Pic}^0(A)$ - the moduli space of degree 0 line bundles on A. As such, on $A \times A^\vee$ there is a natural line bundle P known as the *Poincare bundle* which is trivial over both 0 fibers, and represents the universal family of line bundles on A. We have the following properties:

1. Every abelian variety A is isogenous to its dual $A^\vee$.

2. Given a map $\varphi : A \to B$ there is a unique map $\varphi^\vee : B^\vee \to A^\vee$ such that $(\varphi \circ \psi)^\vee = \psi^\vee \circ \varphi^\vee$.

3. Given a divisor D on A, the map $\lambda_D : A \to A^\vee$ which sends $r \to [D - t] - [D]$ is self-dual

4. A*polarization* is an isogeny $\varphi : A \to A^\vee$ which is self-dual, and such that $(1, \varphi)^* P$ is ample on A. All λ_D are polarizations for any ample D.

5. If a polarization φ has degree 1, we say that φ is a *principal polarization*

6. Every abelian variety over an algebraically cosed field is isogenous to a principally polarized one.

We have the following fundamental reducibility property, which says that the category of Abelian varieties up to isogeny is semisimple:

Proposition 3.2. *Suppose that $B \subset A$ is an abelian subvariety. Then there exists an abelian subvariety $C \subset A$ such that $B \oplus C \to A$ is an isogeny.*

Proof. Fix polarizations λ_D on A. Let $i : B \to A$ be the inclusion map, and consider the map $i^\vee : A^\vee \to B^\vee$. Note that $i^\vee \circ i : B \to B$ is the map λ_{i^*D} and is therefore an isogeny. Thus $B \oplus (\ker i^\vee \to A^\vee$ is surjective with finite kernel. Now letting C be a connected component of ${\lambda_D^*}^\vee$ completes the proof. □

It follows that every Abelian variety is a direct sum of simple subvarieties up to isogeny.

3.1.3 Complex Uniformization

Like the case of Elliptic curves, every abelian variety can be written as $\mathbb{C}^g/L$ for some full-rank integral lattice L. *Unlike* the case of Elliptic curves, however, most L do not yield an algebraic variety.

Lemma 3.3. *There exist lattices $L \subset \mathbb{C}^2$ whose quotients do not give Abelian varieties.*

Proof. Consider the lattice $L_w = \langle (1,0), (i,0), (0,1), (w,i) \rangle$. Note that there is an exact sequence of complex tori $E \to \mathbb{C}/L_w \to E$ where $E := \mathbb{C}/\langle (1,0), (i,0) \rangle$. Now by Proposition 3.2 if $\mathbb{C}/L_w$ were an Abelian Variety this exact sequence would split up to isogeny, and the space of maps $\mathrm{Hom}(E, \mathbb{C}/L_w)$ would be larger than $\mathrm{Hom}(E,E)$. However, it is easy to show that $\mathrm{Hom}(E, \mathbb{C}/L_w) \cong \mathrm{Hom}(\mathbb{C}, \mathbb{C}^2) \cap \mathrm{Hom}(\langle (1,0), (i,0) \rangle, L_w)$. For $w \notin \mathbb{Q}(i)$ it is easy to show that this is indeed $\mathrm{Hom}(E,E)$ which yields a contradiction.

□

Exercise 3.4. Prove both 'easy' claims in the proof above.

Definition 3.5. A *Polarization* for a lattice $L \subset \mathbb{C}^g$ is a positive definite hermitian form H on $\mathbb{C}^g$, such that $\Im H$ takes integer values on L.

It turns out that a lattice gives rise to an Abelian Variety iff it admits a polarization, and there is a natural bijection between polarizations on the lattice and on the corresponding Abelian Variety.

3.1.4 Torsion and Galois Representations

Given an abelian variety A over a field k of characteristic not dividing n, we have that $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. Over $\mathbb{C}$ this follows immediately from the complex uniformization. Moreover, there is a natural perfect pairing $A[n] \times A^\vee[n]$ which is anti-symmetric when composed with any polarization. We call this the *weil-paring.*

For any prime $\ell \neq \operatorname{char} k$, we form the *$\ell$-adic Tate-module* $T_\ell(A)$ and obtain the corresponding Galois representation $\rho_{\ell,A} : G_k \to \mathrm{GSp}\,(T_\ell(A))$. In the case of $\operatorname{char} k = 0$ we may put these together to obtain $\rho_A : G_k \to \prod_\ell \mathrm{GSp}\,(T_\ell(A)) \cong \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

3.1.5 Story over Number Fields

If K is a number field we have several important structure theorems:

Theorem 3.6. *Let A be an abelian variety over K. Then the group of rational points $A(K)$ is finitely generated. Importantly, the torsion subgroup $A(K)_{\mathrm{tor}}$ is finite.*

Much more deeply lies the following landmark theorem of Falting:

Theorem 3.7. *Let A be an Abelian variety over a number field K. Then there are only finitely many isomorphism classes of Abelian varieties over K isogenous to A. I.E. The* isogeny class *of A is finite.*

This has several important corollaries, notably the Tate-Conjecture for Abelian varieties over number fields:

Theorem 3.8. *Let A, B be abelian varieties over a number field K, and ℓ a prime number such that the representations $\rho_{\ell,A}, \rho_{\ell,B}$ are isomorphic over $\mathbb{Q}_\ell$. Then A and B are isogenous over K.*

Proof. We only present a sketch. Suppose the statement is false, and for simplicity assume that A, B are simple and non-isogenous, and their Tate-modules are isomorphic as $\mathbb{Z}_\ell$-Galois representations. Note that this implies that $A[\ell^n] \cong B[\ell^n]$ as G_K-modules.

Now let $C = A \times B$ and consider the finite subgroups $\Delta_{\ell^n} \subset C$ given b the graphs of the isomorphisms $A[\ell^n] \cong B[\ell^n]$. Then C/Δ_{ℓ^n} give a sequence of Abelia varieties defined over K. Moreover, it is easy to show that these are all pair-wise non-isomorphic, and yet isogenous, which contradicts Theorem 3.8.

The general case involves more bookkeeping but no new ideas. □

Exercise 3.9. Prove that under the assumptions of A, B being simple and non-isogenous, the C/Δ_{ℓ^n} are pairwise non-isomorphic.

Especially noteworthy is that this implies the famous Mordell conjecture:

Theorem 3.10. *Let C be a curve over a number field. Then $C(K)$ is finite.*

Proof. This is a sketch of a construction due to Parshin: Suppose that $C(K)$ is infinite. The proof is in 3 steps:

1. One shows that C has a model as smooth projective curve over $\mathcal{O}_{K,S}$ for some finite subset of primes S, and that consequently $C(K) = C(\mathcal{O}_{K,S}$.

2. By looking at curves ramified over C above $Nc_1 - Nc_2$ for $c_1, c_2 \in C(K)$ one constructs an infinite sequence of curves C_i over $\mathcal{O}_{K,S}$ of the same genus g.

3. The Jacobians J_i of the curves C_i are abelian varieties over K with good reduction outside of S, and therefore by a theorem of faltings there are finitely many isomorphism classes of G_K representations for the ℓ-adic Tate modules.

4. By Theorems 3.8 and 3.7 there are finitely many isomorphisms classes of the J_i, but one can show this is not the case with moduli theory giving a contradiction.

□

3.2 Transcendence Theory

In a series of Papers, D.Masser and G.Wüstholz introduced a powerful tool to study Abelian varieties. Their theorem - which we shall heavily use but say nothing of the proof! - is the following:

Theorem 3.11. *[20] Let A be an abelian variety over K of dimension g, and let B be an abelian variety defined over a finite extension L of K. Suppose that A, B are isogenous over $\overline{\mathbb{Q}}$. Then there exists a $\overline{\mathbb{Q}}$ isogeny between them of degree at most $C_g(h(A), [L:\mathbb{Q}])^{\kappa(g)}$.*

In fact, we may take $h(A)$ to be the faltings height of A with respect to any polarization.

This theorem is so spectacular and robustly useful that it takes a while to appreciate just how powerful it is. Even without the uniformity in L, OR without the uniformity in A (which we would have to learn something about the Faltings height to appreciate), we can already give a different proofs of one of Faltings most important theorems:

Proof. of Theorem 3.7

Let A be an abelian variety over K, and suppose that B is another abelian variety over K isogenous to A. Applying Theorem 3.11 there exists an isogeny $\varphi : A_{\overline{\mathbb{Q}}} \to B_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$ of degree $O(1)$. However, the number of subgroups of $A[\text{tor}]$ of size $O(1)$ is bounded. Since $A_{\overline{\mathbb{Q}}} \ker\varphi \cong B_{\overline{\mathbb{Q}}}$ this automatically means that the number of $\overline{\mathbb{Q}}$-isomorphism classes of B is finite.

However, we may say much more. Fix a finite subgroup $G \subset A$. Then G is defined over a finite Galois extension K_G of K over which B is also defined. Moreover, this gives B a polarization φ of fixed degree D defined over K_G. Now automorphisms groups of Abelian varieties preserving polarization are finite, and therefore the group of twists $H^1(\text{Gal}(K_G/K), \text{Aut}(B, \varphi))$ is also finite, completing the proof.

□

3.3 Manin-Mumford

This proof is extremely analogous to the case of powers of Elliptic curves that we covered in the previous lectures, so we say very little about it. In particular the reductions from $\mathbb{C}$ to $\overline{\mathbb{Q}}$ are identical. The only tricky part is extending the lower bounes of Galois orbits. This can be done in 2 ways:

Theorem 3.12. *[17] Let A be an abelian variety over a number field K and $P \in A(\overline{\mathbb{Q}})$ a torsion point of order n. Then $[K(P) : K] \gg_A n^{\delta_g}$ for a fixed constant $\delta > 0$ depending only on the dimension of A.*

As before this is sufficient for the proofs with Bezout's theorem and the Pila-Zannier method, but it is not enough for equidistribution. However, a result of Wintenberger[33, Thm 3] gives us what we need:

Theorem 3.13. *Let A be an abelian variety over a number field K. Then there exists a constant $c_A > 0$ such that the Galois image $\rho_A(G_K)$ contains the central subgroup $((\hat{\mathbb{Z}})^\times)^{c_A}$.*

3.4 The Andre-Oort Conjecture

3.4.1 Siegel Modular Variety

The Siegel upper-half plane is defined to be

$$\mathbb{H}_g := \{Z \in M_g(\mathbb{C}) \mid Z = Z^t, \operatorname{im} Z \text{ is positive definite}\}$$

There is a natural action of $\operatorname{Sp}_{2g}(\mathbb{R})$ on $\mathbb{H}_g$ given by:

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \cdot Z : \ (AZ+B)(CZ+D)^{-1}$$

Given an element $Z \in \mathbb{H}_g$ one may construct a principally polarized abelian variety by considering the torus $\mathbb{C}^g/\langle I_g, Z\rangle$ where we are quotienting out by the integral lattice spanned by the column vectors. Moreover, the conditions on Z imply that the hermitian form $\langle v, w\rangle = vY^{-1}w^*$ gives a polarization on $\langle I_g, Z\rangle$. We define the *Siegel Modular Variety* to be $\mathcal{A}_g := \operatorname{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$.

Theorem 3.14. *1. The Siegel modular variety $\mathcal{A}_g$ is canonically the (coarse) moduli space of principally polarized complex abelian varieties.*

2. $\mathcal{A}_g$ admits a model of an algebraic variety over $\mathbb{Q}$.

3.4.2 Complex Multiplication

The CM Abelian varieties are precisely those Abelian varieties with as many endomorphisms as possible. What does this mean? There are lots of ways to define it. The most intuitive is as follows: They are exactly those Abelian varieties whose endomorphism ring is large enough to admit no deformations. The formal definitio is as follows:

Definition 3.15. A complex Abelian variety A of dimension g is said to be CM (or have *complex multiplications*) if the endomorphis algebra $\operatorname{End}^0(A) := \operatorname{End}(A) \otimes \mathbb{Q}$ contains a commutative subring R of dimension $2g$ over $\mathbb{Q}$.

Exercise 3.16. By considering the action on $H^1(A, \mathbb{Q})$ or otherwise, prove that $2g$ is the largest possible dimension of a commutative subring of $\operatorname{End}^0(A)$.

If A is a simple abelian variety which is CM, then $\operatorname{End}^0(A)$ is a CM field L: a totally complex quadratic extension of a totally real field K. In this case, the action of L on $H^1(A, \mathbb{C})$ gives a list S of g embeddings $L \to C$ such that $S \cup \overline{S} = \operatorname{Hom}(L, \mathbb{C})$. This is known as a *CM type* and is central to the theory.

The CM abelian varieties compromise the special points in $\mathcal{A}_g$.

3.4.3 Weakly Special and Special Abelian Varieties

To state the Andŕ-Oort conjecture we need to define our analogues of Torsion cosets. These will be our special subvarieties of $\mathcal{A}_g$.

One can give a definition of Special subvarieties in terms of Shimura varieties, but we shall not go down that road. See [21] for references. Instead, we shall give a much quicker definition using functional transcendence. The downside of course is this does not readily make available all of the tools of Shimura Varieties, but luckily these do not play much of a role for us in this lecture.

Definition 3.17. Let $\pi : \mathbb{H}^g \to \mathcal{A}_g$ denote the natural quotient map. Note that $\mathbb{H}^g$ is an open set of the affine space $M_g(\mathbb{C})^{\mathrm{Sym}}$ and the quotient map π is highly transcendental.

1. A closed irreducible subvariety $V \subset \mathcal{A}_g$ is said to be *weakly special* if for some irreducible analytic component W of $\pi^{-1}(V)$ we have $\dim W^{\mathrm{zar}} = \dim V$. Note that the irreducible components all differ by elements of $\mathrm{Sp}_{2g}(\mathbb{Z})$ so this is independent of which component we pick. Equivalently, $\pi^{-1}(V)$ is a *real semialgebraic set.*

2. A weakly special subvariety V is said to be special if it contains a special point. In this case, V will contain a topologically dense set of special points.

The above definitions are of course ad-hoc, but they allow one to work with special varieties quite quickly! Here are several examples.

Example 3.18.

1. All points are weakly special.

2. There is a natural map $Y(1)^g \to \mathcal{A}_g$ whose image is a special subvariety.

3. The Hecke correspondences T_n are special subvarieties of $Y(1)^2$ (when mapped to $\mathcal{A}_2$

4. All the fibers of $Y(1)^n$ over any number of co-ordinates are weakly special

5. For any ring R, the subvariety $S_R \subset \mathcal{A}_g$ of Abelian varieties whose endomorphism ring contains R is special, in that all of its irreducible components are.

More than just being algebraic, for any weakly special subvariety $V \subset \mathcal{A}_g$ and any component W of $\pi^{-1}(V)$ we have that W is a $G(\mathbb{R})$ orbit for some semisimple group $G \subset \mathrm{GSp}$ defined over $\mathbb{Q}$, and is in fact a symmetric domain $G(\mathbb{R})/K_G$ where K_G is a maximal compact subgroup. Hence the analogy with Torsion cosets isn't as far fetched as it first seems!

We are now ready to state the André-Oort conjecture:

Theorem 3.19. *[30] Let $V \subset \mathcal{A}_g$ be an irreducible subvariety. Then V contains finitely many maximal special subvarieties.*

Equivalently, the if the special points in V are Zariski-dense, then V is a special subvariety.

3.5 Galois Orbits

3.5.1 The class group approach

Analogously to the case of Elliptic curves, one may describe Galois orbits of CM Abelian varieties explicitly using Class groups. However a serous obstacle emerges in the higher dimensional case that prevents this approach from working (at least for now!) We describe the picture very briefly (for all the details see [29, 32]).

Let K be a CM field with CM type Φ. Then there is another CM field K^* and a natural map $\psi_S : Cl(K^*) \to Cl(K)$ whose image describes the Galois orbit of the corresponding CM abelian variety. In fact, this map is quite simple: it is simply a product over Galois conjugates $I \to \prod_\sigma \sigma(I)^{n_\sigma}$[3]. Now while Brauer-Siegel results allow us to estimate the sizes of the relevant Class groups extremely precisely, understanding the sizes of **images** is difficult!

Why is this the case? Well, consider the multiplication by n map $\varphi_n : Cl(K) \to Cl(K)$. Then understanding the size of the image amounts to understanding the size of $Cl(K)[n]$. In particular, if we want the image to be large, then we only want to know that the cokernel $Cl(K)/Cl(K)[n]$ is large. But even this is a famously difficult problem! We have very few partial results, and only for low values of n or very special fields K.

In the general setting the maps φ_S are a bit more complicated, so what is involved is class groups of Tori, but the problem really comes down to the issue described above. In particular, it would work if we could resolve the following folklore onjecture, first written down by Zhang:

Conjecture 3.1. *Fix $d, n > 1$. Let K be a number field of degree d. Then $|Cl(K)[n]| = D_k^{o(1)}$*

3.5.2 From Heights to Lower Bounds: Masser-Wüstholz

We've briefly mentioned the Faltings height earlier. It is a canonical height one can assign to a polarized abelian variety $h_{\mathrm{Fal}}(A, \varphi)$. The only currenty known way to obtain lower bounds for Galois orbits of CM points is to relate such bounds to upper bounds for heights of CM points. We shall describe what the Faltings height is, and two (very different!) ways to obtain the reduction.

3.5.3 From Heights to Lower Bounds: o-minimality andn Binyamini+Schmidt+Yafaev

3.5.4 Heights: (Averaged) Colmez Conjecture

3.6 The induction Step: Strongly Special Subvarieties

Once we have the Galois lower bounds in place, the argument proceeds by an induction. It is more complicated then the case of modular curves we dealt with in the previous lecture, but the ideas are the same. The hardest cases are to deal with the strongly special subvarieties, which are the special subvarieties that don't deform in a family of weakly specials. There are two approaches to doing this, which we describe below. Both approaches use the following fact:

Any special subvariety $V \subset \mathcal{A}_g$ and any irreducible component $W \subset \pi_g^{-1}(V)$ satisfies that W is the orbit of $G_W(\mathbb{R})$ for a semisimple $\mathbb{Q}$-group $G_W \subset \mathrm{GSp}_{2g}$.

3.6.1 Equidistribution

The dynamics of semisimple groups actions have been studied by many people, and we shall not attempt to give a history here. See [**?**] for a comprehensive (at the time!) set of references. But the central idea is the following: Let $S_i \subset V$ be a collection of special varieties. Let μ_{S_i} denote the measures supported on S_i whose pullbacks

[3] Of course there are all sorts of details such as if the Endomorphism ring is not maximal, but these end up being handleable

to GSp_{2g} are invariant for the actions of the corresponding semisimple groups G_i as discussed above. The paper [**?**] proves - using the powerful meachinery of measure rigidity developed over the previous decades - that if the G_i keep changing (as they do in the strongly special case) then any weak-* limit of the μ_{S_i} is also a homogenous measure: It is supported on the image F in $\mathcal{A}_g$ of the orbit of a real semisimple group $G \subset \mathrm{GSp}_{2g,\mathbb{R}}$. Moreover, F contains the S_i for large enough i.

However, F is now the image of a real semialgebraic set in $\mathbb{H}_g$ which is contained in V, and the functional tarnscendence machinery means that F is contained in a weakly special - and therefore special since it contains CM points - variety $F_{special}$. But now if we assumed that the S_i were an infinite collection of *maximal* strongly special subvarieties we obtaine a contradiction.

3.6.2 o-minimality

Alternatively, it was later realized that one could use the machinery of o-minimality to accomplish what Clozel-Ullmo did with equidistribution. The idea is as follows:

Even though the (strongly) special subvarieties come in countably many discrete families, the set of analytic semisimple group orbits in $\mathbb{H}_g$ come in finitely many real-analytic families. This is essentially because over the reals, there are finitely many semisimple subgroups of GSp_{2g} up to conjugacy. Now instead of asking for the special varieties contained in V, one simply asks for the semisimple group orbits I that are contained in $\pi_g^{-1}(V)$. This is now a definable set (after appropriate fundamental-domain restrictions) and so the o-minimal theory gives that I has finitely many connected components.

However, the functional transcendence tells us that I is dominated by pre-images of Special varieties! Specifically, the maximal elements in I correspond to pre-images of special varieties in V. Now the definability from o-minimality combines with the discreteness stemming from the parametrization of special subvarieties to give finiteness, and one concludes that there are only finitely many families of maximal weakly special varieties in V, which implies there are finitely many maximal strongly special subvarieties.

4 Lecture #4: Generalizations: Hodge Theory and Mixed Shimura Varieties

4.1 Mixed Shimura Varieties

There is a natural way to combine the Manin-Mumford and André-Oort conjectures. The idea is to consider the universal family of Abelian varieties **over** its moduli space. We then may discuss 2 notions of being special: in the base (being a CM point) or in the fiber (being a torsion point). It is natural to combine the two:

Definition 4.1. We define the *mixed Siegel variety* $\mathbb{A}_g$ to be the universal g-dimensional Abelian variety over $\mathcal{A}_g$. Points of $\mathbb{A}_g$ correspond to isomorphism classes of pairs $(A, P \in A(\mathbb{C}))$ of a principally polarized Abelian variety of dimension g, and a point on it. We say that a point $x \in \mathbb{A}_g$ is *special* if A_x has complex multiplication, and also if P_x is torsion.

It is immediate that special points are dense, countable, and defined over $\overline{\mathbb{Q}}$ just as in our previous analysis. One may likewise characterize special subvarieties as for Shimura varieties. Luckily, this has a fantastic description in this setting: [11, Prop 1.1]

Theorem 4.2. *Let $S \subset \mathbb{A}_g$ be a special subvariety.Then*

1. *The projection of S to $\mathcal{A}_g$ is a special subvariety T*
2. *The universal abelian variety A_T over T has a splitting $A_T \sim B \oplus C$ up to isogeny, such that S is isogenous to the transate of B by a torsion point in C.*

Put simply, the special varieties in $\mathbb{A}_g$ are just torsion cosets over special varieties in $\mathcal{A}_g$. One may formulate an analogous conjecture in this mixed setting, which was proven to be equivalent (via the same Pila-Zannier) strategy to the (pure) shimura setting :

Theorem 4.3. *[12] Let $V \subset \mathbb{A}_g$ be an irreducible subvariety. Then V contains finitely many maximal special subvarieties.*

4.2 Hodge Structures

Shimura Varieties are extremely convenient objects to work with, but they are in many ways rather special. It turns out that Shimura varieties are moduli spaces of very special polarized Hodge structures, and it is very natural to formulate many of our conjectures in this context. We recall some basic notions and refer the interested reader to [7] and [14] for details.

4.2.1 Basic Definitions

Definition 4.4. Fix an integer n. Let $H_{\mathbb{Z}}$ be a finite rank free $\mathbb{Z}$-module. A pure Hodge structure on $H_{\mathbb{Z}}$ of weight n is a decomposition into complex vector spaces

$$H_{\mathbb{C}} := H_{\mathbb{Z}} \otimes \mathbb{C} = \bigoplus_{p+q=n} H^{p,q} \tag{1}$$

satisfying $\overline{H^{p,q}} = H^{q,p}$. The dimensions $h^{p,q} = \dim_{\mathbb{C}} H^{p,q}$ are called the Hodge numbers. We say the Hodge structure is effective if $H^{p,q} = 0$ for $p > n$.

Note that the Hodge structure is determined by the *Hodge filtration*

$$F^p := \bigoplus_{r \geq p} H^{r,s}$$

as $H^{p,q} = F^p \cap \overline{F^q}$. Conversely, a descending filtration $F^\bullet$ determines a Hodge structure of weight n if it satisfies

$$F^p \cap \overline{F^{n-p+1}} = 0 \tag{2}$$

for all p.

Example 4.5. A pure weight 1 (or -1) Hodge structure is equivalent to a compact complex torus T. We canonically have an embedding

$$H_1(T,\mathbb{Z}) \to H^0(T,\Omega^1_T)^\vee \oplus H^0(T,\overline{\Omega}^1_T)^\vee : \gamma \mapsto \int_\gamma$$

which yields a decomposition

$$H_1(T,\mathbb{C}) = H^{-1,0} \oplus H^{0,-1}$$

with $H^{-1,0} = H^0(T,\Omega^1_T)^\vee$ and $H^{0,-1} = \overline{H^{-1,0}}$. Projecting $H_1(T,\mathbb{Z})$ to $H^{-1,0}$ we can recover T canonically by the albanese

$$T \xrightarrow{\cong} H^0(T,\Omega^1_T)^\vee / H_1(T,\mathbb{Z}) : p \mapsto \int_0^p .$$

The weight -1 Hodge structure on $H_1(T,\mathbb{Z})$ naturally induces a weight 1 Hodge structure on $H^1(T,\mathbb{Z})$.

Definition 4.6. Suppose $H_\mathbb{Z}$ carries a weight n Hodge structure, and let $q_\mathbb{Z}$ be a $(-1)^n$-symmetric bilinear form—that is, $q_\mathbb{Z}$ is symmetric if n is even and skew-symmetric if n is odd.

1. The Weil operator $C \in \operatorname{End}(H_\mathbb{R})$ is the real endomorphism satisfying

$$C_\mathbb{C} = \bigoplus_{p,q} i^{p-q} \cdot \mathrm{id}_{H^{p,q}} .$$

2. The *Hodge form* is the hermitian form h on $H_\mathbb{C}$ defined by

$$h(u,v) = q_\mathbb{C}(Cu, \overline{v}).$$

3. We say the Hodge structure is *polarized* by $q_\mathbb{Z}$ if the Hodge form is positive-definite and the decomposition (1) is h-orthogonal.

If the Hodge structure is polarized by $q_\mathbb{Z}$, then the Hodge filtration $F^\bullet$ is $q_\mathbb{C}$-isotropic: we have $(F^\bullet)^\perp = F^{n+1-\bullet}$. Conversely, a $q_\mathbb{C}$-isotropic Hodge filtration satisfying (2) determines a $q_\mathbb{Z}$-polarized Hodge structure if the Hodge form is positive-definite.

Example 4.7. A polarized weight 1 (or -1) Hodge structure is equivalent to a polarized abelian variety A. A skew-symmetric integral form $q_\mathbb{Z}$ on $H_1(A,\mathbb{Z})$ can be thought of as an element $h \in H^2(A,\mathbb{Z})$. By the Lefschetz $(1,1)$ theorem, the $q_\mathbb{C}$-isotropicity condition on the Hodge decomposition implies $h = \mathrm{c}_1(L)$ for a line bundle L on A, and the positivity condition implies L is ample.

Example 4.8. We have the following broad generalization of the previous example, which was the original motivation for their introduction. Let Y be a proper Kähler manifold (for example a smooth complex projective variety). After choosing a Kähler form ω, we obtain a weight n Hodge structure on degree n singular cohomology

$$H^n(Y,\mathbb{C}) = \bigoplus_{p+q=n} H^{p,q}(Y) \tag{3}$$

by decomposing harmonic representatives of de Rham cohomology classes into (p, q) parts. Furthermore, suppose Y is a smooth complex projective variety with ample bundle L and set $h = \mathrm{chern}_1(L)$. The singular cohomology $H^*(Y, \mathbb{Q})$ decomposes into polarized Hodge structures as follows. For $n \leq d = \dim X$, let

$$H^{d-n}_{\mathrm{prim}}(Y, \mathbb{Z}) := \ker \left(h^{n+1} \cup : H^{d-n}(Y, \mathbb{Z})_{\mathrm{tf}} \to H^{d+n+2}(Y, \mathbb{Z})_{\mathrm{tf}} \right).$$

Where $(-)_{\mathrm{tf}}$ denotes the torsion-free quotient. We have

$$H^n(Y, \mathbb{Q}) = \bigoplus_{0 \leq k \leq n/2} h^k \cup H^{n-2k}_{\mathrm{prim}}(Y, \mathbb{Q}).$$

$H^n_{\mathrm{prim}}(Y, \mathbb{Z})$ carries a natural integral form

$$q_n(a, b) := \int_Y h^{\dim Y - 2n} \cup a \cup b.$$

The decomposition (3) (associated to the Kähler class h) then induces a weight n Hodge structure on $H_{\mathrm{prim}}(Y, \mathbb{Z})$ polarized by q_n.

Remark 4.9. Note that if $H_{\mathbb{Z}}$ carries a pure Hodge structure, then so too will any tensor power, symmetric power, wedge power, etc. of $H_{\mathbb{Z}}$. The same is true of pure polarized Hodge structures.

4.2.2 The Mumford–Tate group and CM Hodge Structures

Definition 4.10. Suppose $H_{\mathbb{Z}}$ carries a pure weight $2k$ Hodge structure. An integral (resp. rational) class $v \in H_{\mathbb{Z}}$ (resp. $v \in H_{\mathbb{Q}}$) is *Hodge* if $v \in H^{k,k}$.

Note that an integral class $v \in H_{\mathbb{Z}}$ has pure Hodge type if and only if it is a Hodge class. Moreover, v is Hodge if and only if $v \in F^k$.

Example 4.11. The motivation for considering Hodge classes again comes from geometry. Given a smooth projective complex algebraic variety Y and a closed algebraic subvariety $Z \subset Y$, the fundamental class $[Z] \in H^{2\,\mathrm{codim}\, Z}(Y, \mathbb{Z})$ is a Hodge class. The Hodge conjecture says that moreover all rational Hodge classes arise from cycles (up to rational scaling).

The Hodge classes of a particular Hodge structure are described by the Mumford–Tate group:

Definition 4.12. Suppose $H_{\mathbb{Q}}$ carries a pure Hodge structure H. The (special) Mumford–Tate group $\mathrm{MT}_H \subset \mathbf{Aut}(H_{\mathbb{Q}}, q_{\mathbb{Q}})$ of H is the algebraic $\mathbb{Q}$-subgroup of $\mathbf{End}(H_{\mathbb{Q}})$ with the following property: for any tensor power of weight 0 $H' = H^{\otimes k} \otimes (H^{\vee})^{\otimes - k}$, the rational Hodge classes of H' are precisely the rational vectors fixed by MT_H.

There is another way to describe the $\mathbb{Q}$-group: Let $\mathbb{S}^1 := \mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m$ be the *Deligne-Torus.* Then real representations of $\mathbb{S}^1$ are naturally equivalent to bigradings of a real vector space V by $\mathbb{Z}^2$ such that $V^{p,q} = \overline{V^{q,p}}$. Thus, given a polarized Hodge structure we get a map $\varphi_H : \mathbb{S}^1 \to \mathrm{Aut}(H, q)$ defined over the reals. Then MT_H is the smallest $\mathbb{Q}$-algebraic subgroup which contains the image $\varphi_H(\mathbb{S}^1)$.

Exercise 4.13. 1. Define the equivalence defined above for representations of $\mathbb{S}^1$ and prove it is indeed an equivalence of categories.

2. Prove that, as defined above, the group MT_H does indeed fix precisely the Hodge classes of weight 0.

The fact that this characterizes the Mumford-Tate group is a special case of Tannakian Duality.

In defining the CM Hodge structures, we again want to pick out the ones with enough symmetry that it doens't deform in families. What do symmetries amount to? For abelian varieties A we used the endomorphisms. It turns out that $\mathrm{End}(A) \subset \mathrm{End}(H^1(A, \mathbb{Z}))$ are precisely the hodge classes in the Hodge structure $\mathrm{End}(H^1(A))$. So it is natural to generalize by using hodge tensors as a measure of symmetry. We arrive at the following:

Definition 4.14. A Hodge structure is *CM* iff its Mumford-Tate group is a Torus.

Remark 4.15.

Note that the smaller the Mumford-Tate group is, the more Hodge tensors there are.

For a CM hodge structure H, there is no way to deform the hodge structure of H in a positive-dimensional family while preserving all hodge tensors. Thus, CM hodge structures are *rigid*

Connversely, For any Hodge structure H non-toric Mumford-tate group M, one can deform the Hodge structure on H in a positive-dimensional family while keeping Mumford-Tate group contained in M.

4.2.3 Period domains and period maps

In this section we describe the analogues of Shimura Varieties in the Hodge context. One of the biggest complications in the theory of general hodge moduli spaces over Shimura Varieties is that in general, they do not possess an algebraic structure. This means one does not have a universal family to study, making questions of uniformity very difficult. In addition, basic arithmetic questions (as we shall see!) become very far from tractable.

Define the algebraic $\mathbb{Q}$-group $\mathbf{G}(\mathbb{Q}) = \mathrm{Aut}(H_{\mathbb{Q}}, q_{\mathbb{Q}})$; we will often denote $\mathbf{G}(\mathbb{Z}) = \mathrm{Aut}(H_{\mathbb{Z}}, q_{\mathbb{Z}})$. It is then not hard to see that the space D of $q_{\mathbb{Z}}$-polarized pure weight n Hodge structures on $H_{\mathbb{Z}}$ with specified Hodge numbers $h^{p,q}$ is a homogeneous space for $\mathbf{G}(\mathbb{R})$. Indeed, choosing a reference Hodge structure, we have

$$D = \mathbf{G}(\mathbb{R})/V$$

where V is a subgroup of the compact unitary subgroup $K = \mathbf{G}(\mathbb{R}) \cap U(h)$ of $\mathbf{G}(\mathbb{R})$ with respect to the hodge form of the reference Hodge structure. Moreover, D is canonically an open subset (in the euclidean topology) of $\check{D} = \mathbf{G}(\mathbb{C})/P$, the flag variety parametrizing $q_{\mathbb{C}}$-isotropic Hodge filtrations $F^\bullet$ on $H_{\mathbb{C}}$ with $h^{p,n-p} = \dim F^p/F^{p+1}$.

Definition 4.16. Such a D is called a *polarized period domain.*

Example 4.17. Given a smooth projective morphism $f : Y \to X$, consider the local system $R^k f_* \mathbb{Q}$ for some k. In the notation of Example 4.8, $R^n f_* \mathbb{Z}$ can be decomposed into primitive pieces, and each fiber of $R^n_{\mathrm{prim}} f_* \mathbb{Z}$ carries a pure weight n Hodge structure. By a theorem of Griffiths, the resulting map

$$\varphi : X^{\mathrm{an}} \to \mathbf{G}(\mathbb{Z})\backslash D : y \mapsto [H^n_{\mathrm{prim}}(X_y, \mathbb{Z})]$$

is holomorphic and locally liftable to D.

The fundamental observation of Griffiths is that we cannot get arbitrary maps to $\mathbf{G}(\mathbb{Z})\backslash D$ from geometry as in Example 4.17. Indeed, only certain tangent directions of D are accessible to algebraic families. To make this precise, fix a point $x \in D$ and note that a deformation of the Hodge filtration at x in particular yields a deformation of each F^p_x, so we have a natural map

$$T_x D \to \bigoplus_p \mathrm{Hom}(F^p_x, H_{\mathbb{C}}/F^p_x) \tag{4}$$

Definition 4.18. The Griffiths transverse subspace $T^{GT}_x D \subset T_x D$ is the inverse image of $\bigoplus_p \mathrm{Hom}(F^p_x, F^{p-1}/F^p_x)$ under the map in (4).

In other words, to first order each F^p is only deformed inside F^{p-1}. The Griffiths transverse subspaces assemble into a holomorphic subbundle $T^{GT} D \subset TD$.

Remark 4.19. Each pure polarized Hodge structure $x \in D$ on $H_{\mathbb{Z}}$ naturally induces a pure polarized Hodge structure on the Lie algebra $\mathfrak{g}_{\mathbb{R}} \subset \mathrm{End}(H_{\mathbb{R}})$ of weight 0, which we call $\mathfrak{g}_x$. Denote its Hodge filtration by $F^\bullet_x \mathfrak{g}_{\mathbb{C}}$. The Lie algebra of the stabilizer $P_x \subset \mathbf{G}(\mathbb{C})$ of $x \in \check{D}$ is then naturally $F^0_x \mathfrak{g}_{\mathbb{C}}$. Thus, the tangent space $T_x D$ is naturally (and holomorphically) identified with $\mathfrak{g}_{\mathbb{C}}/F^0_x \mathfrak{g}_{\mathbb{C}}$. The Griffiths transverse subspace is $F^{-1}_x \mathfrak{g}_{\mathbb{C}}/F^0_x \mathfrak{g}_{\mathbb{C}}$.

Definition 4.20. By a period map we mean a holomorphic locally liftable Griffiths transverse map

$$\varphi : X^{\mathrm{an}} \to \Gamma\backslash D$$

for a smooth complex algebraic variety X and a finite index $\Gamma \subset \mathbf{G}(\mathbb{Z})$.

Remark 4.21. A period map $\varphi : X^{\mathrm{an}} \to \mathbf{G}(\mathbb{Z})\backslash D$ is equivalent to the data of a pure polarized integral variation of Hodge structures on X. This consists of:

- A local system $\mathscr{H}_{\mathbb{Z}}$ with a flat quadratic form $Q_{\mathbb{Z}}$.
- A holomorphic locally split filtration $F^\bullet$ of $\mathscr{H}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{O}_{X^{\mathrm{an}}}$ such that the flat connection ∇ satisfies Griffiths transversality:

  $$\nabla(F^p) \subset F^{p-1} \text{ for all } p.$$

- We moreover require that $(\mathscr{H}_{\mathbb{Z}}, Q_{\mathbb{Z}}, F^\bullet)$ is fiberwise a pure polarized integral Hodge structure.

The period map lifts to $\Gamma\backslash D$ if Γ contains the image of the monodromy representation of $\mathscr{H}_{\mathbb{Z}}$.

We now defie the analogues of special and weakly-special subvarieties:

Definition 4.22. Let D be a polarized period domain.

1. A weak Mumford–Tate subdomain D' of D is an orbit $M(\mathbb{R})x$ where $x \in D$ and M is a normal algebraic $\mathbb{Q}$-subgroup of MT_x. In fact, D' is a smooth complex submanifold of D, and it is an irreducible component of the locus of Hodge structures H such that $\mathrm{MT}_H \supset M$.

2. If moreover $M = \mathrm{MT}_x$, then $D' = M(\mathbb{R})x$ is called a Mumford–Tate subdomain.

3. Let $\pi : D \to \Gamma\backslash D$ be the quotient map. For $D' \subset D$ a (weak) Mumford–Tate subdomain, $\pi(D') \subset \Gamma\backslash D$ is a complex analytic subvariety which we call a (weak) Mumford–Tate subvariety. Likewise, given a period map $\varphi : X^{\mathrm{an}} \to \Gamma\backslash D$, we call $\varphi^{-1}\pi(D')$ a (weak) Mumford–Tate subvariety of X.

Given Definition 4.12, we see that we can also think of a Mumford–Tate subdomain as a component of the locus of Hodge structures for which some number of rational tensors are Hodge.

Theorem 4.23 (Theorem 1.6 of [8])**.** *Let $\varphi : X^{\mathrm{an}} \to \Gamma\backslash D$ be a period map. Then any weak Mumford–Tate subvariety of X is algebraic.*

4.3 André-Oort Conjecture for Hodge Structures: Arithmetic Issues

Since we have no universal family, we must formulate our conjectures for individual families of Hodge structures. We give the following, but a precise formulation may be found in []klingler-conjectures:

Conjecture 4.1. *Let V be an irreducible complex variety, and $\varphi : V \to \Gamma\backslash D$ be a period map. Suppose that V has a Zariski-dense set of points whose image is CM. Then $\varphi(V)$ is a Mumford-Tate variety. In fact, $\varphi(V)$ must be isomorphic to a Shimura Variety via a 'Hodge Morphism'.*

One of the serious difficulties (very likely the primary difficulty) with this conjecture is the lack of understanding regarding the Galois structure. In fact, we do not even know that the CM points on V are defined over $\overline{\mathbb{Q}}$ (or, for that matter, that V must be defined over $\overline{\mathbb{Q}}$).

The problem is that due to their transcendental nature, we do not have a good notion of an action of $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ on isomorphism classes of Hodge structures. Note that we had such an action for Abelian varieties only via their algebraic co-ordinates, which are highly transcendental on the period domain. For instance, for elliptic curves we used the transcendental j-function.

To set things up geometrically, suppose that $Y/\mathbb{C}$ is an algebraic variety and $\sigma \in \mathrm{Aut}(C/\mathbb{Q})$. Then we have a Hodge structure $H^k_{\mathrm{prim}}(Y)$. Now by considering $\sigma(Y)$ we obtain another Hodge structure $H^k_{\mathrm{prim}}(\sigma(Y))$ of the same type, and it is very tempting to define $\sigma(H^k_{\mathrm{prim}}(Y))$ to be $H^k_{\mathrm{prim}}(\sigma(Y))$. However, this runs the risk of not being well-defined. Hypothetically, we might have another variety $Y'/\mathbb{C}$ such that $H^k_{\mathrm{prim}}(Y)$ and $H^k_{\mathrm{prim}}(Y')$ were isomorphic but $H^k_{\mathrm{prim}}(\sigma(Y))$ and $H^k_{\mathrm{prim}}(\sigma(Y'))$ were not.

Proposition 4.24. *The Hodge conjecture implies that if Y, Y' are smooth projective varieties and $\sigma \in \mathrm{Aut}(C/\mathbb{Q})$, then $H^k_{\text{prim}}(Y) \cong H^k_{\text{prim}}(Y')$ implies that $H^k_{\text{prim}}(\sigma(Y)) \cong H^k_{\text{prim}}(\sigma(Y')$*

Proof. The isomorphism defines a Hodge class in

$$H^k_{\text{prim}}(Y, \mathbb{Q}) \cong H^k_{\text{prim}}(Y', \mathbb{Q})^\vee \subset H^{2k}(Y \times Z, \mathbb{Q}).$$

By the Hodge conjecture this class is represented by an algebraic subvariety $W \subset Y \times Z$. Now one simply shows that $\sigma(W)$ defines an isomorphism $H^k_{\text{prim}}(\sigma(Y)) \cong H^k_{\text{prim}}(\sigma(Y')$. This is clear, since this can be checked at the level of Etale cohomology, which is purely algebraic. □

It turns out that there is a weaker notion of the Hodge conjecture, formulated by Deligne, which is slightly more natural:

Conjecture 4.2. *Suppose that Y is a smooth projective variety and $\sigma \in \mathrm{Aut}(\mathbb{C})$. Let $v \in H^k_{\text{prim}}(Y, \mathbb{Z})$ be a Hodge class. By considering the image of v in De-Rham cohomology we obrain a class $\sigma(v) \in H^k_{\text{prim}}(Y, \mathbb{C})$. Then $\sigma(v)$ is also a Hodge class. In particular, $\sigma(v)$ lies in $H^k_{\text{prim}}(Y, \mathbb{Q})$.*

It can be shown (in much the same way as above) that the Hodge conjecture implies the Absolute Hodge Conjecture. Moreover, given the Absolute Hodge conjecture we get a well defined action of $\mathrm{Aut}(\mathbb{C})$ on the geometric Hodge classes in $\Gamma\backslash D$. Finally, we get the following very nice corollary:

Corollary 4.25. *Assume the Absolute Hodge Conjecture 4.2. Let V be a $\overline{\mathbb{Q}}$-variety with a smooth projective family $Y \to V$ over it. Then the locus of points $v \in V$ such that $H^k_{\text{prim}}(Y_v)$ is a CM Hodge structure is countable, and defined over $\overline{\mathbb{Q}}$.*

The above statement is open unconditionally, even for very low-dimensional cases like $k = 2$ for families of surfaces defined over a curve. Any progress towards it would be of extreme importance.

4.4 Mixed Hodge Structures

Finally, we mention that by considering mixed Hodge structures, we may generalize the setting of Mixed Shimura Varieties. Rather than give the precise definitions, we illustrate by describing some specific geometric examples.

Example 4.26. Consider $Y \to X$ where $X = \mathbb{G}_m$ and $Y = X \times X$ and $Z := \{1\} \times X \cup \Delta_X$ Then the fiber of (Y, Z) over a point $p \in X$ is $(\mathbb{G}_m, \{1, p\}$. We now consider the **relative** cohomology $H^1(Y_p; Z_p)$. This now has the structure of a mixed Hodge structure, and it is an extension of the pure structure $\mathbb{Z}(0)$ by the pure structure $\mathbb{Z}(1)$. It is split as a direct sum precisely at $p = 1$, and it turns out to have extra hodge tensors precisely when p is a root of unity. Thus, this allows us to reframe Lang's conjecture in the context of a Mixed André-oort conjecture for (the powers of) this family.

5 Group Projects

5.1 Independence of CM points in Abelian Varieties

The idea behind this project is the incompatibility of the algebraic structure of CM points on the one hand, and the additive structure in Abelian Varieties on the other. In [6] The authors consider a correspondence $V \subset E \times S$ where E is an elliptic curve and S is a Modular curve. They prove many results, but notably the following theorem:

Theorem 5.1. *Let $\Gamma \subset E$ be a finitely generated group, and let Γ' be its division group. Then the intersection $V \cap \Gamma' \times S_{CM}$ is finite.*

One idea they use is as follows:

1. Reduce to a number field by specialization arguements.
2. Galois orbits of CM points are large, so the points in Γ' must have large Galois orbits also.
3. Equidistribution results now give that a weak-* limit of the Galois orbits projects to Haar measure in both variables
4. The cusp makes this incompatible with the measure being supported on V.

The same idea works for several other variants (such as morphisms from a shimura curve to an Abelian variety) and the authors give many many generalizations, including to points of low height and various other p-adic analogues.

In [24, Cor 1.2]this result is generalized to take into account all Γ of bounded rank at once:

Theorem 5.2. *consider a correspondence $V \subset E \times S$ where E is an elliptic curve and S is a Shimura curve. Fix a positive integer r.*

1. *There exists a positive integer N such that if T is a collection of r CM points of discriminant at least N, with no isogenies of degree $\leq N$ between them, then the elements of $V(T) := \pi_E(\pi_S^{-1}(T))$ are linearly independent.*
2. *If $\Gamma \subset E$ is a group of rank r, then the number of CM points with a V-image in Γ' is at most $N(r)$, independently of Γ.*

The problem is re-cast there as an unlikely intersection problem, with a key observation being that $(P_1, \dots, P_r) \in E^r$ are linearly independent if they do not lie in a proper abelian subvariety of E^r. The result then follows from an Ax-Schanuel theorem, as well as lower bounds for Galois orbits.

The project here would be to generalize the result in [24] to correspondences between arbitrary Shimura varieties and arbitrary Abelian varieties. The goal would be something like the following:

Conjecture 5.1. *Let S be a shimura variety and A an abelian variety, and $V \subset S \times A$ a proper irreducible subvariety, dominant on each factor, finite over S Consider the subset $W \subset S_{CM}^r$ of CM points whose V-images in A are linearly dependent. Then*

1. W is contained in finitely many shimura varieties

2. If $\Gamma \subset A$ is a group of rank r, then the number of CM points with a V-image in Γ' is contained in a union of at most $N(r)$ proper special subvarieties, independently of γ'.

One may of course hope for stronger finiteness results but this is the direction we would be heading in. Studying both [6, 24] would be crucial for this project, and there are many places to start:

1. Consider low-dimensional cases, such as $S = Y(1) \times Y(1)$ or $S = \mathcal{A}_2$ and $\dim A = 2$, with V being induced by a morphism. Also considering $r = 1$ should greatly simplify the structure of special varieties. Also start by assuming A is defined over $\overline{\mathbb{Q}}$ .Already here the result would be interesting!

2. Use the Galois orbits bounds from [31] to generalize the results in [24, §5], and read the corresponding papers of Masser[18] for the heights on abelian varieties part.

3. In another direction, I think one the theorem in [24, Cor 1.2] is highly inoptimal, and I wonder if one could remove the need to consider isogenies in the definition of N-independence. This would involved understanding whether it is POSSIBLE in a non-constant map $\varphi : Y(1) \to E$ and $N > 1$ to have $\varphi(T_N) \subset E^2$ contained in a proper abelian coset. This is more of a geometric question and I am not sure of the answer, but I suspect it is “no”, and it would be interesting either way!

5.2 Obtaining/effectivizing explicit exponents for Galois lower bounds

This question is focused on the following problem:

Question 5.3. *Let $g, d > 1$. Let A be a g-dimensional (principally polarized?) Abelian Variety, with Discriminant D. Let $\mathbb{Q}(A)$ be its field of definition. What is the ‘best’ bound of the form $[\mathbb{Q}(A) : \mathbb{Q}] \geq a(g)|D|^{b(g)}$?*

- *How large can $b(g)$ be, either provably or conjectured?*
- *Can this be effectivized, either GRH or unconditionally?*
- *How many CM abelian varieties are there defined over $\mathbb{Q}$ of dimension g?*

This question was open for a long time, except in the case of Elliptic curves where it is settled (ineffectively unless you assume GRH) by ther Brauer-Siegel theorem, as discussed in Lecture #2. In higher degree, the question was studied by relating Galois orbits to sizes of maps between Class groups of Tori (see [29, 32] for results and details). That approach turns out to be quite difficult because it relates to bounds for Torsion in Class groups, which is a very difficult open problem. Such bounds are not required up to $g = 3$, and are sufficiently obtainable up to $g = 6$, but beyond that this approach fails. Nevertheless, if one assumes the following folklore conjecture (first made by Zhang(this approach becomes very feasible:

Conjecture 5.2. *Fix $d, n > 1$. Let K be a number field of degree d. Then $|Cl(K)[n]| = D_k^{o(1)}$*

This approach would involve understanding Discriminants of Tori over number fields, and the reflex norm-maps for distinct CM types:

Question 5.4. *Assume Zhang's conjecture. What is the largest possible value of $b(g)$?*

The references given say something of the following type: Given a CM field K, one obtains a 'norm' map $Cl(K^*) \rightarrow Cl(K)$ between the class groups of the reflex field of K and K. This can be obtained through a map of tori $\varphi : \mathrm{Res}_{K^*/\mathbb{Q}} \mathbb{G}_m \rightarrow \mathrm{Res}_{K/\mathbb{Q}} \mathbb{G}_m$, and the relevant factor is essentially the size of the discriminant of the Torus which is the image of T. How small can this be in terms of ths discrimiant of T??

Alternatively, a polynomial lower bound for Galois orbits of CM abelian varieties was obtained in [31], but an explicit exponent has not been worked out or at all optimized. This would involve understanding the various ingredients in the proof, and attempting to trace through an explicit exponent. Relevant is the work of Masser-Wüstholz([20] and several others) which is used to obtain isogeny estimates. The methods of [4] might be relevant, and related is [22] who study a related question for K3 surfaces.

If this goes very well, a potential direction for this project would be to try and classify all CM abelian varieties of dimension g defined over $\mathbb{Q}$, in an analogous way to the class number one problem, which was solved effectively by Goldfeld[13].

5.3 Good reduction of CM points

Remark 5.5. **This is definitely the most difficult and speculative project! Very interesting and a great opportunity to learn a lot of material, but could very well be genuinely too difficult or even false!**

One of the central properties of CM abelian varieties is that they have good reduction everywhere. One may reformulate this for $\mathcal{A}_g$ by providing a scheme over $\mathbb{Z}$. by saying (roughly) that the CM points all extend to $\mathcal{O}_K$ points of $\mathcal{A}_g$ for some number field K. This requires picking an integral model, so an even more intrinsic formulation is the following:

1. For every p there are subsets of $U_p \subset \mathcal{A}_g(\overline{\mathbb{Q}}_p)$ which are finite unions of affinoids that the CM points all land in U_p for every p
2. For almost every p one may take U_p to be the points corresponding to a model of $\mathcal{A}_g$. This is independent of the model.

For arbitrary Shimura varieties one may try to formulate the same question, except integral canonical models are far from known at all places. This question comes up in [2, §5] but is sidestepped for the 'bad primes' - so that (2) is known but (1) is not. But it may not be that hard, and just follow from unipotent properties of inertia representations - I just don't know!

For the abelian variety case useful background reading could be the paper of Serre and Tate [28] and the theory of Complex Multiplication. Moreover Milne[21]. The main thing to read is definitely [2, §5] and the background therein.

This project has much relevance to, but little overlap with, the lecture material, and will rely heavily on p-adic geometry, Galois theory, Etale cohomology, and some comfort with abstract Shimura Varieties.

References

[1] Yves André. Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire. *J. Reine Angew. Math.*, 505:203–208, 1998.

[2] J.Pila with appendix by H.Esnault M.Groechenig A.Shankar, J.Tsimerman. Canonical heights on shimura varieties and the andré-oort conjecture.

[3] B.Edixhoven. Special points on the product of two modular curves.

[4] Gal Binyamini and David Masser. Effective André-Oort for non-compact curves in Hilbert modular varieties. *C. R. Math. Acad. Sci. Paris*, 359:313–321, 2021.

[5] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[6] Alexandru Buium and Bjorn Poonen. Independence of points on elliptic curves arising from special points on modular and Shimura curves. I. Global results. *Duke Math. J.*, 147(1):181–191, 2009.

[7] J. Carlson, S. Müller-Stach, and C. Peters. *Period mappings and period domains*, volume 85 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2003.

[8] E. Cattani, P. Deligne, and A. Kaplan. On the locus of Hodge classes. *J. Amer. Math. Soc.*, 8(2):483–506, 1995.

[9] Bas Edixhoven. Special points on products of modular curves. *Duke Math. J.*, 126(2):325–348, 2005.

[10] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.

[11] Ziyang Gao. A special point problem of André-Pink-Zannier in the universal family of Abelian varieties. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 17(1):231–266, 2017.

[12] Ziyang Gao. Towards the Andre–Oort conjecture for mixed Shimura varieties: The Ax–Lindemann theorem and lower bounds for Galois orbits of special points. *J. Reine Angew. Math.*, 732:85–146, 2017.

[13] Dorian Goldfeld. The Gauss class number problem for imaginary quadratic fields. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 25–36. Cambridge Univ. Press, Cambridge, 2004.

[14] M. Green, P. Griffiths, and M. Kerr. *Mumford-Tate groups and domains*, volume 183 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2012.

[15] Ilya Khayutin. Joint equidistribution of CM points. *Ann. of Math. (2)*, 189(1):145–276, 2019.

[16] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[17] D. W. Masser. Small values of the quadratic part of the Néron-Tate height on an abelian variety. *Compositio Math.*, 53(2):153–170, 1984.

[18] D. W. Masser. Linear relations on algebraic groups. In *New advances in transcendence theory (Durham, 1986)*, pages 248–262. Cambridge Univ. Press, Cambridge, 1988.

[19] David Masser. *Elliptic functions and transcendence*. Lecture Notes in Mathematics, Vol. 437. Springer-Verlag, Berlin-New York, 1975.

[20] David Masser and Gisbert Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[21] J. S. Milne. Shimura varieties and moduli. In *Handbook of moduli. Vol. II*, volume 25 of *Adv. Lect. Math. (ALM)*, pages 467–548. Int. Press, Somerville, MA, 2013.

[22] Martin Orr and Alexei N. Skorobogatov. Finiteness theorems for K3 surfaces and abelian varieties of CM type. *Compos. Math.*, 154(8):1571–1592, 2018.

[23] Jonathan Pila. O-minimality and the André-Oort conjecture for $\mathbb{C}^n$. *Ann. of Math. (2)*, 173(3):1779–1840, 2011.

[24] Jonathan Pila and Jacob Tsimerman. Independence of CM points in elliptic curves. *J. Eur. Math. Soc. (JEMS)*, 24(9):3161–3182, 2022.

[25] M. Raynaud. Courbes sur une variété abélienne et points de torsion. *Invent. Math.*, 71(1):207–233, 1983.

[26] M. Raynaud. Sous-variétés d'une variété abélienne et points de torsion. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 327–352. Birkhäuser Boston, Boston, MA, 1983.

[27] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[28] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[29] Jacob Tsimerman. Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points. *J. Amer. Math. Soc.*, 25(4):1091–1117, 2012.

[30] Jacob Tsimerman. The André-Oort conjecture for $\mathcal{A}_\}$. *Ann. of Math. (2)*, 187(2):379–390, 2018.

[31] Jacob Tsimerman. The André-Oort conjecture for $\mathcal{A}_\}$. *Ann. of Math. (2)*, 187(2):379–390, 2018.

[32] Emmanuel Ullmo and Andrei Yafaev. Nombre de classes des tores de multiplication complexe et bornes inférieures pour les orbites galoisiennes de points spéciaux. *Bull. Soc. Math. France*, 143(1):197–228, 2015.

[33] J.-P. Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553:1–16, 2002.