Integer points on complements of dual curves and on genus one modular curves

Ryan Christopher Chen

a senior thesis submitted in partial fulfillment
of the requirements for the degree of
Bachelor of Arts in Mathematics at
Princeton University

Adviser: Shou-Wu Zhang

June 2019[1]

[1] (July 2024) This work would benefit from revision. This is an original unrevised version from 2019.

Abstract

Higher dimension analogs of Siegel's theorem on the finiteness of integer points are known in limited cases and often come with restrictions on the divisor at infinity, e.g. that the divisor should have many irreducible components. In the first half of this thesis, we give a new class of prime divisors in the plane, namely duals of certain smooth plane curves, whose complements have finitely many integer points. This is accomplished using a moduli of curves interpretation. In the second half of this thesis, we give a proof of the finiteness of integer points on genus one modular curves. This result is not new, but the proof we give is based on the p-adic period map and ideas from a recent new proof of the Mordell conjecture by Lawrence and Venkatesh.

Acknowledgements

I express sincere thanks to my adviser Shou-Wu Zhang – his guidance has been generous and inspirational. I also acknowledge Akshay Venkatesh for a helpful discussion regarding this thesis.

I give thanks to Christopher Skinner for his teaching and advising. I am grateful for John Duncan, Florian Frick, Steven J. Miller, and Ken Ono for their formative mentorship, and acknowledge the Princeton math department for its support. I also thank my professors including Matt Baker, Francesc Castella, Robert Gunning, Alexandru Ionescu, Mark McConnell, and Zoltán Szabó for their support. I appreciate my peers and their friendship.

I thank my parents and my brother Eric for their enduring support and encouragement.

Declaration

I declare that I have not violated the Honor Code during the composition of this work. This paper represents my own work in accordance with University regulations.

I authorize Princeton University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purposes of scholarly research.

Contents

Chapter 1

Introduction

Let K be a number field and S a finite set of primes in its ring of integers. Siegel's theorem asserts that any affine curve over K containing infinitely many S-integer points has genus zero, and has at most two points at infinity [8, 50]. Analogous results for finiteness of integer points on higher dimensional varieties are less complete. There is a theorem of Faltings [19] which states that the complement of an ample divisor on an abelian variety contains only finitely many S-integer points; this was later generalized to the semiabelian case by Vojta [55]. Outside of semiabelian varieties less is known, and many theorems require that the divisor at infinity split into several components. For example, there is a result of Vojta [54, Theorem 2.4.1] on Zariski non-density of S-integer points which imposes a lower bound on the number of components of this divisor based on the Picard number and rank of K-rational points in the Picard variety. Some theorems of Levin [38] have similar requirements, e.g. for surfaces that the divisor at infinity consists of at least 5 ample prime divisors in general position; see also [7] for further results of this type. For prime divisors, there are results of Faltings [17], Zannier [59], and Levin [38] that prove finiteness of S-integer points on the complements of certain singular plane curves. However, these results impose, in addition to various ampleness conditions, that the curve has only simple cuspidal or nodal singularities.

Our main result in the first half of this thesis is to give a new class of irreducible divisors in $\mathbb{P}^2$ whose complements have finitely many S-integer points; these produce affine surfaces with finitely many S-integer points.

Theorem 1.0.1. *Let $C \to \mathbb{P}^2$ be a smooth plane curve over K with has non-prime degree $d \geq 6$, and with no d-fold or $(d-1)$-fold tangent lines. Select a homogeneous equation $g(a, b, c)$ with integer coefficients that defines the dual plane curve C^*. The complement of this curve in $\mathbb{P}^2$ has finitely* *many S-integer points.*

See Theorem 2.2.4 and subsequent discussion for a more precise statement. The condition on tangent lines will hold generically, and includes dual curves not covered by [17, 38, 59], see Remark 2.2.5.

The theorem is proved using a moduli interpretation of the complement of the dual curve; we construct and study a family of cyclic $\mathbb{P}^1$-covers over this space. This allows us to reduce the theorem to the Shafarevich conjecture on good reduction of curves outside some finite set of primes. Such use of a moduli interpretation also appears in Faltings's proof [16] of the Mordell conjecture, on finiteness of rational points of curves with genus at least two. The proof uses the Parshin construction [47] on such curves to reduce the Mordell conjecture to the Shafarevich conjecture, which Faltings then proved.

In the second half of the thesis, we use the moduli interpretation of open modular curves to show finiteness of their integer points. Such results are not new; for example, they are consequences of Siegel's theorem and of the Shafarevich conjecture. The proof that we give, however, is based on the techniques from a recent new proof of the Mordell conjecture [36]. We adapt these techniques to genus one modular curves and study the variation of Galois representations using the complex and p-adic period map. In this way, we are able to deduce finiteness of integer points.

Theorem 1.0.2. *Let N be an integer so that the compactified modular curve $X_1(N)$ is genus one. Let $\mathcal{Y}$ be the corresponding open modular curve, defined over the ring of S-integers. Then $\mathcal{Y}$ has finitely many S-integer points.*

See Theorem 3.0.1 and Theorem 3.0.2 for a more precise statement.

We now describe the organization of this thesis. In Chapter 2, we prove Theorem 1.0.1. Section 2.1 consists of brief preliminaries on families of curves and the moduli space of genus g curves. In Section 2.2, we first discuss a concrete interpretation of Theorem 1.0.1 as a finiteness result for affine surfaces, and discuss curves satsifying the conditions of the theorem. We then describe dual curves over a general base. Afterwards we use this theory to construct and study smooth families of curves over $\mathbb{P}^2$ minus the dual curve, defined over the ring of S-integers; this study yields the desired finiteness result. In Chapter 3, we prove Theorem 1.0.2 using the p-adic period map. We first briefly record some preliminary facts about the period map in Section 3.1, then discuss and use in Section 3.2 an elliptic curve group structure on genus one modular curves over the S-integer ring. In Section 3.3, we use the theory of period maps and explicit computations on the modular curve to conclude the desired finiteness result.

To conclude the introduction, we fix some notation.

Notation 1.0.3. All schemes are assumed to be separated.

K a number field

S a finite set of primes of the ring of integers $\mathcal{O}_K$ of K which contains the archimedean places

$\mathcal{O}$ the ring of S-integers

$k(x)$ for the residue field of $x \in X$ for a scheme X

$X(Y)$ for $\mathrm{Hom}_T(Y, X)$, where T is an understood base-scheme

We also use $X(Y)$ to denote the subset of X consisting of points that lie in the set-theoretic image of some $f \in X(Y)$. For example, if X is finite type over an algebraically closed field k, $X(\operatorname{Spec} k)$ may denote the closed points of X.

X_Z for $X \times_Y Z$ when $X \to Y$ and $Z \to Y$ are understood morphisms of schemes

X_y for the fiber of $X \to Y$ above $y \in Y(Z)$; e.g. when Z is the spectrum of an algebraically closed field

We often replace $\operatorname{Spec} A$ with A, e.g. $X(A)$ instead of $X(\operatorname{Spec} A)$, X_L instead of $X_{\operatorname{Spec} L}$, etc.

Notation 1.0.4. This notation is used in Chapter 3.

L a finite Galois extension of the number field K

v a prime of K unramified in L and lying over a rational prime p; assume $K_v/\mathbb{Q}_p$ is unramified

$\mathcal{O}_v$ the ring of integers of K_v

w_i the primes of L lying above v

X^σ the pullback of $X \to \operatorname{Spec} L$ along $\operatorname{Spec} L \xrightarrow{\sigma} \operatorname{Spec} L$ for $\sigma \in \operatorname{Gal}(L/K)$

$P \equiv Q \pmod{v}$ for $v \notin S$ and for sections P, Q of $X \to \operatorname{Spec} \mathcal{O}$ which agree upon pullback along $\operatorname{Spec} k(v) \to \operatorname{Spec} \mathcal{O}$

$[\ell]$ for multiplication by ℓ on a group scheme X, and $X[\ell]$ for pullback of the identity section along $X \xrightarrow{[\ell]} X$; when clear, we may write ℓ instead of $[\ell]$

$\operatorname{Res}_{E/F}$ the Weil restriction, where E/F is a finite field extension

G_E the absolute Galois group $\operatorname{Gal}(\overline{E}/E)$ for a field E

$\operatorname{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(G_E)$ the category of crystalline $\mathbb{Q}_p$-representations of G_E for E a characteristic zero local field of residual characteristic p

MF^{ϕ}_E where E is an unramified finite extension of $\mathbb{Q}_p$ with Frobenius automorphism σ, and MF^{ϕ}_E is the category of triples (V, ϕ, Fil) where V is a finite dimensional E vector space with a σ-semilinear automorphism ϕ; Fil is an exhaustive, separated, decreasing filtration on V

$T_p(A)$ the p-adic Tate module, for an abelian variety A

$V_p(A)$ for $T_p(A) \otimes \mathbb{Q}$

Chapter 2

Integer points on complements of dual curves

Given a smooth plane curve C over K of non-prime degree $d \geq 6$ without d-fold or $(d-1)$-fold tangents, we prove that the complement of its dual curve can have only finitely many integer points. For a precise statement, see Theorem 2.2.4 below.

We now give a brief description of the general idea. We construct cyclic covers of $\mathbb{P}^2$ branched at C. Any line in $\mathbb{P}^2$ will pull back to a cyclic cover of $\mathbb{P}^1$, and such a curve is singular if and only if the line was tangent to C. This construction thus induces a family of smooth curves on the complement of the dual curve. We may then apply the moduli space theory for curves and the Shafarevich conjecture on good reduction of curves to this family. This reduces the proof of the theorem to ruling out isotriviality on positive dimension components, which is verified in Section 2.2.3.

2.1 Preliminaries

We begin by fixing some notions and conventions regarding algebraic families of curves, i.e. curves over a general base-scheme. These notions will also be used regularly in Chapter 3. Curves over general schemes facilitate our discussion of families of curves, as well as our study of the dual curve over the ring $\mathcal{O}$.

Definition 2.1.1. Let Y be a scheme over a base-scheme T. Morphisms are understood to be over T.

- By a *geometric point* of Y, we mean a morphism $\operatorname{Spec} k \to Y$, where k is an algebraically closed field.
- Let k be an algebraically closed field. We use *curve* to refer to a projective curve (unless otherwise specified), i.e. an integral, dimension one scheme which is proper over $\operatorname{Spec} k$.
- By a *relative curve* or *curve* over Y, we mean a flat proper morphism $X \to Y$ whose geometric fibers are curves. If the morphism is moreover smooth, we say the relative curve is smooth (but may omit this, if smoothness is understood).
- By a *relative smooth genus g curve*, we mean a relative smooth curve whose geometric fibers have fixed genus g.
- If a relative smooth genus 1 curve over Y has a fixed section (i.e. an "identity section"), we say it is an *elliptic curve* over Y.
- Let $X \to Y$ be a relative curve, where X and Y are finite type over T. We say the relative curve is *defined over T*.
- If a relative curve defined over an algebraically closed field has all fibers over closed points isomorphic, we say the curve is *isotrivial*.
- Let $X \to Y$ be a relative curve, and fix a closed immersion $X \to \mathbb{P}^n_Y$. If Y is integral and noetherian, we take the *degree* of the relative curve to be the degree of $X_{k(y)} \subseteq \mathbb{P}^n_{k(y)}$ for any choice of $y \in Y$. This is well-defined by flatness, i.e. it is independent of the choice of y [27, Theorem III.9.9].
- Given a smooth curve $X \to K$, we say it has *good reduction* at a prime v of K there is a smooth curve $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_{K,v}$ recovering $X \to K$ upon base-change, where $\mathcal{O}_{K,v}$ is the localization of $\mathcal{O}_K$ at v. We use the same terminology if K is replaced with a non-archimedean local field and $\mathcal{O}_{K,v}$ is replaced with the appropriate ring of integers.

Consider a relative smooth genus g curve $\mathcal{X} \to \mathcal{Y}$ defined over $\mathcal{O}$. For any $y \in \mathcal{Y}(\mathcal{O})$, the fiber $\mathcal{X}_y$ is a proper smooth $\mathcal{O}$-scheme, i.e. the smooth genus g curve $(\mathcal{X}_y)_K$ over K has good reduction outside of S. We may then seek to bound $\mathcal{Y}(\mathcal{O})$ using the following tools.

Theorem 2.1.2 (Faltings)**.** *For fixed g and S, there are finitely many isomorphism classes of smooth genus g curves over K with good reduction outside of S.*

Theorem 2.1.2 was a conjecture due to Shafarevich [56], and was proved by Faltings in his proof of the Mordell conjecture [16].

Theorem 2.1.3. *Take $g \geq 2$. There is a scheme $\mathcal{M}_g$ which is a coarse moduli space (see [43, Definition 5.6]) for the functor*

$$\mathbf{Sch} \to \mathbf{Set}$$
$$Y \mapsto \left\{ \begin{array}{c} \textit{Isomorphism classes of relative} \\ \textit{smooth genus } g \textit{ curves over } Y \end{array} \right\}$$

where **Sch** *is the category of noetherian schemes.*

This is [43, Theorem 5.11]. For further references on contructions of such moduli spaces, see [10, 33, 34, 35, 44].

The following corollary combines this moduli space theory with the Shafarevich conjecture. Informally speaking, it shows that Zariski density of integer points on the base of a relative curve $\mathcal{X} \to \mathcal{Y}$ over $\mathcal{O}$ implies that the family is isotrivial. Thus, to rule out Zariski density, it suffices to rule out isotriviality of the family, which is an easier condition to verify. This is precisely how we prove our theorem: having constructed our family in Section 2.2.2, we verify that it is not isotrivial along any positive dimension component in Section 2.2.3.

Corollary 2.1.4. *Fix $g \geq 2$. Let $\mathcal{X} \to \mathcal{Y}$ be a relative smooth genus g curve defined over $\mathcal{O}$. If $\mathcal{Y}(\mathcal{O})$ is a Zariski dense subset of $\mathcal{Y}$, the relative curve is isotrivial upon pullback to any geometric connected component of $\mathcal{Y}_K$.*

Proof. As discussed above, each element of $\mathcal{Y}(\mathcal{O})$ restricts to an element of $\mathcal{Y}_K(K)$ and the fiber of $\mathcal{X}_K \to \mathcal{Y}_K$ over these points are smooth genus g curves with good reduction outside of S. By Theorem 2.1.2, there are only finitely many isomorphism classes of such curves. Under the induced morphism $\mathcal{Y}_K \to \mathcal{M}_g$, each point of $\mathcal{Y}_K(K)$ whose fiber has good reduction must map to one of finitely many distinguished points on $\mathcal{M}_g$. Such points must have their residue fields contained in K - in particular, they may only specialize to points whose residue fields have positive characteristic. No point of $\mathcal{Y}_K$ can map to a point whose residue field is positive characteristic. Thus, we may apply Zariski density of the elements of $\mathcal{Y}_K(K)$ whose fibers have good reduction to conclude $\mathcal{Y}_K \to \mathcal{M}_g$ is constant on connected components.

Now, consider an algebraically closed field k and Z a connected component of $\mathcal{Y}_k$. The modular morphism $Z \to \mathcal{M}_g$ associated to $\mathcal{X}_Z \to Z$ must be constant; let q be the point it maps to. The fiber of $\mathcal{M}_g \times_{\mathbb{Z}} k = (\mathcal{M}_g)_k \to \mathcal{M}_g$ over q consists of finitely many discrete points (corresponding to the finitely many embeddings $k(q) \to k$). By connectedness of Z, the induced morphism of k-schemes $Z \to (\mathcal{M}_g)_k$ is constant as well. Thus, all sections $\operatorname{Spec} k \to Z$ become equal upon post-composition with $Z \to (\mathcal{M}_g)_k \to \mathcal{M}_g$, and since $\mathcal{M}_g$ is a coarse moduli space (i.e., using the natural bijection between $\mathcal{M}_g(k)$ and isomorphism classes of smooth genus g curves over k), we conclude that $\mathcal{X}_Z \to Z$ is indeed isotrivial. $\square$

2.2 Integer points in the plane

In this section, we give a precise statement of our main theorem of the chapter in Theorem 2.2.4, and state it in a way that does not depend on the choice of $\mathcal{O}$-model of the dual curve. We discuss how our main theorem may be interpreted as the finiteness of $\mathcal{O}$-points on an affine surface in Construction 2.2.7, and discuss curves satisfying the conditions of our main theorem in Proposition 2.2.9 and Example 2.2.10.

We begin by recalling the classical notion of the dual curve.

Definition 2.2.1. Let k be an algebraically closed field, and consider the projective plane $\mathbb{P}^2_k$ and its dual plane $(\mathbb{P}^2_k)^* \simeq \mathbb{P}^2_k$, with homogeneous coordinates x, y, z and a, b, c respectively. Given any smooth plane curve $C \to \mathbb{P}^2_k$, there is a *dual curve* $C^* \to (\mathbb{P}^2_k)^*$, whose points $(a : b : c)$ are precisely those corresponding to lines $ax + by + cz = 0$ tangent to C.

To see that C^* is genuinely a curve, give a homogeneous polynomial $h(X, Y, Z)$ for C, and note that the dual curve is the image of the *Gauss map*

$$\begin{aligned} C &\xrightarrow{\quad\quad \mathcal{G} \quad\quad} \mathbb{P}^2_k \\ (x : y : z) &\longmapsto \left(\tfrac{\partial h}{\partial X}(x,y,z) : \tfrac{\partial h}{\partial Y}(x,y,z) : \tfrac{\partial h}{\partial Z}(x,y,z)\right) \end{aligned}$$

which is finite by [48, Theorem 1.16]. Hence C^* is closed, irreducible, and dimension one (and is given the induced reduced structure, as a scheme). It has degree $m = d(d-1)$ [57, §IV.6].

Remark 2.2.2. This construction still holds if we replace k with the non-algebraically closed number field K. Indeed, h will have coefficients in K, and the Gauss map $C \to \mathbb{P}^2_K$ will again be finite, so we obtain the dual curve $C^* \to \mathbb{P}^2_K$. This is compatible under extension of K, e.g. $(C_L)^* = (C^*)_L$ for an arbitrary field extension L/K. (Note that, in characteristic zero, reduced implies geometrically reduced [51, Lemma 020I].)

Notation 2.2.3. For a scheme T, we write $\mathbb{P}^2_T \cong \mathbb{P}^2_{\mathbb{Z}} \times_{\mathbb{Z}} T$ for the projective plane over T and

$(\mathbb{P}^2_T)^* \simeq (\mathbb{P}^2_T)$ for the dual projective plane over T, with homogeneous coordinates x, y, z and a, b, c respectively.

Theorem 2.2.4. *Let $C \to \mathbb{P}^2_K$ be a smooth plane curve over K such that*

- *C has non-prime degree $d \geq 6$*
- *and $C_{\overline{K}}$ does not have any d-fold or $(d-1)$-fold tangent lines.*

Construct the open subscheme $\mathcal{Y} \to (\mathbb{P}^2_{\mathcal{O}})^*$ as the complement of the scheme-theoretic image of $C^* \to (\mathbb{P}^2_K)^* \to (\mathbb{P}^2_{\mathcal{O}})^*$. Then $\mathcal{Y}(\mathcal{O})$ is finite.

Remark 2.2.5. The requirement that $C_{\overline{K}}$ does not have d-fold or $(d-1)$-fold tangent lines is not very restrictive. For $d \geq 5$, a standard dimension count shows that this holds for generic (smooth) plane curves, see Proposition 2.2.9. See also Example 2.2.10 for an explicit example.

In the statement of Theorem 2.2.4, the scheme-theoretic image, as a set, is simply the Zariski closure of the set-theoretic image. More explicitly, suppose C^* is given by a homogeneous polynomial $g(a, b, c)$ with coefficients in $\mathcal{O}$ (clear denominators if necessary). Theorem 2.2.4 implies that the complement of the closed subscheme of $(\mathbb{P}^2_{\mathcal{O}})^*$ defined by $g(a, b, c)$ has finitely many $\mathcal{O}$-points.

Remark 2.2.6. Suppose L/K is a finite extension, and let S' be a finite set of primes of L which contains all primes lying over those in S. Write $\mathcal{O}'$ for the ring of S' integers. Proving Theorem 2.2.4 with L, S', and C_L replacing K, S, and C would imply the previous version. Note that forming the scheme-theoretic image of a quasi-compact morphism (e.g. $C^* \to (\mathbb{P}^2_{\mathcal{O}})^*$) commutes with flat base-change (e.g. $(\mathbb{P}^2_{\mathcal{O}'})^* \to (\mathbb{P}^2_{\mathcal{O}})^*$), see [51, Lemma 081I]. For this reason, we will occasionally enlarge K and S when convenient.

Construction 2.2.7. We now give a further concrete interpretation of the finiteness of $\mathcal{O}$-points from Theorem 2.2.4. To this end, we exhibit a closed immersion $(\mathbb{P}^2_K)^* \to \mathbb{P}^n_K$ which pulls back to $\big((\mathbb{P}^2_K)^* \setminus C^*)\big) = \mathcal{Y}_K \to \mathbb{A}^n_K$. As a closed subscheme of $\mathbb{A}^n_K$, $\mathcal{Y}_K$ will lie over only finitely many points of $\mathbb{A}^n_{\mathcal{O}}(\mathcal{O})$. These are just n-tuples with all entries lying in $\mathcal{O}$.

Proof of Construction 2.2.7. We first expand S so that $\mathcal{O}$ is a principal ideal domain. Furthermore, expand S so that we can select a homogeneous equation $g(a, b, c)$ for C^* whose coefficients are all units in $\mathcal{O}$. The closed subscheme of $(\mathbb{P}^2_{\mathcal{O}})^*$ defined by $g(a, b, c)$ is then the same as the scheme theoretic image of $C^* \to (\mathbb{P}^2_{\mathcal{O}})^*$, by an application of Gauss's lemma for polynomials.

Then, consider the commutative diagram

$$
\begin{tikzcd}
D_K \arrow[rrrr] \arrow[dr] \arrow[dd] & & & & \mathcal{H}_K \arrow[dr] \arrow[dd] & \\
& D \arrow[rrrr] \arrow[dd] & & & & \mathcal{H} \arrow[dd] \\
(\mathbb{P}^2_K)^* \arrow[rr, "\mathcal{V}"] \arrow[dr] & & \mathbb{P}^n_K \arrow[rr, "\sim"] \arrow[dr] & & \mathbb{P}^n_K \arrow[dr] & \\
& (\mathbb{P}^2_{\mathcal{O}})^* \arrow[rr, "\mathcal{V}"] & & \mathbb{P}^n_{\mathcal{O}} \arrow[rr, "\sim"] & & \mathbb{P}^n_{\mathcal{O}} \\
\mathcal{Y}_K \arrow[uu] \arrow[rrrr] \arrow[dr] & & & & \mathbb{A}^n_K \arrow[uu] \arrow[dr] & \\
& \mathcal{Y} \arrow[uu] \arrow[rrrr] & & & & \mathbb{A}^n_{\mathcal{O}} \arrow[uu] \, .
\end{tikzcd}
\tag{2.1}
$$

Each commutative square is a pullback. Here $\mathcal{V}$ denotes the Veronese embedding (closed immersion)

$$
\begin{array}{ccc}
(\mathbb{P}^2_{\mathcal{O}})^* & \xrightarrow{\quad\mathcal{V}\quad} & \mathbb{P}^n_{\mathcal{O}} \\
(a : b : c)] & \longmapsto & (\{a^i b^j c^k\}_{i+j+k=m}) \, .
\end{array}
\qquad n = \binom{m+2}{2} - 1 \quad \text{where } m = \deg(C^*) = \deg(g)
$$

Also

D is the closed subscheme determined by $g(a, b, c)$, so that $D_K = C^*$

$\mathcal{H}$ is the "hyperplane at infinity," corresponding to a fixed affine piece $\mathbb{A}^n_{\mathcal{O}} \to \mathbb{P}^n_{\mathcal{O}}$.

Remark 2.2.8. We do not refer to D as a "dual curve over $\mathcal{O}$," see [14, §V.4] for subtleties on curves and their duals curves over an arbitrary noetherian base (as opposed to curves and their duals over the spectrum of a field). Later, we will study the dual curve over an arbitrary integral noetherian scheme, see Definition 2.2.15. However, this is only done as a closed set, i.e. we will not worry about the right scheme structure on the dual curve itself.

We now describe the depicted automorphism $\mathbb{P}^n_{\mathcal{O}} \xrightarrow{\sim} \mathbb{P}^n_{\mathcal{O}}$. Since we are free to enlarge the set of primes S, we do so and assume that we can give a homogeneous equation for C^* whose coefficients are all units in $\mathcal{O}$. Then, there is an automorphism $\mathbb{P}^n_{\mathcal{O}} \xrightarrow{\sim} \mathbb{P}^n_{\mathcal{O}}$ that makes all squares above pullbacks.

Indeed, if

$$g(a,b,c) = \sum_{\substack{i+j+k=m \\ i,j,k\geq 0}} \gamma_{i,j,k}\ a^i b^j c^k$$

and $\mathbb{P}^n_{\mathcal{O}} \cong \operatorname{Proj} \mathcal{O}[\{x_{i,j,k}\}_{i+j+k=m}]$, then the desired automorphism $\mathbb{P}^n_{\mathcal{O}} \xrightarrow{\sim} \mathbb{P}^n_{\mathcal{O}}$ is such that $\mathcal{H}$ pulls back to the hyperplane

$$\sum_{\substack{i+j+k=m \\ i,j,k\geq 0}} \gamma_{i,j,k}\ x_{i,j,k}$$

in $\mathbb{P}^n_{\mathcal{O}}$.

With this set-up, Theorem 2.2.4 implies that $\mathcal{Y}_K$ as a closed subscheme of $\mathbb{A}^n_K$ lies over only finitely many points of $\mathbb{A}^n_{\mathcal{O}}$. □

Proposition 2.2.9. *Let k be an algebraically closed field and fix $d \geq 4$. View $\mathbb{P}^N_k$ as parameterizing plane curves of degree at most d, where $N = \binom{d+2}{2} - 1$. Write $Y \subseteq \mathbb{P}^N_k$ for the Zariski open subset corresponding to smooth degree d plane curves. Given m with $4 \leq m \leq d$, the locus $Z_m \subseteq Y$ of smooth curves with a tangent of multiplicity at least m is Zariski closed and has pure codimension* $\operatorname{codim} Z_m = m - 3$.

When $m = 4$, this is the well-known the fact that generic (smooth) curves do not have tangents of multiplicity greater than 3. Furthermore, this states that the generic curve with a tangent of degree at least m does not have a tangent of degree $m+1$. The proof is a standard dimension count which we record for completeness.

Proof. For plane curves C, D and a point x in the plane, write $(C,D)_x$ for the intersection number. Consider the correspondence

$$X = \{(\text{point } x, \text{line } L, \text{curve } C) : (L,C)_x \geq m\} \subset \mathbb{P}^2_k \times_k \mathbb{P}^2_k \times_k Y.$$

Here, X is a closed subscheme. The projection of X to $\mathbb{P}^2_k \times_k \mathbb{P}^2_k$ has image

$$W = \{(\text{point } x, \text{line } L) : x \in L\} \subseteq \mathbb{P}^2_k \times_k \mathbb{P}^2_k.$$

To see this, note that the smooth curve given by the affine equation $y = x^m + x^d + y^d$ has tangent line $y = 0$ with multiplicity m at $x = y = 0$. This shows that we can construct a smooth curve with prescribed tangent order m at a given point on a given line.

The theorem on the dimension of fibers (see for example [27, Exercise II.3.4.22]) shows that W is pure dimension 3, and another application of the same theorem shows X is pure dimension $N-(m-3)$. The projection $X \to Y$ is proper (hence closed) and has finite fibers (any given smooth plane curve has finitely many tangent lines of order at least 3). Since Z_m is the image of $X \to Y$, the theorem of the dimension of fibers shows that Z_m has dimension $N-(m-3)$ as claimed. $\square$

Example 2.2.10. The degree 6 homogeneous equation

$$yz^5 + x^4z^2 + x^6 + y^6 \tag{2.2}$$

defines a curve C (say, over $\mathbb{Q}$) satisfying the conditions of Theorem 2.2.4. Indeed, C is a smooth plane curve, has six 4-fold tangents, and no 5-fold or 6-fold tangents. The six 4-fold tangents are at the points $(0 : y : 1)$ where y is a root of $y^6 + 1 = 0$.

To see that the other flex points (i.e. points where the tangent line intersects with multiplicity at least three) are all ordinary (the tangent line intersects to degree exactly three), first recall that the flex points of a smooth plane curve C are precisely the intersection points of C and its Hessian curve. If C is given by a homogeneous equation $f(x,y,z)$ of degree d, the Hessian curve H is defined by the homogeneous degree $3(d-2)$ equation given by the determinant

$$\left| \frac{\partial^2 f}{\partial x_i \partial x_j} \right| .$$

Moreover, if a flex point x has a m-fold tangent, the intersection multiplicity of H and C at x is $m-2$. References for these facts on the Hessian may be found in [15, Page 271], [20, §4.5], and [52, Proposition 9].

Let C be the degree 6 curve of Equation (2.2), and work over $k = \overline{\mathbb{Q}}$. With a computer [53], we find that the intersection with its Hessian H (a degree 12 curve) consists of the 6 points $(0 : y : 1)$ with $y^6 + 1 = 0$, each with multiplicity two, and the closed subscheme defined by the homogeneous ideal generated by

$$x^6 + y^6 + x^4z^2 + yz^5 \text{ and } 12y^{10} + 20x^4y^4z^2 - 120x^2y^5z^3 - 36y^5z^5 + 5x^2z^8 + 2z^10.$$

This is the intersection of a degree 6 curve and a degree 10 curve, and lies in the chart $z \neq 0$. We may pass to the corresponding ideal of $k[x,y]$ and check that this ideal is equal to its radical, so this piece must consist of 60 distinct points. Bézout's theorem then implies that the intersection number is one at all 60 of these points (and there are 6 more points, as described above, with intersection number 2).

Remark 2.2.11. As mentioned in the introduction, there is a theorem of Levin [38] (which covers those of [17] and [59]) that proves finiteness of $\mathcal{O}$-points on the complements of certain singular plane curves. In addition to ampleness conditions, this requires that the curve has only simple nodes and cusps. Curves satisfying the condition of Theorem 2.2.4 with tri-tangents, higher order tangents, etc. will yield dual curves which are not covered under the conditions of [38]. The curve given in Example 2.2.10 is an explicit example. Moreover, Proposition 2.2.9 shows that, among degree $d \geq 6$ curves of non-prime degree with a tangent of degree at least 4, the curves that satisfy the conditions of Theorem 2.2.4 are generic. All such curves correspond to dual curves with non-ordinary cusps.

2.2.1 Dual curves over a general base

In this section, we study smooth curves and their duals over an arbitrary integral noetherian base. This is more general than we will need, as our application is to curves over $\mathcal{O}$, but the general formalism facilitates our discussion. As mentioned in Remark 2.2.8, we are not concerned with identifying the right scheme structure on the dual curve (which may not be reduced, even if one starts with a reduced curve), and instead content ourselves with its construction as a closed set, as we are interested in its complement. Some discussion on the dual curve's scheme structure may be found in [14, §V.4]. They use a setup similar to the one presented below, and our formulation of the dual curve agrees with theirs (as a closed set).

Let T be an arbitrary integral noetherian scheme T and fix the following:

$C \to \mathbb{P}^2_T$	a closed immersion with $C \to T$ a smooth curve of degree $d \geq 2$
x, y, z	homogeneous coordinates on $\mathbb{P}^2_T$
a, b, c	homogeneous coordinates on the dual plane $(\mathbb{P}^2_T)^* \simeq \mathbb{P}^2_T$
Σ	the closed subscheme of $\mathbb{P}^2_T \times_T (\mathbb{P}^2_T)^*$ defined by $ax + by + cz = 0$
Σ_C	for $\Sigma \times_{\mathbb{P}^2_T} C$.

This is depicted in the following commutative diagram.

$$\begin{tikzcd}
\Sigma_C \arrow[r] \arrow[dr] & \Sigma \arrow[rr] & & \mathbb{P}^2_T \times_T (\mathbb{P}^2_T)^* \arrow[dl] \arrow[dr] & \\
& C \arrow[r] & \mathbb{P}^2_T & & (\mathbb{P}^2_T)^* .
\end{tikzcd} \tag{2.3}$$

Lemma 2.2.12. *The relative curve C contains no lines in the following sense: for every geometric point $\bar{t}$ of T, $C_{\bar{t}} \to \mathbb{P}^2_{\bar{t}}$ does not contain any lines.*

Proof. Since T is integral and noetherian, flatness of $C \to T$ implies that $C_{\bar{t}} \to \mathbb{P}^2_{\bar{t}}$ is a degree d plane curve for any geometric point $\bar{t}$. Moreover, $C_{\bar{t}}$ is smooth, so the classical theory for plane curves implies that $C_{\bar{t}}$ is irreducible and thus contains no lines. □

Lemma 2.2.13. *The morphism $\Sigma_C \xrightarrow{f} (\mathbb{P}^2_T)^*$ is surjective and finite.*

Proof. We first check properness, which follows because closed immersions are proper, properness is stable under base-change and composition, and $\mathbb{P}^2_{\mathbb{Z}} \to \mathbb{Z}$ is proper. Next, consider a geometric point $\bar{s}\colon \operatorname{Spec} k \to (\mathbb{P}^2_T)^*$ with corresponding geometric point $\bar{t}\colon \operatorname{Spec} k \to (\mathbb{P}^2_T)^* \to T$. We may diagram chase and compute the corresponding geometric fiber of f above $\bar{s}$ as

$$(\Sigma_C)_{\bar{s}} \cong C \times_{\mathbb{P}^2_T} (\mathbb{P}^2_T \times_T \operatorname{Spec} k) \times_{\mathbb{P}^2_T \times_T \operatorname{Spec} k} \Sigma_{\bar{s}} \cong C_{\bar{t}} \times_{\mathbb{P}^2_{\bar{t}}} \Sigma_{\bar{s}}.$$

From the construction, $\Sigma_{\bar{s}}$ will be a line in $\mathbb{P}^2_T \times_T \operatorname{Spec} k \cong \mathbb{P}^2_{\bar{t}} \cong \mathbb{P}^2_k$. Thus, the fiber $(\Sigma_C)_{\bar{s}}$ is the intersection of $C_{\bar{t}}$ and a line in $\mathbb{P}^2_{\bar{t}}$. Since C contains no lines by Lemma 2.2.12, the classical theory implies that this intersection is nonempty and finite. This shows that f is surjective with finite geometric fibers, and thus finite fibers. By properness, we conclude that it is also a finite morphism [51, Lemma 02OG]. □

Remark 2.2.14. The degree of the finite morphism $\Sigma_C \xrightarrow{f} (\mathbb{P}^2_T)^*$ coincides with the degree of $C \to \mathbb{P}^2_T$, as a relative curve over T. To see this, work over the generic point η of $(\mathbb{P}^2_{\mathcal{O}})^*$. As in the proof of Lemma 2.2.13, one computes that $(\Sigma_C)_\eta$ is the (scheme-theoretic) intersection of $C_{k(\eta)}$ and a line in $\mathbb{P}^2_{k(\eta)}$. Bézout's theorem implies that $(\Sigma_C)_\eta \to \operatorname{Spec} k(\eta)$ is finite of degree $\deg(C_{k(\eta)})$, which is also the degree of C as a relative curve.

Now we may form the sheaf Ω of relative differentials for $\Sigma_C \xrightarrow{f} (\mathbb{P}^2_T)^*$. Since these schemes are noetherian and f is finite type by Lemma 2.2.13, we know Ω is a coherent $\mathcal{O}_{\Sigma_C}$-module [27, Remark 8.9.1]. Since f is finite by Lemma 2.2.13, it is proper, so $f_*\Omega$ is coherent [23, Theorem 3.2.1]. This implies the support $\operatorname{supp}(f_*\Omega)$ is closed in $(\mathbb{P}^2_T)^*$.

Definition 2.2.15. We define the *dual curve*, as a closed set, to be $\operatorname{supp}(f_*\Omega)$.

Remark 2.2.16. For our application, we will want to relate the dual curve of Definition 2.2.15 when $T = \operatorname{Spec} \mathcal{O}$ to the scheme-theoretic image discussed in Theorem 2.2.4. This will be discussed in Section 2.2.2, where we see that they agree if we expand S.

Proposition 2.2.17. *Let y be a point of $(\mathbb{P}^2_T)^*$. Then, y lies in the dual curve* $\operatorname{supp}(f_*\Omega)$ *if and only if the fiber of $\Sigma_C \xrightarrow{f} (\mathbb{P}^2_T)^*$ above y is ramified over* $\operatorname{Spec} k(y)$.

Proof. Write s for the natural morphism $\operatorname{Spec} k(y) \to (\mathbb{P}^2_T)^*$ for the natural morphism, and t for the composition $\operatorname{Spec} k(y) \xrightarrow{s} (\mathbb{P}^2_T)^* \to T$. We have the fiber product diagram

$$\begin{tikzcd} \Sigma_C \arrow[d, "f"'] & (\Sigma_C)_s \cong C_t \times_{\mathbb{P}^2_{k(y)}} \Sigma_s \arrow[l, "s'"'] \arrow[d, "f'"] \\ (\mathbb{P}^2_T)^* & \operatorname{Spec} k(y) \arrow[l, "s"'] \end{tikzcd} \quad . \tag{2.4}$$

Since f is finite, it is affine. Thus pushforward of a quasi-coherent sheaf along f commutes with arbitrary base change [51, Lemma 02KG]. Sheaves of relative differentials are also compatible under base-change, so if Ω is the sheaf of relative differentials for f and Ω' is the sheaf of relative differentials for f', we have $\Omega' \cong s'^*\Omega$, see for example [27, Proposition II.8.10]. So we conclude

$$f'_*\Omega' \cong f'_*(s'^*\Omega) \cong s^*(f_*\Omega).$$

Using Nakayama's lemma, we conclude that y lies outside of $\operatorname{supp}(f_*\Omega)$ if and only if $s^*(f_*\Omega) = 0$. Since f is finite, f' is also finite, so $C_t \times_{\mathbb{P}^2_{k(y)}} \Sigma_s$ consists of finitely many closed points. Thus, $\Gamma(C \times_{\mathbb{P}^2_T} \Sigma_s, \Omega') = f'_*\Omega' = 0$ if and only if $\Omega' = 0$ because $C \times_{\mathbb{P}^2_k} \Sigma_t$. Thus, y lies outside $\operatorname{supp}(f_*\Omega)$ if and only if f' is unramified (i.e. $\Omega' = 0$). $\square$

Corollary 2.2.18. *When T is the spectrum of an algebraically closed field k, the dual curve of Definition 2.2.15 coincides with the dual curve of Definition 2.2.1, as closed sets.*

Proof. The classical dual curve over an algebraically closed field may be characterized by its closed points: these are precisely the points of $(\mathbb{P}^2_k)^*$ corresponding to lines which are tangent to C. From the construction, a closed point $s\colon \operatorname{Spec} k \to (\mathbb{P}^2_k)^*$ corresponds to the line Σ_t in $\mathbb{P}^2_k$. This is tangent to C if and only if $(\Sigma_C)_s = C \times_{\mathbb{P}^2_k} \Sigma_s$ is non-reduced, which occurs if and only if $(\Sigma_C)_s$ is ramified over $\operatorname{Spec} k$. Proposition 2.2.17 implies that this occurs if and only if s lies in $\operatorname{supp}(f_*\Omega)$. $\square$

Lemma 2.2.19. *If T' is integral and noetherian, formation of the dual curve (as a closed set) is compatible with base-change $T' \to T$.*

Proof. We impose integrality and noetherianity on T' because we have only defined the complement of the dual curve over an integral noetherian base. The base-change functor $\mathbf{Sch}/T \to \mathbf{Sch}/T'$ preserves fiber products (it is a right adjoint) so all of Diagram (2.3) is compatible with base-change, e.g. $\Sigma_{C_{T'}} \cong \Sigma_C \times_T T'$. Consider the following fiber product diagram.

$$\begin{tikzcd}
\Sigma_C \arrow[d, "f"'] & \Sigma_C \times_T T' \arrow[l, "g'"'] \arrow[d, "f'"] \\
(\mathbb{P}^2_T)^* & (\mathbb{P}^2_{T'})^* \arrow[l, "g"']
\end{tikzcd} \tag{2.5}$$

As in the proof of Proposition 2.2.17, affine-ness of f implies pushforward of a quasi-coherent sheaf along f commutes with base-change, and we also have that formation of sheaves of differentials commutes with base-change. Writing Ω and Ω' for sheaves of relative differentials for f and f' respectively, we have

$$f'_*\Omega' \cong {f'}_*(g'^*\Omega) \cong g^*(f_*\Omega).$$

Since $f_*\Omega$ is coherent, we know that $\operatorname{supp}(g^*(f_*\Omega)) = g^{-1}(\operatorname{supp}(f_*\Omega))$ [51, Lemma 056J], so that $\operatorname{supp}(f'_*\Omega') = g^{-1}(\operatorname{supp}(f_*\Omega))$ as claimed. $\square$

Corollary 2.2.20. *When $T = \operatorname{Spec} K$, the dual curve of Definition 2.2.15 coincides with that of Remark 2.2.2, as a closed set.*

Proof. Consider Diagram (2.3), with an additional arrow $C \xrightarrow{\mathcal{G}} (\mathbb{P}^2_K)^*$ for the Gauss map. Fixing an embedding and base-changing the entire diagram from $\mathbf{Sch}/K$ to $\mathbf{Sch}/\overline{K}$, we obtain the commutative diagram

$$\begin{tikzcd}
\Sigma_{C_{\overline{K}}} \arrow[rr] \arrow[dr] \arrow[dd] & & \Sigma_{\overline{K}} \arrow[rr] \arrow[dd] & & \mathbb{P}^2_{\overline{K}} \times_{\overline{K}} (\mathbb{P}^2_{\overline{K}})^* \arrow[dl] \arrow[dr] \arrow[dd] & \\
& C_{\overline{K}} \arrow[rr] \arrow[dd] \arrow[rrrr, bend right, "\mathcal{G}"] & & \mathbb{P}^2_{\overline{K}} \arrow[dd] & & (\mathbb{P}^2_{\overline{K}})^* \arrow[dd, "g"] \\
\Sigma_C \arrow[rr] \arrow[dr] & & \Sigma \arrow[rr] & & \mathbb{P}^2_K \times_K (\mathbb{P}^2_K)^* \arrow[dl] \arrow[dr] & \\
& C \arrow[rr] \arrow[rrrr, bend right, "\mathcal{G}"] & & \mathbb{P}^2_K & & (\mathbb{P}^2_K)^* \, .
\end{tikzcd} \tag{2.6}$$

where vertical squares are pullbacks. If $D \subseteq (\mathbb{P}^2_K)^*$ denotes the dual curve as a closed set, in the sense of Definition 2.2.15, the conclusions of Corollary 2.2.18 and Lemma 2.2.19 imply that $g^{-1}(D) = \mathcal{G}(C_{\overline{K}})$. But $\mathcal{G}(C) = (g \circ \mathcal{G})(C_{\overline{K}})$, so $D = \mathcal{G}(C)$ as claimed. □

We record a few useful properties of the schemes and morphisms from Diagram (2.3).

Proposition 2.2.21. *The morphisms $\Sigma \to \mathbb{P}^2_T$ and $\Sigma \to (\mathbb{P}^2_T)^*$ are smooth.*

Proof. From the symmetry in the definition of Σ, we can just check smoothness of $\Sigma \to (\mathbb{P}^2_T)^*$. This is proper (closed immersion followed by base-change of the projection $\mathbb{P}^2_{\mathbb{Z}} \to \mathbb{Z}$) hence finite type. These are noetherian schemes, so the morphism is of finite presentation. The fiber over $\operatorname{Spec} k \to \mathbb{P}^2_T$ is isomorphic to $\mathbb{P}^1_k$, which is regular.

It remains to check flatness. By construction, Σ is a closed subscheme of two-dimensional projective space over $(\mathbb{P}^2_T)^*$, and the fiber over any point y of $(\mathbb{P}^2_T)^*$ is some $\mathbb{P}^1_{k(y)}$ as a closed subscheme of $\mathbb{P}^2_{k(y)}$. Thus, the Hilbert polynomial is constant across all fibers, and since $(\mathbb{P}^2_T)^*$ is integral and noetherian, we conclude that $\Sigma \to (\mathbb{P}^2_T)^*$ is flat [27, Theorem 9.9]. □

Corollary 2.2.22. *If T is a regular scheme then Σ_C is a regular scheme.*

Proof. Smoothness is stable under base-change, so Proposition 2.2.21 implies $\Sigma_C \to C$ is smooth. Since $C \to T$ is smooth, we have $\Sigma_C \to T$ smooth as well. Since T is regular, Σ_C is regular as well by [39, Theorem 4.3.36]. □

Corollary 2.2.23. *If T is a regular scheme, the morphism $(\Sigma_C)_Y \to Y$ is étale.*

Proof. The morphism is a finite type morphism of noetherian schemes, so certainly finitely presented. Since Σ_C is regular by Corollary 2.2.22, we have that $\Sigma_C \to (\mathbb{P}^2_T)^*$ is a surjective finite morphism (by Lemma 2.2.13) of regular noetherian schemes, hence flat by [39, Remark 4.3.11]. Unramifiedness follows from Proposition 2.2.17, see [24, Theorem 17.4.1] for characterizations of unramified morphisms. □

Proposition 2.2.24. *If T is a regular scheme, the dual curve as a closed set is pure of codimension one, i.e. each of its irreducible components has codimension one.*

Proof. This follows from purity of the branch locus: if $M \xrightarrow{g} N$ is a finite morphism of regular noetherian schemes that isn't everywhere ramified, then $\operatorname{supp}(\Omega_{M/N})$ and $\operatorname{supp}(g_*\Omega_{M/N}) = g(\operatorname{supp}(\Omega_{M/N}))$ are pure of codimension one, see [51, Lemma 0BMB]. We apply this to $\Sigma_C \xrightarrow{f} (\mathbb{P}^2_{\mathcal{O}})^*$, and use the regularity of Σ_C proved in Corollary 2.2.22. To see that f is not everywhere ramified, pick any geometric point $\overline{s}$ of $(\mathbb{P}^2_T)^*$ that corresponds to a non-tangent line to $C_{\overline{s}}$ (see proof of Lemma 2.2.13), which exists because $C_{\overline{s}}$ is smooth. □

2.2.2 Constructing a family of curves

In this section, we apply the theory of Section 2.2.1 to the case $T = \operatorname{Spec} \mathcal{O}$. Using this, we will construct a relative curve over the complement of the dual curve, whose fibers are cyclic covers of $\mathbb{P}^1$, see Construction 2.2.30.

The input data of Theorem 2.2.4 is a plane curve $C \to \mathbb{P}^2_K$ such that $C \to \operatorname{Spec} K$ is smooth. To construct a dual curve over $\mathcal{O}$ in the sense of Definition 2.2.15, we want to select a model $\mathcal{C} \to \mathbb{P}^2_{\mathcal{O}}$ such that $\mathcal{C} \to \operatorname{Spec} \mathcal{O}$ is smooth. This is justified in Corollary 2.2.26 below.

Lemma 2.2.25 (Generic smoothnes)**.** *Let S be a integral noetherian scheme with generic point η. Let $\mathcal{Z} \to S$ be a proper morphism. If $\mathcal{Z}_\eta \to \operatorname{Spec} k(\eta)$ is smooth, then there is a dense open subscheme $S' \to S$ so that $\mathcal{Z}_{S'} \to S'$ is smooth.*

When $S = \operatorname{Spec} \mathcal{O}$, this is a statement about almost everywhere good reduction, see Corollary 2.2.26. A similar fact is discussed in [28, Proposition A.9.1.6]. For an older treatment of almost everywhere good reduction, see [49]. We include a proof the lemma for completeness.

Proof of Lemma 2.2.25. Since $\mathcal{Z} \to S$ is finite type and S is reduced, we know $\mathcal{Z} \to S$ is generically flat, i.e. flat when restricted to a dense open subscheme of S [51, Proposition 052B]. Furthermore, the points at which $\mathcal{Z} \to S$ is not smooth form a closed subset of $\mathcal{C}$, and this set does not intersect the generic fiber because $\mathcal{Z}_\eta \to \operatorname{Spec} k(\eta)$ is assumed to be smooth [51, Lemma 01V9]. By properness, the image in S of this closed set is closed. Since this closed subset of S does not contain the generic point, its complement S' is dense and open. We have that $\mathcal{C} \to S'$ is smooth by construction. $\square$

Corollary 2.2.26. *Let $C \to \mathbb{P}^n_K$ be a closed immersion, with $C \to \operatorname{Spec} K$ a smooth degree d curve. Expanding S if necessary, there is a divisor $\mathcal{C} \to \mathbb{P}^n_{\mathcal{O}}$ which recovers $C \to \mathbb{P}^n_K$ upon base-change, and such that $\mathcal{C}$ is a smooth $\mathcal{O}$-scheme. We have $\mathcal{C} = \operatorname{div}(s)$ for some $s \in \Gamma(\mathbb{P}^2_{\mathcal{O}}, \mathcal{O}(d))$.*

Proof of Corollary 2.2.26. By taking a homogeneous degree equation for C with $\mathcal{O}$ coefficients, we obtain a divisor $\mathcal{C} \to \mathbb{P}^n_{\mathcal{O}}$ recovering $C \to \mathbb{P}^n_K$ upon base-change. Smoothness upon expanding S follows from a direct application of Lemma 2.2.25, with $S = \operatorname{Spec} \mathcal{O}$ and $\mathcal{Z} = \mathcal{C}$. Restriction to a dense open subscheme of $\operatorname{Spec} \mathcal{O}$ is the same as expanding the set S. Global sections of $\mathcal{O}(d)$ are homogeneous degree d equations with $\mathcal{O}$-coefficients. $\square$

Notation 2.2.27. For the rest of this section, we fix the following notation

$C \to \mathbb{P}^2_K$ a closed immersion with C a smooth degree $d \geq 2$ curve over K

$C^* \to (\mathbb{P}^2_K)^*$ the dual curve of C, in the sense of Remark 2.2.2

$\mathcal{C} \to \mathbb{P}^2_{\mathcal{O}}$ a model over $\mathcal{O}$ for $C \to \mathbb{P}^2_K$ as in Corollary 2.2.26

$Y \to (\mathbb{P}^2_K)^*$ complement of the dual curve of C

$\mathcal{Y} \to (\mathbb{P}^2_{\mathcal{O}})^*$ complement of the dual curve of $\mathcal{C}$

Note $\mathcal{Y}_K = Y$ by Lemma 2.2.19.

Proposition 2.2.28. *Expanding S if necessary, $\mathcal{Y}$ coincides with the complement of the scheme-theoretic image of $C^* \to (\mathbb{P}^2_K)^* \to (\mathbb{P}^2_{\mathcal{O}})^*$.*

Proof. By Proposition 2.2.24, we know $\mathcal{Y}$ is the complement of a closed set $D \subseteq (\mathbb{P}^2_{\mathcal{O}})^*$ of pure codimension one. Let us impose the induced reduced structure on D, so that $D \to (\mathbb{P}^2_{\mathcal{O}})^*$ is a divisor. If we expand S so that $\mathcal{O}$ is a principal ideal domain, we have $\mathrm{Cl}((\mathbb{P}^2_{\mathcal{O}})^*) \cong \mathbb{Z}$, i.e. consists of the twisting sheaves $\mathcal{O}(m)$ for $m \in \mathbb{Z}$. This implies D is given by a homogeneous equation $g(a, b, c)$ with $\mathcal{O}$ coefficients. Furthermore, D_K recovers C^* as a closed set by Corollary 2.2.20 and is also reduced, so $D_K = C^*$. That is, $g(a, b, c)$ is also a homogeneous equation for C^*. If we expand S further so that $g(a, b, c)$ is primitive, e.g. some coefficient is a unit in $\mathcal{O}$, this implies that $g(a, b, c)$ defines both D and the scheme-theoretic image of C^* in $(\mathbb{P}^2_{\mathcal{O}})^*$, by an application of Gauss's lemma for polynomials. $\square$

Thus, to prove Theorem 2.2.4, it is equivalent to prove finiteness of $\mathcal{Y}(\mathcal{O})$. We could have stated the theorem in this alternate way, but this would have required stating Definition 2.2.15 before stating the theorem. Furthermore, the current statement of Theorem 2.2.4 allowed for the concrete discussion of Construction 2.2.7 immediately following the theorem statement. Also, the construction of $\mathcal{Y}$ relies on the choice of an $\mathcal{O}$-model for C, while Theorem 2.2.4 does not.

Our strategy for proving the theorem is to construct a suitable relative curve over $\mathcal{Y}$, show that it cannot be isotrivial along a geometric component of any positive dimension closed subscheme, and to apply Corollary 2.1.4.

Informally speaking, the construction for the relative curve is to first fix an m-fold cover of $\mathbb{P}^2_{\mathcal{O}}$ branched at $\mathcal{C}$ (this will be made precise below); then points in $\mathcal{Y}$ correspond to lines not tangent to $\mathcal{C}$, which will pullback to curves of some fixed genus.

The following proposition allows us to construct the desired m-fold cover.

Construction 2.2.29. Fix an integer $m \geq 2$. Let M be an integral noetherian $\mathbb{Z}[1/m]$-scheme, and $\mathcal{L}$ an invertible sheaf on M. Fix a nonzero section $s \in \Gamma(M, \mathcal{L}^{\otimes m})$ with $\operatorname{div}(s)$ an effective divisor. We construct a finite, flat surjection

$$\pi \colon N \to M$$

and $s' \in \Gamma(N, \pi^*\mathcal{L})$ such that

(a) formation of π and s' is compatible with base-change $M' \xrightarrow{g} M$ for M an integral noetherian $\mathbb{Z}[1/m]$ scheme,

(b) the morphism π is degree m in the sense that the fiber of π over the generic point is m dimensional,

(c) we have $(s')^{\otimes m} = \pi^* s$,

(d) we have $\operatorname{supp}(\pi_*\Omega_{N/M}) = \operatorname{supp}(\operatorname{div}(s))$; in particular π is étale outside of $\operatorname{supp}(\operatorname{div}(s))$,

(e) and if M is a smooth curve over an algebraically closed field k and $\operatorname{div}(s)$ is regular (i.e. reduced) then N is also a smooth curve.

We refer to this construction as an *m-fold cyclic cover.* The construction presented below may be found in [1, §I.17] and [37, §4.1.B]. Those authors are working with complex varieties, but the same construction generalizes to certain schemes as in the above lemma statement. This covering is branched at $\operatorname{div}(s)$ in the sense of condition (c).

Proof of Construction 2.2.29. (Construction) If $\mathcal{L}^*$ denotes the dual of $\mathcal{L}$, we first consider projection $\mathbb{V}(\mathcal{L}^*) \xrightarrow{\pi} M$ from the total space of $\mathcal{L}^*$, i.e. $\mathbb{V}(\mathcal{L}^*) = \mathbf{Spec}\operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*)$. Let $T \in \Gamma(\mathbb{V}(\mathcal{L}^*), p^*\mathcal{L})$ denote the tautological section. Formally, we specify T by a morphism

$$\mathcal{O}_{\mathbb{V}(\mathcal{L}^*)} \to \pi^*\mathcal{L} \otimes \mathcal{O}_{\mathbb{V}(\mathcal{L}^*)}.$$

Pushforward gives an equivalence of categories between quasi-coherent $\mathcal{O}_{\mathbb{V}(\mathcal{L}^*)}$ modules and quasi-coherent $\mathcal{O}_M$-modules with a $\operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*)$-module structure [27, Exercise II.5.17]. Applying the projection formula, we may thus specify T via the natural inclusion

$$\operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*) \to \mathcal{L} \otimes \operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*),$$

i.e. as a summand.

Having specified the tautological section T, we take N to be the divisor of zeros for the section

$$T^m - \pi^* s \in \Gamma(\mathbb{V}(\mathcal{L}^*), p^*\mathcal{L}^{\otimes m}).$$

Over an open affine neighborhood $\operatorname{Spec}(A) \to M$ where $\mathcal{L}$ is trivial, we have $\mathbb{V}(\mathcal{L}^*) = \operatorname{Spec}(A[t])$ with tautological section t. The morphism $\pi \colon N \to M$ may be identified with

$$\operatorname{Spec}(B) = \operatorname{Spec}(A[t]/(t^m - a)) \to \operatorname{Spec}(A) \tag{2.7}$$

where $\Gamma(\operatorname{Spec}(A), \mathcal{L}) \xrightarrow{\sim} A$ sends $s \mapsto a$.

We may take

$$s' = T|N \in \Gamma(N, p^*\mathcal{L}).$$

In the local description above this is t; this will be justified upon proving property (a).

We first verify that π is finite and flat. These are both immediate from the local description as $A[t]/(t^m - a)$ is free of rank m over A. Surjectivity is also clear, as π is a dominant finite morphism.

(Proof of properties (a), (b), (c), (d), and (e))

For (a), we first have that formation of $\mathbb{V}(\mathcal{L}^*)$ is compatible with base-change, i.e. we have the fiber product diagram

$$\begin{tikzcd}
\mathbb{V}(\mathcal{L}^*) \arrow[d, "\pi"'] & \mathbb{V}(g^*\mathcal{L}^*) \arrow[l, "g"'] \arrow[d, "\pi'"] \\
M & M' \arrow[l, "g'"']
\end{tikzcd} \tag{2.8}$$

This may be verified by commuting pullback with tensor product, dualizing, and direct sum to check

$$g'^* \operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*) \cong \operatorname{Sym}_{\mathcal{O}_{M'}}((g'^*\mathcal{L})^*)$$

and then checking that $\mathbf{Spec}(g'^*(\mathscr{A})) \cong \mathbf{Spec}(\mathscr{A}) \times_M M'$ for $\mathscr{A}$ a quasi-coherent $\mathcal{O}_M$-algebra. Similarly, the natural inclusion $\operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*) \to \mathcal{L} \otimes \operatorname{Sym}_{\mathcal{O}_M}(\mathcal{L}^*)$ is compatible with base change, as we may see by again commuting pullbacks with tensor product, dualizing, and direct sum. So we conclude the tautological section T is compatible with base-change as well. This implies the same for s'.

For (b), this is again immediate from the local description. If k is the fraction field of A, the fiber over the generic point is $k[t]/(t^m - a)$.

For (c), this is also immediate from the local description.

For (d), we may again consider the local description, as sheaves of differentials are compatible with pullback. The sheaf $\pi_*\Omega_{N/M}$ is coherent. In the notation of Equation (2.7), this sheaf locally corresponds to a free A/a-module of rank $m-1$, with basis $\{t^i\ dt\}_{i=0}^{m-2}$ (here we use invertibility of m in A), which shows $\operatorname{supp}(\pi_*\Omega_{N/M}) = \operatorname{supp}(\operatorname{div}(s))$. For the claim regarding étale-ness, we have already seen that π is flat and the local description shows that it is locally of finite presentation. To see that it is unramified, we may argue as in Proposition 2.2.17 and Corollary 2.2.23. That is, we commute pushforward along π with pullback to the residue field of a point in M, and then note that it suffices to check étale-ness on fibers [24, Corollary 17.2].

For (e), smoothness over k (equivalently, regularity because k is algebraically closed) follows from the local description and the Jacobian condition (see [39, Theorem 4.2.19] for the Jacobian criterion). To see that N is integral, first note that B is an integral domain, in the local notation above. This is because A is regular and A/a is regular hence reduced, so we may consider a height one prime containing a (by the Krull principal ideal theorem) and apply Eisenstein's criterion to $t^m - a$. That N is integral then follows because it is connected and covered by spectra of integral domains. We know N is dimension one because $N \to M$ is finite and M is dimension one. Properness of $N \to \operatorname{Spec} k$ follows because $N \to M$ is finte, hence proper, and $M \to \operatorname{Spec} k$ is assumed to be proper. □

Fix a divisor m of the degree d. So that we may apply Construction 2.2.29 for our situation and ensure separability for m-fold covers, we enlarge S so that $\mathcal{O}$ is a $\mathbb{Z}[1/m]$-scheme, i.e. S contains the primes lying above m.

$$
\begin{tikzcd}
 & & \mathcal{X}' \arrow[dd] \arrow[dr] & & & \\
 & & & \mathcal{X}'' \arrow[dd] & & \\
\Sigma_{\mathcal{C}} \arrow[rr] \arrow[dr] & & \Sigma \arrow[rr, crossing over] & & \mathbb{P}^2_{\mathcal{O}} \times_{\operatorname{Spec}\mathcal{O}} (\mathbb{P}^2_{\mathcal{O}})^* \arrow[dl] \arrow[dr] & \\
 & \mathcal{C} \arrow[rr] & & \mathbb{P}^2_{\mathcal{O}} & & (\mathbb{P}^2_{\mathcal{O}})^* \ .
\end{tikzcd}
\tag{2.9}
$$

Construction 2.2.30. We construct a relative smooth genus $g = 1 - m + \frac{1}{2}d(m-1)$ curve $\mathcal{X} \to \mathcal{Y}$.

Proof of Construction 2.2.30. We apply Construction 2.2.29 using

$$m, \quad M = \mathbb{P}^2_{\mathcal{O}}, \quad \mathcal{L} = \mathcal{O}(d/m), \quad \text{and } s \in \Gamma(\mathbb{P}^2_{\mathcal{O}}, \mathcal{O}(d)) \text{ such that } \operatorname{div}(s) = \mathcal{C}.$$

Note that such s exists by Corollary 2.2.26. Let $\mathcal{X}'' \to \mathbb{P}^2_{\mathcal{O}}$ be the constructed m-fold cover. This covering pulls back to $\mathcal{X}' \to \Sigma$ as depicted in Diagram (2.9). With the open immersion $\mathcal{Y} \to (\mathbb{P}^2_{\mathcal{O}})^*$ understood, write

$$\mathcal{X} = \mathcal{X}' \times_{(\mathbb{P}^2_{\mathcal{O}})^*} \mathcal{Y}.$$

We now verify that $\mathcal{X} \to \mathcal{Y}$ is a relative genus g curve. Properness follows because the covering $\mathcal{X}'' \to \mathbb{P}^2_{\mathcal{O}}$ is finite hence proper, closed immersions and $\mathbb{P}^2_{\mathbb{Z}} \to \mathbb{Z}$ are proper, and properness is stable under composition and base-change. All morphisms from Diagram (2.9) are finite type morphisms of noetherian schems, so $\mathcal{X} \to \mathcal{Y}$ will be locally of finite presentation.

We verify flatness of $\mathcal{X}' \to (\mathbb{P}^2_{\mathcal{O}})^*$, which will imply flatness for $\mathcal{X} \to \mathcal{Y}$. We know $\mathcal{X}'' \to \mathbb{P}^2_{\mathcal{O}}$ is flat from Construction 2.2.29, and we also know $\Sigma \to (\mathbb{P}^2_{\mathcal{O}})^*$ is flat by Proposition 2.2.21. Thus $\mathcal{X}' \to (\mathbb{P}^2_{\mathcal{O}})^*$ is flat because flatness is stable under composition and base-change.

It remains to check that the geometric fibers are regular. If $\bar{s}\colon \operatorname{Spec} k \to (\mathbb{P}^2_{\mathcal{O}})^*$ is a geometric point, we have $\Sigma_{\bar{s}} \cong \mathbb{P}^1_k$. We may compute the fiber of $\mathcal{X}' \to \Sigma$ over $\Sigma_{\bar{s}}$ using the compatibility under pullback that was shown in Construction 2.2.29(a). Since $\Sigma_{\bar{s}} \to \mathbb{P}^2_k$ is a line, the sheaf $\mathcal{O}(1)$ on $\mathbb{P}^2_{\mathcal{O}}$ pulls back to $\mathcal{O}(1)$ on $\Sigma_{\bar{s}}$. So the fiber $\mathcal{X}' \to \Sigma$ over $\Sigma_{\bar{s}}$ is given by Construction 2.2.29 applied to

$$m, \quad M = \mathbb{P}^1_k, \quad \mathcal{L} = \mathcal{O}(d/2), \quad \text{and } s \in \Gamma(\mathbb{P}^1_k, \mathcal{O}(d)) \text{ such that } \operatorname{div}(s) = (\Sigma_{\mathcal{C}})_{\bar{s}}.$$

Furthermore, if $\bar{s}$ factors through $\mathcal{Y}$, then $\operatorname{div}(s)$ is regular since $(\Sigma_C)_{\mathcal{Y}} \to \mathcal{Y}$ is unramified by Corollary 2.2.23 (recall that, informally, geometric points $\bar{s}$ of $\mathcal{Y}$ correspond to lines which are not tangent to $\mathcal{C}_k$, and $(\Sigma_C)_{\bar{s}}$ is the intersection). By Construction 2.2.29(e) we conclude that $\mathcal{X}_{\bar{t}}$ is a regular curve. The m-fold cover $\mathcal{X}_{\bar{t}} \to \Sigma_{\bar{t}}$ is separable since k has characteristic coprime to m (we have inverted m in $\mathcal{O}$ by expanding S), so the Riemann-Hurwitz formula shows that $\mathcal{X}$ has genus $g = 1 - m + \frac{1}{2}d(m-1)$ as claimed. $\square$

2.2.3 Finiteness of integer points

In this section, we study the family $\mathcal{X} \to \mathcal{Y}$ from Construction 2.2.29, and we rule out isotriviality of along geometric components of any positive dimension closed subscheme of $\mathcal{Y}$. As discussed previously, this allows us to prove Theorem 2.2.4 using Corollary 2.1.4.

We know that geometric fibers of $\mathcal{X} \to \mathcal{Y}$ are cyclic covers of $\mathbb{P}^1_k$ with branch points that can be explicitly described, i.e. the intersection of a line with C_k. We study the variation of these branch points.

Lemma 2.2.31. *Fix a rational prime p and an integer $r \geq 3$. Let X be a nonsingular projective curve over $\mathbb{C}$. Consider covers $X \xrightarrow{\alpha} \mathbb{P}^1_{\mathbb{C}}$ and $X \xrightarrow{\beta} \mathbb{P}^1_{\mathbb{C}}$ which*

- *are degree p,*
- *have all ramification indices equal to 1 or p,*
- *and are branched at $r \cdot p$ points on $\mathbb{P}^1_{\mathbb{C}}$.*

There is a unique automorphism $\mathbb{P}^1_{\mathbb{C}} \xrightarrow{\phi} \mathbb{P}^1_{\mathbb{C}}$ such that the following diagram commutes:

$$\begin{tikzcd} & X \arrow[dl, "\beta"'] \arrow[dr, "\alpha"] & \\ \mathbb{P}^1_{\mathbb{C}} \arrow[rr, "\phi"] & & \mathbb{P}^1_{\mathbb{C}} \end{tikzcd} .$$

In particular, ϕ bijectively maps the set of branch points of β to the set of branch points of α.

We have that p-fold Cyclic covers of $\mathbb{P}^1_{\mathbb{C}}$, as in Construction 2.2.29, with a reduced branch locus consisting of at least $3 \cdot p$ points satisfy these condition. Lemma 2.2.31 is a direct consequence of a result of Namba [45] as stated in [29]: if a compact Riemann surface M of genus $g \geq (p-1)^2 + 1$ admits a degree p cover of $\mathbb{P}^1_{\mathbb{C}}$, then M has a unique base-point free linear system of degree p and dimension 1.

Proof. Using the Riemann-Hurwitz formula, we calculate that X has genus

$$g = \frac{1}{2}(p-1)(rp-2).$$

When $r \geq 3$, we have $g \geq (p-1)^2 + 1$ for $p \geq 2$, so the described result of Namba [45] implies that the automorphism ϕ exists. Uniqueness follows from surjectivity of β. $\square$

Lemma 2.2.31 lets us study isomorphism classes of cyclic covers of $\mathbb{P}^1_{\mathbb{C}}$ via their branch points. Informally speaking, we control the way branch points may collide in an isotrivial family. To this end, we introduce a numerical invariant for sets of points on $\mathbb{P}^1_{\mathbb{C}}$.

Definition 2.2.32. Let $r \geq 4$. Consider distinct points $q_1, \ldots, q_r \in \mathbb{P}^1_{\mathbb{C}}$. Pick any affine chart $\mathbb{A}^1_{\mathbb{C}} \simeq \mathbb{C}$ containing all r points, and let $z_1, \ldots, z_r \in \mathbb{C}$ be the corresponding complex numbers. Then we set

$$\operatorname{prox}(q_1, \ldots, q_r) = \min_{\substack{i,j,k,l \\ \text{distinct}}} \left(\left| \frac{\phi_{z_l}(z_i) - \phi_{z_l}(z_j)}{\phi_{z_l}(z_i) - \phi_{z_l}(z_k)} \right| \right) \quad \text{where } \phi_{z_l}(z) = \frac{1}{z - z_l}. \tag{2.10}$$

Notation 2.2.33. Given $z_1, \ldots, z_r \in \mathbb{C}$, we'll write $\operatorname{prox}(z_1, \ldots, z_r)$ for the function defined in Equation (2.10) for convenience (i.e. inputs of this function are complex numbers, rather than points on $\mathbb{P}^1_{\mathbb{C}}$).

Well-definedness will be verified in Lemma 2.2.34 below. Informally speaking, the quantity of Definition 2.2.32 is meant to measure the proximity of $z_1, \ldots, z_r \in \mathbb{C}$ to one another, in a way that is invariant under automorphisms of $\mathbb{P}^1_{\mathbb{C}}$.

Lemma 2.2.34. *In the notation of Definition 2.2.32,* $\operatorname{prox}(q_1, \ldots, q_r)$ *is independent of the affine chart* $\mathbb{A}^1_{\mathbb{C}} \simeq \mathbb{C}$*. Furthermore, we have*

$$\operatorname{prox}(\phi(q_1), \ldots, \phi(q_r)) = \operatorname{prox}(q_1, \ldots, q_r)$$

for any automorphism ϕ *of* $\mathbb{P}^1_{\mathbb{C}}$*.*

Proof. Chart independence amounts to the following claim:

$$\operatorname{prox}(\phi(z_1), \ldots, \phi(z_r)) = \operatorname{prox}(z_1, \ldots, z_r) \tag{2.11}$$

for any linear fractional transformation ϕ, i.e.

$$\phi(z) = \frac{az + b}{cz + d} \quad \text{with } a, b, c, d \in \mathbb{C},$$

such that $\phi(z_i) \neq \infty$ for all i. This is a straightforward check: note that $\phi_{\phi(z_l)} \circ \phi$ and ϕ_{z_l} both send $z_l \mapsto \infty$, so we must have $\phi_{\phi(z_l)} \circ \phi = \psi \circ \phi_l$ for some linear affine transformation, i.e. $\psi(z) = ez + f$

with $e, f \in \mathbb{C}$. Since

$$\frac{\psi(w_1) - \psi(w_2)}{\psi(w_3) - \psi(w_4)} = \frac{w_1 - w_2}{w_3 - w_4}$$

for distinct $w_1, w_2, w_3, w_4 \in \mathbb{C}$, the claim about chart independence follows.

The second half of the lemma regarding automorphisms of $\mathbb{P}^1_{\mathbb{C}}$ also follow from this computation: pick a chart $\mathbb{A}^1_{\mathbb{C}}$, that contains all q_i and $\phi(q_i)$, and directly apply the previous computation justifying Equation (2.11). $\square$

We use $\operatorname{prox}(q_1, \ldots, q_r)$ to measure degeneration as in the following lemma.

Lemma 2.2.35. *Fix $r \geq 4$ and consider continuous functions*

$$\begin{aligned} [0,1] &\xrightarrow{z_i} \mathbb{C} \\ t &\longmapsto z_i(t) \qquad \textit{for } 1 \leq i \leq r \end{aligned}$$

satisfying the following properties:

- *For any fixed $0 \leq t < 1$, all $z_i(t)$ are distinct.*
- *For $t = 1$, at least two of the $z_i(t)$ intersect.*
- *For $t = 1$, no $r - 1$ of the $z_i(t)$ coincide.*

Then we have

$$\lim_{t \to 0} \operatorname{prox}(z_1(t), \ldots, z_r(t)) = 0$$

Proof. The computation which follows is a straightforward check. Without loss of generality, suppose that $z_1(t)$ and $z_2(t)$ intersect at $t = 1$, and also that neither $z_3(t)$ nor $z_4(t)$ intersect $z_1(t)$ at $t = 1$. Furthermore, we apply a translation so that $z_r(t)$ is constant - this is permissible by Lemma 2.2.34. Then

$$\lim_{t \to 0} |\phi_{z_4}(z_1(t)) - \phi_{z_4}(z_2(t))| = 0 \quad \text{and} \quad \lim_{t \to 0} |\phi_{z_4}(z_1(t)) - \phi_{z_4}(z_3(t))| > 0 \quad (\text{possibly } +\infty)$$

which proves the lemma, by definition of $\operatorname{prox}(z_1(t), \ldots, z_r(t))$. $\square$

Notation 2.2.36. If X is a nonsingular projective curve over $\mathbb{C}$ admitting a cover $X \to \mathbb{P}^1_{\mathbb{C}}$ satisfying the conditions of Lemma 2.2.31, write $\operatorname{prox}(X) = \operatorname{prox}(q_1, \ldots, q_{mp})$, where $q_i \in \mathbb{P}^1_{\mathbb{C}}$ are the branch points. This is well-defined by Lemma 2.2.31 and Lemma 2.2.34, and is positive by construction (all q_i are distinct).

Proof of Theorem 2.2.4. By Proposition 2.2.28, we may prove finiteness of $\mathcal{Y}(\mathcal{O})$. Let $\mathcal{Z}$ be its Zariski closure, with the reduced induced structure. If $\mathcal{Z}_{\mathbb{C}}$ has dimension zero (i.e. it is finitely many points) then $\mathcal{Y}(\mathcal{O})$ is certainly finite by separatedness, so suppose instead that $\mathcal{Z}_{\mathbb{C}} \to \mathcal{Y}_{\mathbb{C}}$ has positive dimension, and pick a connected component W with positive dimension.

Using the base-change compatibility of Construction 2.2.29, we can be explicit about the family $\mathcal{X}'_{\mathbb{C}} \to (\mathbb{P}^2_{\mathbb{C}})^*$ (see Construction 2.2.30 for notation). Write $h(x, y, z)$ for a homogeneous degree d equation defining $C_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$. In the affine chart $a \neq 0$ (recall that we have set a, b, c as homogeneous coordinates on $(\mathbb{P}^2_{\mathbb{C}})^*$), the fiber above a point $(a : b : c)$ is an m-fold cyclic cover of $\mathbb{P}^1_{\mathbb{C}}$ whose branch divisor (i.e. $\operatorname{div}(s)$ in the notation of Construction 2.2.29) is given by

$$h\left(\frac{by + cz}{-a}, y, z\right), \tag{2.12}$$

and similarly in the charts $b \neq 0$ and $c \neq 0$.

By Bézout's theorem, the Zariski closure $\overline{W}$ of W in $(\mathbb{P}^2_{\mathbb{C}})^*$ must intersect the dual curve $(C^*)_{\mathbb{C}}$. Select a path γ in $\overline{W}$, i.e. a continuous map $\gamma\colon [0, 1] \to \overline{W}$, such that $\gamma(1)$ lies on $(C^*)_{\mathbb{C}}$, and $\gamma(t)$ lies in W for $0 \leq t < 1$. Write X_t for the fiber of $\mathcal{X}'_{\mathbb{C}} \to (\mathbb{P}^2_{\mathbb{C}})^*$ over $\gamma(t)$. By Corollary 2.1.4, all X_t are isomorphic, for $0 \leq t < 1$. Furthermore, we may assume without loss of generality that the image of γ lies in the chart $a \neq 0$ of $(\mathbb{P}^2_{\mathbb{C}})^*$. Then, $-b/a$ and c/a pull back along γ to continuous functions of t, so substituting in Equation (2.12) yields a function

$$\tilde{h}(t, y, z) \tag{2.13}$$

which is a homogeneous polynomial of degree d in y and z whose coefficents are $\mathbb{C}$-valued continuous functions of t, and whose evaluation at a fixed t gives an equation defining the branch divisor of $X_t \to \mathbb{P}^1_{\mathbb{C}}$. We may change variables so that $\tilde{h}(1, 1, 0) \neq 0$. Since the complex roots of a complex polynomial vary continuously with continuously varying coefficients [26], we may modify γ if necessary (i.e. shorten it) so that $\tilde{h}(t, 1, 0) \neq 0$ for all t. Then, we have d continuous functions $[0, 1] \xrightarrow{x_i} \mathbb{C}$ such that

$$\tilde{h}(t, y, z) = \prod_{i=1}^{d} (y - z_i(t) z)$$

up to a scalar. This is because the roots must vary continuously.

By Proposition 2.2.17 and Lemma 2.2.19, the condition that $\gamma(t)$ lies in W (hence $\mathcal{Y}_{\mathbb{C}}$) implies that all $z_i(t)$ are distinct for fixed t with $0 \leq 1 < 1$. Similarly, at least two of the $z_i(t)$ coincide at $t = 1$ because $\gamma(1)$ lies on the dual curve $(C^*)_{\mathbb{C}}$. The conditions of Theorem 2.2.4 that $C_{\overline{K}}$ has no $r-1$-fold or r-fold tangents imply that no $r-1$ of the $z_i(t)$ coincide at $t = 1$.

Thus, the hypotheses of Lemma 2.2.35 are satisfied, which implies

$$\lim_{t \to 0} \operatorname{prox}(z_1(t), \ldots, z_d(t)) = 0. \tag{2.14}$$

Since we have assumed in Theorem 2.2.4 that d is non-prime of degree $d \geq 6$, we may select $r \geq 3$ and p prime such that $d = r \cdot p$. Set $m = r$, in the notation of Construction 2.2.30.

Then all X_t for $0 \leq t < 1$ satisfy the conditions of Lemma 2.2.31, and Equation (2.14) cannot hold, as all such X_t are isomorphic by construction. That is, for $0 \leq t < 1$, the quantity $\operatorname{prox}(z_1(t), \ldots, z_d(t))$ must be equal to some fixed positive constant (what we called $\operatorname{prox}(X_0)$ in Notation 2.2.36), a contradiction. $\square$

Chapter 3

Integer points on genus one modular curves

In this chapter we prove finiteness of integral points on open modular curves $Y_1(N)$ whose compactifications are genus one. This is not a new result, but we give a proof that adapts the methods of a recent new proof of the Mordell conjecture, on the finiteness of rational points on curves of genus at least two [36]. That paper also uses these techniques to prove the S-unit equation using the Legendre family of elliptic curves; our study of modular curves in this chapter is similar in spirit.

We now give a very brief description of the general idea. The initial setup is similar to that of Chapter 2: given a relative curve $\mathcal{X} \to \mathcal{Y}$ defined over $\mathcal{O}$, fibers over elements of $\mathcal{Y}(\mathcal{O})$ are curves with good reduction outside S, upon base-change to K. We apply this to the universal elliptic curve over our modular curve.

Instead of using the Shafarevich conjecture (Theorem 2.1.2), we use the fact that the corresponding local Galois representations will be crystalline, and that their variation may be studied in the category $\mathrm{MF}^{\phi}_{K_v}$ using a v-adic period mapping, see Section 3.1. This, in turn, may be compared with de Rham cohomology and the Hodge filtration. Using a result of Faltings, we are able to reduce the theorem to showing that there are only finitely many points whose Galois representations lie in a fixed isomorphism class, see Lemma 3.3.5. Bounding such a set amounts to bounding a certain centralizer, on the level of objects in $\mathrm{MF}^{\phi}_{K_v}$, relative to the image of a full residue disc under the period map. This is accomplished by a modification of the universal elliptic curve, whose construction is described in Section 3.2, and an explicit monodromy computation from Section 3.3.1.

Theorem 3.0.1. *Let $N \geq 4$ be an integer. There is a smooth affine curve $\mathcal{Y} \to \mathbb{Z}[1/N]$ which* *represents the functor*

$$\mathbf{Sch}/\mathbb{Z}[1/N] \to \mathbf{Set}$$

$$Z \mapsto \left\{ \begin{array}{c} \textit{Isomorphism classes of } (E/Z, \alpha) \textit{ where} \\ E/Z \textit{ is an elliptic curve and } \alpha \in E(Z) \\ \textit{is exact order } N \textit{ in each geometric fiber} \end{array} \right\}.$$

Furthermore, $\mathcal{Y} \to \mathbb{Z}[1/N]$ *is an open subscheme of a proper smooth curve* $\mathcal{X} \to \mathbb{Z}[1/N]$.

Taking base-change yields the modular curves $\mathcal{X}_{\mathbb{C}} = X_1(N)$ and $\mathcal{Y}_{\mathbb{C}} = Y_1(N)$ over $\mathbb{C}$. We will be interested in values of N for which $\mathcal{X} \to \mathbb{Z}[1/N]$ is a genus one curve, for example $N = 11$. For the rest of this section, fix such an N. Using Notation 1.0.3, expand the set S so it contains all primes lying above those dividing N, and reuse the symbols $\mathcal{X}$ and $\mathcal{Y}$ in place of $\mathcal{X}_{\mathcal{O}}$ and $\mathcal{Y}_{\mathcal{O}}$.

Theorem 3.0.2. *The set* $\mathcal{Y}(\mathcal{O})$ *is finite.*

This result is certainly not new. For example, it is an immediate consequence of Siegel's theorem on integer points and is also a consequence of the Shafarevich conjecture. As mentioned above, our objective is to study this question using the p-adic period mapping and techniques from [36].

The representability described in Theorem 3.0.1 implies that $\mathcal{Y}$ carries a relative elliptic curve $\mathcal{E} \to \mathcal{Y}$ which is universal for the moduli problem described in Theorem 3.0.1. We would like to study the variation of Galois representations in this family of curves, but we will need to introduce a modified version of this family, as will be discussed in Section 3.2.1.

As in Remark 2.2.6, we may freely enlarge the number field K and the finite set of primes S to prove Theorem 3.0.1, and we make use of this fact during the proof without further comment.

3.1 Preliminaries

This section is devoted to collecting facts on p-adic Hodge theory, the period map, and some related results from [36]. These are facts that we will use in Section 3.3.3, and have been included here in an effort to be somewhat self-contained. Until noted in Section 3.2.1, we recycle the symbols $\mathcal{X}, \mathcal{Y}$, etc. to denote general schemes, and not necessarily the modular curves described in Theorem 3.0.1.

3.1.1 Preliminaries from p-adic Hodge theory

In this section, we collect some facts about Galois representations and p-adic Hodge theory.

Let $X \to Y$ be a morphism of K-schemes, and $X_{K_v} \to Y_{K_v}$ be the corresponding morphism of K_v-schemes. Let $y \in Y(L)$. The fiber of y in Y_{K_v} is a closed subscheme

$$\operatorname{Spec}(L \otimes_K K_v) = \operatorname{Spec}\left(\bigoplus L_{w_i}\right)$$

where w_i are the primes lying above v. Write y_i for the corresponding L_{w_i} point in Y_{K_v}.

Lemma 3.1.1. *When restricted to $G_{L_{w_i}}$, the G_L-module $H^*_{\text{et}}(X_y \times_L \overline{L}, \mathbb{Q}_p)$ is isomorphic to the $G_{L_{w_i}}$ module $H^*_{\text{et}}(X_{K_v,y_i} \times_{L_{w_i}} \overline{L_{w_i}}, \mathbb{Q}_p)$.*

Proof. The restriction of the G_L-module $H^*_{\text{et}}(X_y \times_L \overline{L}, \mathbb{Q}_p)$ to $G_{L_{w_i}}$ is given by $H^*_{\text{et}}((X_y)_{L_{w_i}} \times_{L_{w_i}} \overline{L_{w_i}}, \mathbb{Q}_p)$. The lemma follows upon verifying that $(X_y)_{L_{w_i}} = (X_y) \times_L L_{w_i}$ is naturally isomorphic to X_{K_v,y_i}, i.e. that we have the fiber product

$$\begin{array}{ccc} X \times_L L_{w_i} & \longrightarrow & X \times_K K_v \\ \downarrow & & \downarrow \\ L_{w_i} & \longrightarrow & L \times_K K_v \ . \end{array}$$

$\square$

Lemma 3.1.2. *Let X be smooth curve over L. We have an isomorphism of G_K-modules*

$$H^1_{\text{et}}(X \times_K \overline{K}, \mathbb{Q}_p) \cong H^1_{\text{et}}(\operatorname{Res}_{L/K} X \times_K \overline{K}, \mathbb{Q}_p).$$

On the left-hand side, X is given the structure of an K-scheme via $X \to \operatorname{Spec} L \to \operatorname{Spec} K$. The same holds when L, K are replaced with L_{w_i}, K_v.

Proof. One computes that

$$X \times_K L \cong \coprod_{\sigma \in \mathrm{Gal}(L/K)} X^\sigma \qquad \text{and} \qquad \left(\operatorname{Res}_{L/K} X\right) \times_K L \cong \prod_{\sigma \in \mathrm{Gal}(L/K)} X^\sigma,$$

where the product is over L. For $\operatorname{Res}_{L/K}$, see for instance the discussion in [58, §I.3] or the notes at [40]. We can then identify

$$H^1_{\text{et}}(X \times_K \overline{K}, \mathbb{Q}_p) \cong \bigoplus_{\sigma \in \mathrm{Gal}(L/K)} H^1_{\text{et}}(X^\sigma \times_L \overline{L}, \mathbb{Q}_p)$$

$$H^1_{\text{et}}\left(\prod_{\sigma \in \mathrm{Gal}(L/K)} \left(X^\sigma \times_L \overline{L}\right), \mathbb{Q}_p\right) \cong H^1_{\text{et}}(\operatorname{Res}_{L/K} X \times_K \overline{K}, \mathbb{Q}_p).$$

Using the Künneth formula for étale cohomology and noting $H^0_{\text{et}}(X^\sigma \times_L \overline{L}, \mathbb{Q}_p) = \mathbb{Q}_p$, we have

$$\bigoplus_{\sigma \in \mathrm{Gal}(L/K)} H^1_{\text{et}}(X^\sigma \times_L \overline{L}, \mathbb{Q}_p) \xrightarrow{\sim} H^1_{\text{et}}\left(\prod_{\sigma \in \mathrm{Gal}(L/K)} \left(X^\sigma \times_L \overline{L}\right), \mathbb{Q}_p \right),$$

and G_K-equivariance follows from naturality. $\square$

See a general version of the Künneth formula in [9, Corollary 1.11]. For a statement closer to the one applied here, here [42, Theorem 22.4].

In the following diagram, we collect the morphisms underlying our interchange between schemes, Galois representations, and filtered ϕ-modules. By "naive restriction", we mean an L_w scheme X viewed as a K_v scheme via $X \to L_w \to K_v$. Our main reference for this material is the exposition in [5].

Proposition 3.1.3. *We have the diagram*

$$\begin{tikzcd}[column sep=large, row sep=huge]
\text{\textit{Elliptic curves over } } L_w \text{ \textit{with good reduction}} \arrow[r, "H^1_{\text{et}}(- \times_{L_w} \overline{L_w}, \mathbb{Q}_p)"] \arrow[d, bend right=60, "\text{\textit{naive restriction}}"'] \arrow[d, bend left=60, "\mathrm{Res}_{L_w/K_v}(-)"] & \mathrm{Rep}^{\text{cris}}_{\mathbb{Q}_p}(G_{L_w}) \arrow[r, "D_{\text{cris}}(-)"] \arrow[d, bend right=60, "\text{\textit{scalar extension}}"'] \arrow[d, bend left=60, "\mathrm{Ind}^{G_{K_v}}_{G_{L_w}}(-)"] & \mathrm{MF}^\phi_{L_w} \arrow[d, bend left=60, "\text{\textit{forget}}"] \\
\text{\textit{Elliptic curves over } } K_v \text{ \textit{with good reduction}} \arrow[r, "H^1_{\text{et}}(- \times_{K_v} \overline{K_v}, \mathbb{Q}_p)"] \arrow[u, "- \times_{K_v} L_w"] \arrow[u, phantom, shift right=6ex, "\dashv"] \arrow[u, phantom, shift left=6ex, "\dashv"] & \mathrm{Rep}^{\text{cris}}_{\mathbb{Q}_p}(G_{K_v}) \arrow[r, "D_{\text{cris}}(-)"] \arrow[u, "-|G_{L_w}"] \arrow[u, phantom, shift right=6ex, "\dashv"] \arrow[u, phantom, shift left=6ex, "\dashv"] & \mathrm{MF}^\phi_{K_v} \arrow[u, "- \otimes_{K_v} L_w"] \arrow[u, phantom, shift left=6ex, "\dashv"]
\end{tikzcd}.$$

The arrows $D_{\text{cris}}(-)$ are fully-faithful embeddings. "Parallel" vertical arrows yield commutative diagrams.

Proof. The adjunctions for the left-most categories follow from definitions, and the other adjunctions are those between extension, restriction, and co-extension of scalars (as $\mathbb{Q}_p[G_{L_w}]$- and $\mathbb{Q}_p[G_{K_v}]$-modules for the middle categories). That $H^*_{\text{et}}\left(- \times_{K_v} \overline{K_v}, \mathbb{Q}_p\right)$ takes schemes with good reduction to crystalline representations is from work of Brueil [4, Thm. 1.4], Fontaine [21, 5.5,6.2], Grothendieck [25, Exp. IX,Thm. 5.13], and Kisin [32, Cor 2.2.6]. See also exposition in [5, §7.1]. That $- \times_{K_v} L_w$ corresponds to the restriction $-|G_{L_w}$ follows from definitions.

For abelian varieties A, $H^1_{\text{et}}(A \times_{L_w} \overline{L_w}, \mathbb{Q}_p)$ is dual to $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. That the Galois representation associated to $\mathrm{Res}_{L_w/K_v}(-)$ then corresponds to $\mathrm{Ind}^{G_{K_v}}_{G_{L_w}} V_p(-)$ is written out, for example, in [30, Example 4.11].

In Lemma 3.1.2 we saw that the naive restriction and Res_{L_w/K_v} agree same after taking $H^1_{\mathrm{et}}\left(- \times_{K_v} \overline{K_v}, \mathbb{Q}_p\right)$. Since G_{K_v}/G_{L_w} is finite, scalar extension and $\mathrm{Ind}_{G_{L_w}}^{G_{K_v}}$ coincide as well – see [22, Exericse 4.1.4] or [5, Exercise 3.4.3].

For correspondences with the morphisms between $\mathrm{MF}^{\phi}_{L_w}$ and $\mathrm{MF}^{\phi}_{K_v}$, we refer to the exposition in [5], see for example Exercise 3.4.3. We remark that, once the correspondence between restriction $-|G_{L_w}$ and $- \otimes_{K_v} L_w$ is established, one way to obtain the correspondence between $\mathrm{Ind}_{G_{L_w}}^{G_{K_v}}$ and *forget* is as follows: D_{cris} is fully faithful (see exposition in [5, Proposition 9.1.11]), with essential image the so-called weakly admissible objects, see [6, Thm. A]. Upon checking that $\mathrm{Ind}_{G_{L_w}}^{G_{K_v}}$ preserves the property of being crystalline and that the forgetful functor preserves weak-admissibility (use for example the criterion [5, Lemma 8.1.13] due to Fontaine as well as [5, Proposition 9.3.1]), we may match the two as right adjoints to $|G_{L_w}$ and $- \otimes_{K_v} L_w$ respectively.

□

3.1.2 Preliminaries on period maps

The primary source for the exposition in this section is [36, §3]. We use period maps to study the variation of Hodge structures in a family and make use of a comparison between the complex and p-adic period maps.

Let $\mathcal{X} \to \mathcal{Y}$ be a proper smooth morphism of smooth finite type $\mathcal{O}$-schemes, and write $X \to Y$ for the base-change to K. Suppose, further, that Y is an integral scheme. Fix embeddings $\iota\colon K \to \mathbb{C}$ and $v\colon K \to K_v$, choosing v lying over a rational prime p so that

- we have $p > 2$,
- we have $K_v/\mathbb{Q}_p$ unramified,
- and no prime above p lies in S.

Also, fix a base-point $y_0 \in \mathcal{Y}(\mathcal{O})$. With some abuse of notation, we also use y_0 to denote the corresponding point in $Y(K)$, $Y_{\mathbb{C}}(\mathbb{C})$, and $Y_{K_v}(K_v)$. Consider the base-changes $X_{\mathbb{C}} \to Y_{\mathbb{C}}$ and $X_{K_v} \to Y_{K_v}$. Fix the v-adic neighborhood $\Omega_v = \{y \in Y_{K_v}(K_v) : y \text{ extends to an } \mathcal{O}_v \text{ point } y \equiv y_0 \pmod{v}\}$. For a sufficiently small neighborhood Ω_ι of y_0 in the complex topology on $Y_{\mathbb{C}}(\mathbb{C})$, and a fixed nonnegative integer q, the *Gauss-Manin connection* gives identifications of de-Rham cohomologies

$$H^q_{\mathrm{dR}}(X_{K_v,y_0}/K_v) \xrightarrow{\sim} H^q_{\mathrm{dR}}(X_{K_v,y}/K_v) \quad \text{for } y \in \Omega_v \tag{3.1}$$
$$H^q_{\mathrm{dR}}(X_{\mathbb{C},y_0}/\mathbb{C}) \xrightarrow{\sim} H^q_{\mathrm{dR}}(X_{\mathbb{C},y}/\mathbb{C}) \quad \text{for } y \in \Omega_\iota.$$

Furthermore, the Gauss-Manin connection in Ω_v is compatible with the Frobenius operator ϕ on $H^q_{\mathrm{dR}}(X_{K_v,y}/K_v)$. See [36, Diagram 3.9] and the references [3, Corollary 7.4] and [2, Ch V].

The Gauss-Manin connection, however, need not identify the Hodge filtrations, and the period maps detect the variation of these filtrations in Ω_v and Ω_ι. Set

$$V = H^q_{\mathrm{dR}}(X_{y_0}/K) \tag{3.2}$$

and consider the Hodge filtration $V = F^0V \supseteq F^1V \supseteq \cdots$. Then we form the flag variety $\mathcal{H}/K$ whose K-points are flags in V with the same dimensional data.

Set $V_{\mathbb{C}} = V \otimes_K \mathbb{C}$ and $V_{K_v} = V \otimes_K K_v$. For each $y \in \Omega_v$, the identification of Equation (3.1) carries the Hodge filtration on $H^q_{\mathrm{dR}}(X_{K_v,y}/K)$ to a flag on V_{K_v}, which we denote $h^v_y \in \mathcal{H}_{K_v}(K_v)$. We similarly write $h^\iota_y \in \mathcal{H}_{\mathbb{C}}(\mathbb{C})$ for $y \in \Omega_\iota$. Thus we have *period maps*

$$\begin{array}{ccccccc} \Omega_v & \xrightarrow{\Phi_v} & \mathcal{H}_{K_v}(K_v) & \qquad & \Omega_\iota & \xrightarrow{\Phi_\iota} & \mathcal{H}_{\mathbb{C}}(\mathbb{C}) \\ y & \longmapsto & h^v_y & & y & \longmapsto & h^\iota_y\ . \end{array}$$

The period maps Φ_v and Φ_ι are moreover K_v- and $\mathbb{C}$-analytic, respectively, i.e they are defined by power series which are absolutely convergent on Ω_v and Ω_ι respectively; we refer to [36, § 3.3] on this. The complex period map Φ_ι will be used via the following lemma.

Lemma 3.1.4 (Lemma 3.1 in [36])**.** *The Zariski closure of $\Phi_v(\Omega_v)$ in $\mathcal{H}_{K_v}$ has dimension equal to that of the Zariski closure of $\Phi_\iota(\Omega_\iota)$ in $\mathcal{H}_{\mathbb{C}}$.*

We omit the proof, referring to [36]; the key point is that both period maps may be expressed using the same power series with K-coefficients. This lemma allows us to study the v-adic period map through the complex period map, as a proxy. In turn, the complex period map may be studied via monodromy, which we now describe.

We have only discussed the complex period map Φ_ι on the neighborhood $\Omega_{\mathbb{C}} \subset Y_{\mathbb{C}}(\mathbb{C})$. However, it extends to an analytic map $\Phi_\iota \colon \widetilde{Y_{\mathbb{C}}(\mathbb{C})} \to \mathcal{H}_{\mathbb{C}}(\mathbb{C})$, where $\widetilde{Y_{\mathbb{C}}(\mathbb{C})}$ is the universal cover of $Y_{\mathbb{C}}(\mathbb{C})$. Furthermore, there is a monodromy action of $\pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0)$ on $V_{\mathbb{C}}$ and thus $\mathcal{H}(\mathbb{C})$, and the period map Φ_ι from the universal cover is equivariant under this monodromy action.

If W denotes the Zariski closure of $\Phi_\iota(\Omega_\iota)$ in $\mathcal{H}_{\mathbb{C}}$, the pre-image $\Phi_\iota^{-1}(W) \subseteq \widetilde{Y_{\mathbb{C}}(\mathbb{C})}$ must contain all of $\widetilde{Y_{\mathbb{C}}(\mathbb{C})}$, i.e. it is an analytic set containing an open disc. In particular, $\Phi_\iota^{-1}(W)$ must contain all $\pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0)$ translates of Ω_ι, so

$$W \supseteq \pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0) \cdot h^\iota_{y_0} \tag{3.3}$$

which will allow us to calculate a lower bound on the dimension of W, and thus the dimension of the Zariski closure of $\Phi_v(\Omega_v)$ by Lemma 3.1.4. Write $\overline{\pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0) \cdot h^\iota_{y_0}}$ for the Zariski closure in $\mathcal{H}_{\mathbb{C}}$. The following is a repackaged version of [36, Proposition 3.3].

Corollary 3.1.5. *Let G be a subgroup of $\mathrm{GL}(V_v)$, and fix some $h^v \in \mathcal{H}_{K_v}$. If the Zariski closure $\overline{G}$ in $\mathrm{GL}(V_v)$, viewed as an algebraic group, has dimension*

$$\dim(\overline{G}) < \dim(\overline{\pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0) \cdot h^\iota_{y_0}})$$

then $\Phi_v^{-1}(G \cdot h^v)$ is contained in a K_v-analytic strict subset of Ω_v – by this, we mean the zero set of a nonzero absolutely convergent power series on Ω_v. Here $G \cdot h^v$ is the orbit of h^v under the G-action on $\mathcal{H}_{K_v}$. In particular, if Y is dimension one then $\Phi_v^{-1}(G \cdot h^v)$ must be finite.

Proof. The flag variety $\mathcal{H}_{K_v}$ is a quotient of $\mathrm{GL}(V_v)$ by some parabolic subgroup. Then the orbit $G \cdot h^v$ is the image of some translate of G under the quotient $\mathrm{GL}(V_v) \to \mathcal{H}_{K_v}$, a morphism of varieties. The Zariski closure of this image has dimension bounded above by $\dim(\overline{G})$. By Lemma 3.1.4 and Equation (3.3), we know the Zariski closure of $\Phi_v(\Omega_v)$ has dimension bounded below by $\dim(\overline{\pi_1(Y_{\mathbb{C}}(\mathbb{C}), y_0) \cdot h^\iota_{y_0}})$. More explicitly, if we embed $\mathcal{H}_{K_v}$ into projective space, this means there is some homogeneous polynomial which vanishes on $G \cdot h^v$ but not all of $\Phi_v(\Omega_v)$. Since Φ_v is itself K_v-analytic, such a homogeneous polynomial pulls back to a nonzero K_v-analytic function on Ω_v, and its zeroes contain $\Phi_v^{-1}(G \cdot h^v)$. □

3.2 Set-up

3.2.1 Genus one modular curves as elliptic curves

For the rest of the chapter, we reserve the symbols $\mathcal{X}$ and $\mathcal{Y}$ for the modular curves over $\mathcal{O}$ as described in Theorem 3.0.1 and the following discussion. It will be useful to view $\mathcal{X} \to \operatorname{Spec} \mathcal{O}$ (see

Theorem 3.0.1 and the following discussion for notation) as a relative elliptic curve with a group structure, rather than just a relative genus one curve.

Definition 3.2.1. We refer to the reduced induced structure on $\mathcal{X} \setminus \mathcal{Y}$ as the *cuspidal divisor*, or the *cusps*.

The cuspidal divisor is finite étale over $\operatorname{Spec} \mathcal{O}$, see [11, Theorem IV.3.4]. Upon expanding the number field K, we may assume that the cuspidal divisor admits a section – indeed, it admits a K-rational point for a suitable finite extension of K, and properness implies that this extends to an $\mathcal{O}$-point.

Definition 3.2.2. Fix once and for all a section $e \in \mathcal{X}(\mathcal{O})$ of the cuspidal divisor. We refer to the elliptic curve $\mathcal{X} \to \mathcal{O}$ as this relative genus one curve with this fixed section, viewed as the identity section.

Having fixed this identity section, $\mathcal{X}$ becomes a commutative group scheme over $\operatorname{Spec} \mathcal{O}$, see [31, Theorem 2.1.2]. For simplicity, let us expand K further so that every point of the cuspidal divisor is in the image of some section, i.e. the cuspidal divisor is the disjoint union of finitely many copies of $\operatorname{Spec} \mathcal{O}$. We refer to any such section as a *cusp*.

Theorem 3.2.3 (Manin-Drinfeld [13, 41], special case)**.** *If $\alpha \in \mathcal{X}(\mathcal{O})$ is any cusp, then α has finite order in the group $\mathcal{X}(\mathcal{O})$, i.e. $[\ell]\alpha = e$ for some integer ℓ.*

This theorem was originally stated for the modular curve over $\mathbb{C}$, but one easily reduces to a number field over which the cusps are defined, and properness of $\mathcal{X} \to \mathcal{O}$ implies that it must extend to our situation over $\mathcal{O}$.

Construction 3.2.4. Once and for all, fix a prime $\ell \geq 5$ such that $[\ell]\alpha = \alpha$ for all cusps α. That is, if $[\ell_\alpha]\alpha = e$ by Theorem 3.2.3, apply Dirichlet's theorem on primes in arithmetic progressions and set $\ell \equiv 1 \pmod{\ell_\alpha}$ for each of the finitely many cusps. Then the inverse image of $\mathcal{Y}$ under $\mathcal{X} \xrightarrow{[\ell]} \mathcal{X}$ is an open subscheme $\mathcal{Y}' \subseteq \mathcal{Y}$, because $[\ell]$ preserves the cuspidal divisor.

Write $\mathcal{E}' \to \mathcal{Y}'$ for the pullback of $\mathcal{E} \to \mathcal{Y}$ (see Theorem 3.0.1 for notation) along $\mathcal{Y}' \to \mathcal{Y}$. We study the variation of Galois representations in the family $\mathcal{E}' \to \mathcal{Y}$, which factors as

$$\mathcal{E}' \to \mathcal{Y}' \xrightarrow{[\ell]} \mathcal{Y}.$$

Notation 3.2.5. We retain this notation $\mathcal{E}$, $\mathcal{Y}'$, and $\mathcal{Y}$ from Construction 3.2.4 for the rest of this chapter. We also reserve the notation $E' \to Y' \xrightarrow{[\ell]} Y$ for the base-change of this diagram to K.

Similarly, we reserve X for $\mathcal{X}_K$, where $\mathcal{X}$ is as in Theorem 3.0.1. Taking $\mathcal{E}' \to \mathcal{Y}$ to be the family $\mathcal{X} \to \mathcal{Y}$ of Section 3.1.2, we write Φ_v, Φ_ι, $\mathcal{H}_{K_v}$, $\mathcal{H}_{\mathbb{C}}$, etc. for the period maps and flag varieites discussed in that section.

As is the case with the modified families appearing in [36] (e.g. the modified Legendre family), this modification of the universal elliptic curve gives us better control over a certain centralizer, as we will see in Section 3.3.3.

3.2.2 A few reductions

We enlarge S so that it contains all primes lying above ℓ. We enlarge K so that all points of $\mathcal{X}[\ell]$ are defined over $\mathcal{O}$, in the sense that every point of $\mathcal{X}[\ell]$ is in the image of a section $\operatorname{Spec} \mathcal{O} \to \mathcal{X}$. Indeed, $\mathcal{X}[\ell]$ is finite étale over $\mathcal{O}$ [31, Theorem 2.3.1], so this may be achieved with a finite extension of K.

Let m be the smallest positive integer such that any section $\operatorname{Spec} \mathcal{O} \to \mathcal{X}[\ell^{m+1}]$ factors through $\mathcal{X}[\ell^m]$ (i.e., there is an $\mathcal{O}$-point of exact order ℓ^m but there are no $\mathcal{O}$-points of exact order ℓ^{m+1}). We know m exists because $\mathcal{X}_K(K) = \mathcal{X}(\mathcal{O})$ (by properness) is a finitely generated abelian group, by the Mordell-Weil theorem.

Lemma 3.2.6. *Let*

$$U = \{Q \in \mathcal{Y}(\mathcal{O}) : Q \notin [\ell]\mathcal{X}(\mathcal{O})\}.$$

Then, $\mathcal{Y}(\mathcal{O}) \subseteq U \cup [\ell]U \cup [\ell^2]U \cup \cdots \cup [\ell^m]U$.

Here $[\ell^n]U$ is obtained by multiplying points in U by ℓ^n.

Proof of Lemma 3.2.6. First note that multiplication behaves well with being in $\mathcal{Y}(\mathcal{O})$, in the sense that if $\ell Q' = Q$ for $Q' \in \mathcal{X}(\mathcal{O})$ and $Q \in \mathcal{Y}(\mathcal{O})$ then $Q' \in \mathcal{Y}(\mathcal{O})$. This was esssentially verified in Construction 3.2.4 (whose notation we retain). Indeed, we know Q' must factor through $\mathcal{Y}'$ which is an open subscheme of $\mathcal{Y}$, hence $Q' \in \mathcal{Y}(\mathcal{O})$.

Then, we may take points $Q \in \mathcal{Y}(\mathcal{O})$ and repeatedly divide by ℓ. If $\ell^r Q' = Q$ for $r \leq m$ and $Q' \in U$ then we are done. If we instead find that $\ell^{m+1}Q' = Q$ for some $Q' \in \mathcal{X}(\mathcal{O})$, then we can select $P \in \mathcal{X}(\mathcal{O})$ of exact order ℓ^m so $P \in U$, and take $P + \ell Q' \in U$ with $\ell^m(P + \ell Q') = Q$, i.e. $Q \in \ell^m U$. □

This reduces the proof of Theorem 3.0.2 to showing finiteness of the set U.

Remark 3.2.7. For the remainder of this chapter, we will primarily work over K, i.e. with E', Y', Y, and X. Properness implies $X(K) = \mathcal{X}(\mathcal{O})$, so we will view $Q \in X(K)$ as the same thing as $Q \in \mathcal{X}(\mathcal{O})$ without further comment.

For any point $Q \in U$, we can select $Q' \in X(\overline{K})$ such that $\ell Q' = Q$, and form the extension field $K(Q')$, i.e. the residue field of the point Q'. Since $Q \in U$, we necessarily have $Q' \notin X(K)$, i.e. Q' does not factor through $\operatorname{Spec} K$. Since we have assumed all points of $X[\ell]$ are defined over K, this extension $K(Q')/K$ is Galois and does not depend on the choice of Q', so we set $K(\ell^{-1}Q) = K(Q')$. When unambiguous, we write $L = K(\ell^{-1}Q)$.

We now collect a few useful facts about this extension:

Lemma 3.2.8.

(i) For any fixed $Q \in U$, we have $\operatorname{Gal}(K(\ell^{-1}Q)/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ or $\operatorname{Gal}(K(\ell^{-1}Q)/K) \cong \mathbb{Z}/\ell\mathbb{Z}$.

(ii) Varying over $Q \in U$, there are finitely many isomorphism classes of $K(\ell^{-1}Q)$.

Proof. Galois cohomology yields the exact sequence

$$\begin{array}{ccccc} 0 \longrightarrow & X(K)/\ell X(K) & \xrightarrow{\delta} & \mathrm{H}^1(K, X[\ell]) \cong \operatorname{Hom}(G_K, (\mathbb{Z}/\ell\mathbb{Z})^2) \\ & Q & \longmapsto & (g \mapsto g \cdot Q' - Q') \end{array}$$

since points of $X[\ell]$ are defined over K. Here Q' is any point with $\ell Q' = Q$. Then, $K(\ell^{-1}Q)$ is the fixed field corresponding to $\delta(Q)$, so $\operatorname{Gal}(K(\ell^{-1}Q)/K)$ is a subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^2$. We know $K(\ell^{-1}Q)/K = K(Q')/K$ is a nontrivial extension because $Q \in U$, i.e. Q' cannot be defined over K. This proves part (i). Part (ii) is a standard fact, whose proof we omit. One shows that the extensions $K(\ell^{-1}Q)$ are unramified outside ℓ and the primes dividing the conductor of X, then applies Hermite-Minkowski finiteness which statesthat, for a number field, there are finitely many extensions of a fixed degree unramified outside a finite set of primes (see for example, [46, Chapter III, Theorem 2.13]). $\square$

By Lemma 3.2.8(ii) it suffices to prove finiteness of the set $U_L = \{Q \in U : K(\ell^{-1}Q) \cong L\}$ for a fixed number field L. Having fixed this L, we may apply the Chebotarev density theorem to choose a prime v of K such that

(i) $\begin{cases} v = w & \text{if } \operatorname{Gal}(L/K) \cong \mathbb{Z}/\ell\mathbb{Z} \\ v = w_1 \cdots w_\ell & \text{if } \operatorname{Gal}(L/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \end{cases}$

where w and w_i are primes of L, and the w_i are distinct

(ii) the prime $p > 2$ of $\mathbb{Q}$ below v is unramified in K

(iii) no prime of S lies above p.

For the rest of this chapter, the primes p, v, w, w_i will be as selected above. For notational purposes, we say that w_i are the primes lying over v even if v is inert in L.

Working in one of finitely many residue discs, we have reduced Theorem 3.0.2 to the following proposition, which we prove in the last section.

Proposition 3.2.9. *For fixed $Q_0 \in U_L$, the set $U_{0,L} = \{Q \in U_L : Q \equiv Q_0 \mod v\}$ is finite.*

3.3 The period map and the modified universal elliptic curve

In Sections 3.3.1 and 3.3.2, we prove Lemma 3.3.1 and Lemma 3.3.2 respectively, which will be needed in the proof of Proposition 3.2.9. These lemmas are analogous to Lemma 4.3 and Lemma 4.4 in [36].

The point of Lemma 3.3.1 will be to show that the image under the period mapping of a full residue disc is large. The fiber of a given point $Q \in U_{0,L}$ consists of finitely many closed points $Q' \in Y'(L)$; the proof structure of Proposition 3.2.9 is to show that the points $Q \in U_{0,L}$ giving fixed isomorphism classes of $\rho_{Q'}|G_L$ for Q' in the fiber have small image under the period mapping – Lemma 3.3.2 allows us to conclude that few isomorphism classes are relevant.

3.3.1 Computing monodromy

Lemma 3.3.1. *Write $E'_{\mathbb{C},Q'}$ for the fiber of $E'_{\mathbb{C}} \to Y'_{\mathbb{C}}$ above $Q' \in Y'_{\mathbb{C}}(\mathbb{C})$. There is a subgroup G of $\mathrm{SL}_2(\mathbb{Z})$ whose orbits in $\mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$ are infinite, such that action of monodromy*

$$\pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0) \to \mathrm{Aut}\left(\bigoplus_{\ell Q' = Q_0} H^1_{\mathrm{dR}}(E'_{\mathbb{C},Q'}(\mathbb{C})/\mathbb{C})\right) \simeq \mathrm{GL}_2(\mathbb{C})^{\oplus \ell^2} \tag{3.4}$$

contains $G^{\oplus \ell^2}$, upon choosing an appropriate basis.

By orbits in $\mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$, we mean under the usual action

$$\gamma \cdot (w : z) = (aw + bz : cw + dz) \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } (w : z) \in \mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$$

Proof of Lemma 3.3.1. The computation is essentially the same across different values of N (the level of the modular curve); we illustrate the general principle. We'll depict the following fictional situation in Figure 3.1: the scenario is that $X_1(N)$ has two cusps 0 (the identity in the elliptic curve group law) and α, the cusp α has order two, and also $\ell = 3$ (in spite of our requirement $\ell \geq 5$). No such genus one modular curve exists (for example, $X_1(11)$ has ten cusps), but an accurate diagram with all cusps and all generators would become very crowded. None of these simplifications change the calculation that follows.

The fundamental group of $Y_{\mathbb{C}}(\mathbb{C})$ with basepoint ⧫ is generated by the depicted three loops a, b, c, with lifts as shown. Although the filled in circles are not points of $Y'_{\mathbb{C}}(\mathbb{C})$, our family $E' \to Y'$ was constructed as the fiber over Y' of $E \to Y$. In particular, the monodromy is trivial about all of the black points, as the loops can be homotoped to a constant map on $Y_{\mathbb{C}}(\mathbb{C})$.

Let Q'_0 denote the base-point ⧫ in the middle of the diagram for $Y'_{\mathbb{C}}$. We first describe the full monodromy representation of $\pi_1(Y'_{\mathbb{C}}(\mathbb{C}), Q'_0)$ on $H^1_{\mathrm{dR}}(E'_{\mathbb{C},Q'_0}(\mathbb{C})/\mathbb{C})$. This action may be identified with $\Gamma_1(N)$ – indeed, the filled-in black circles play no role, and we are really computing monodromy in the family $E \to Y$. We know, from the classical theory, that Y has fundamental group $\Gamma_1(N)$, with universal cover the upper half plane (there are no elliptic points when $N \geq 4$), which provides local trivializations of the cohomology group. Any loop in $\pi_1(Y'_{\mathbb{C}}(\mathbb{C}), Q'_0)$ lifts to a path from a point to some $\Gamma_1(N)$ translate; this element of $\Gamma_1(N)$ specifies the action on cohomology.

When $\ell = 3$, every point has $\ell^2 = 9$ pre-images (marked by ⧫ symbols). The loop $c \in \pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0)$ acts trivially on the cohomology of each of the pre-images, except for the one depicted in the center of the diagram (next to the cusp α), which we called Q'_0. Similarly, if $d \in \pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0)$ is a thin loop around the cusp β towards the bottom-left (not depicted), the same holds for $(ab)^{-1}d(ab)$. In an appropriate basis, the action of these two loops on $H^1_{\mathrm{dR}}(E'_{\mathbb{C},Q'_0}(\mathbb{C})/\mathbb{C})$ may be identified with

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \gamma \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \gamma^{-1} \quad \text{for some } \gamma \in \mathrm{SL}_2(\mathbb{Z}) \text{ with } \gamma \cdot (1:0) \neq (1:0), \tag{3.5}$$

and the action is trivial on $H^1_{\mathrm{dR}}(E'_{\mathbb{C},Q'}(\mathbb{C})/\mathbb{C})$ for $Q' \neq Q'_0$ and $\ell Q' = Q_0$, i.e. Q' a different ⧫. Direct computation shows that the subgroup G of $\mathrm{SL}_2(\mathbb{Z})$ generated by the elements listed in Equation (3.5) does not have any finite orbits in $\mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$.

Thus, we see that the monodromy action (i.e. the image in Equation (3.4)) contains $(\gamma, 1, 1, \ldots, 1)$ for any $\gamma \in G$. We may repeat the same construction for all ℓ^2 pre-images (note a and b act tran-

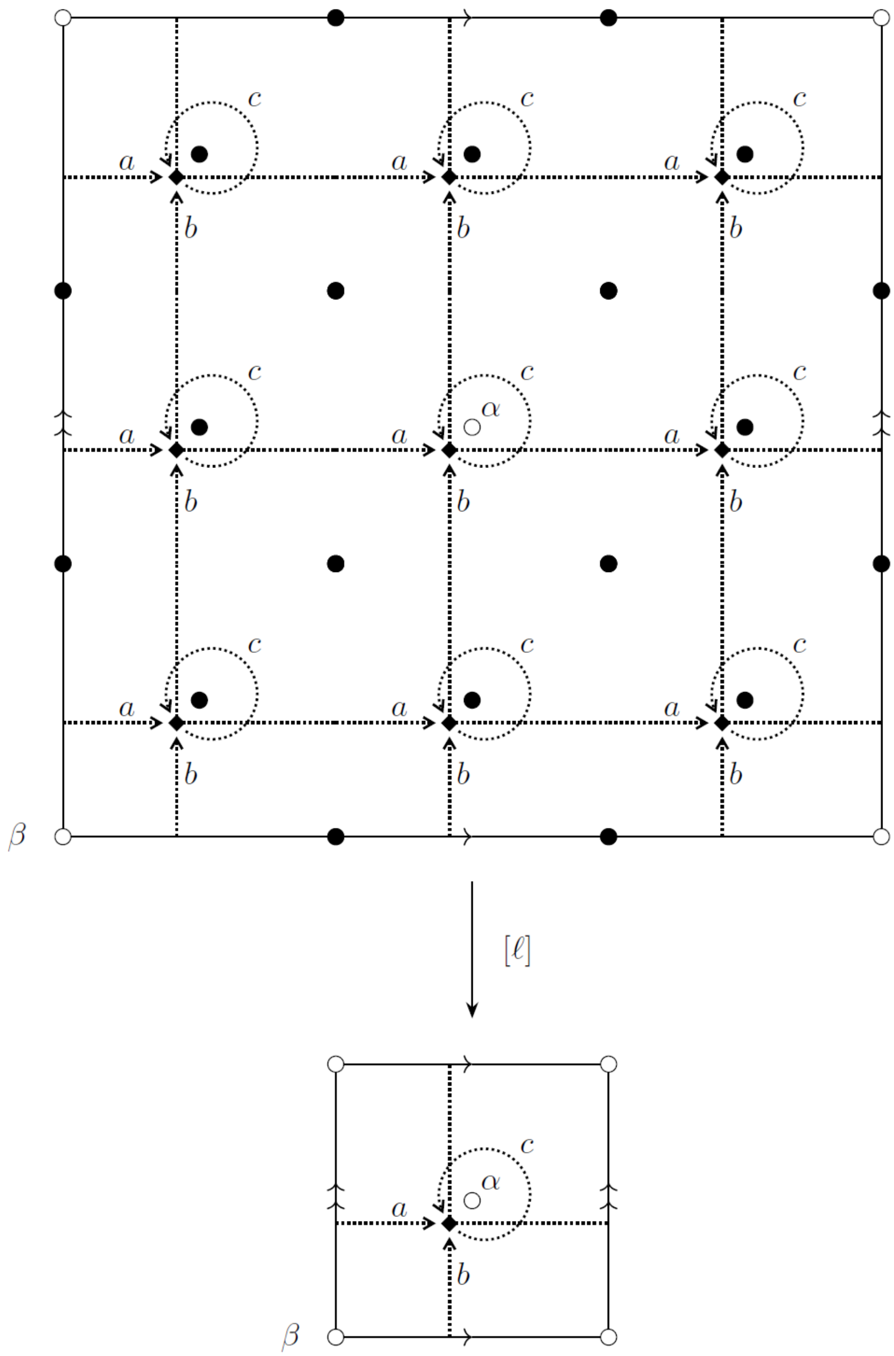

Figure 3.1: Monodromy and $Y'_{\mathbb{C}} \xrightarrow{[\ell]} Y_{\mathbb{C}}$.

sitively on these pre-images), to see that the action contains all elements of the form $(1, \gamma, 1, \ldots, 1)$ for $\gamma \in G$, etc., so the action must contain all of $G^{\oplus \ell^2}$, in some basis. $\square$

3.3.2 Controlling semisimplicity

Lemma 3.3.2. *Let L be a number field, and $p \geq 3$ a rational prime unramified in L. For all but finitely many $Q' \in Y'(L)$ such that $E'_{Q'}$ has good reduction at all primes above p, the Galois representation ρ of G_L on the Tate module $V_p(E'_{Q'})$ (with $\mathbb{Q}_p$-coefficients) is simple.*

Proof of Lemma 3.3.2. We are in the same situation of [36, Lemma 4.4]. For sake of exposition, however, we include and elaborate on their argument.

We need to exclude the existence of a one-dimensional subrepresentation $W \subseteq V_p(E_{Q'})$. The representation of G_L on $V_p(E_{Q'})$ is pure of weight 1 - this restricts to the subrepresentation. By good reduction, the representation $\rho|G_{L_u}$ is crystalline, so we may apply the formula

$$\sum_{u|p} [L_u : \mathbb{Q}_p] a_u(\rho) = \frac{1}{2}[L : \mathbb{Q}]$$

from [36, Lemma 2.10] where $a_u(\rho)$ are the weights of the Hodge filtrations on W_{dR} associated to the local representation $\rho|G_{L_u}$. The space W is one dimensional, so all $a_u(\rho)$ are integers, and in particular, some $a_u(\rho) \geq 1$. Furthermore, functoriality of the relation between representations and filtered ϕ-modules shows that $F^2(W_{\mathrm{dR}}) = 0$. Indeed the filtration on $H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u)$ (associated to the representation on $V_p(E_[Q'])$ is strictly decreasing, so $F^2(H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u)) = 0$. Because W_{dR} is a subobject of $H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u)$ in the category of filtered L_u modules, we find $F^2(W_{\mathrm{dR}}) = 0$. By the same reasoning, we must have $F^1(H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u) = W_{\mathrm{dR}}$.

Since W_{dR} is one dimensional, the Newton and Hodge polygons are equal. We have just shown that the Hodge polygon consists of a slope one line, so we conclude that the slope of the Newton polygon here is one as well. This is also the slope of Frobenius on W_{dR}. By this, we mean $\operatorname{ord}_p(\lambda)/\operatorname{ord}_p(q)$, where λ is the eigenvalue of the L_u-linear map $\mathrm{Frob}_u^{[L_u:\mathbb{Q}_p]}$, and q is the residue degree of the prime u.

For the L_u module $H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u)$, the Hodge polygon consists of a slope zero line followed by a slope one line of length one. Since the Newton and Hodge polygons share a starting and ending point, and we have already seen that Frobenius has slope one on the subrepresentation W_{dR}, its other slope must be zero. This argument shows that $\mathrm{Frob}_u^{[L_u:\mathbb{Q}_p]}$ has distinct eigenvalues, and that W_{dR} is a one dimensional eigenspace of slope one. As remarked following Equation (3.1), the Gauss-Manin connection induces an identification $H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u) \cong H^1_{\mathrm{dR}}(E_{Q'_0,L_u}/L_u)$ in a residue disk that is compatible with the action of ϕ. In particular, it must identify the slope one eigenspace to the slope one eigenspace.

So we conclude that, if $V_p(E_{Q'})$ were reducible, then $F^1(H^1_{\mathrm{dR}}(E_{Q',L_u}/L_u))$ must coincide with a fixed W_{dR} when identified with $H^1_{\mathrm{dR}}(E_{Q'_0,L_u}/L_u)$. But the p-adic period map is analytic and nonconstant, so this can occur at only finitely many points in each residue disk. $\square$

3.3.3 Finiteness of integer points via the period mapping

In this section we prove Proposition 3.2.9, making use of Lemmas 3.3.1 and 3.3.2.

We first discuss how we may reconcile differences between the cases $\mathrm{Gal}(L/K) \cong \mathbb{Z}/\ell\mathbb{Z}$ and $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.

When $\mathrm{Gal}(L/K) \cong \mathbb{Z}/\ell\mathbb{Z}$, the fiber over $Q \in U_{0,L}$ in Y' consists of ℓ distinct points in $Y'(L)$. Each such point consists of ℓ geometric points in the K-scheme Y'. Since v is inert in L, the same holds for Y' replaced with Y'_{K_v}, L replaced with L_w, etc.

When instead $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, the fiber of $Q \in U_{0,L}$ in Y' is a single point of $Y'(L)$, which consists of ℓ^2 geometric points in the K-scheme Y'. However, since v splits as $w_1 \cdots w_\ell$ in L, this is no longer the case if we work over K_v. Indeed, if we denote with some abuse Q for its fiber (a K_v-point) in Y_{K_v}, the fiber over Q in Y'_{K_v} now splits into ℓ points, one in each $Y'(L_{w_i})$.

In either case, when we change to K_v-schemes, the fiber in Y'_{K_v} above Q thus consists of ℓ points, each defined over a degree ℓ extension of K_v. So that we may consider the two cases simultaneously, we'll denote these ℓ points Q'_i, and say that they are defined over L_{w_i}. Which these are will depend on $\mathrm{Gal}(L/K)$; that is, when $\mathrm{Gal}(L/K) \cong \mathbb{Z}/\ell\mathbb{Z}$ we have that all ℓ copies of w_i and L_i are equal, while the the w_i are different when $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.

In what follows, we use $\rho_{Q'_i}$ to denote the representations of $G_{L_{w_i}}$ on $H^1_{\mathrm{et}}\left(E'_{K_v,Q'_i} \times_{L_{w_i}} \overline{L_{w_i}}, \mathbb{Q}_p\right)$ and ρ_Q for the represenation of G_{K_v} on $H^1(E'_{K_v,Q} \times_{K_v} \overline{K_v}, \mathbb{Q}_p)$. We also fix notation for the ℓ-tuple

$$\rho' := (\rho_{Q'_1}|G_{L_{w_1}}, \ldots, \rho_{Q'_\ell}|G_{L_{w_\ell}}).$$

Sometimes, we write $\rho_Q|G_{K_v}$, for example, to emphasize that this is a G_{K_v}-representation.

Next, we describe crucial additional structure on $D_{\mathrm{cris}}(\rho_Q)$ that arises from our modified family $E' \to Y' \to Y$.

Proposition 3.3.3. *There is a natural identification*

$$\bigoplus_{i=1}^{\ell} D_{\mathrm{cris}}(\rho_{Q_i'}|G_{L_w}) =$$

$$\bigoplus_{i=1}^{\ell}(H^1_{\mathrm{dR}}(E'_{L_{w_i},Q_i'}/L_{w_i}), \phi_i, \textit{Hodge filtration}) \xrightarrow{\textit{forget}} (H^1_{\mathrm{dR}}\left(E'_{K_v,Q}/K_v\right), \phi, \textit{Hodge filtration})$$

$$= D_{\mathrm{cris}}(\rho_Q).$$

Proof. The fiber $E'_{K_v,Q}$ is the disjoint union over the fibers $E'_{K_v,Q_i'}$. These are L_{w_i}-schemes, but become K_v-schemes upon the naive restriction $L_{w_i} \to K_v$. Thus, we may apply Lemma 3.1.2 and Proposition 3.1.3 to conclude that

$$\rho_Q|G_{K_v} \cong \bigoplus_{i=1}^{\ell} \mathrm{Ind}_{G_{L_w}}^{G_{K_v}} \rho_{Q_i'}|G_{L_{w_i}}.$$

Since S contains no primes above p, $E'_{K_v,Q_i'}$ has good reduction, which implies that the representations $\rho_{Q'}|G_{L_w}$ are crystalline. (See diagram of Proposition 3.1.3 and the citations in its proof.)

Then, the fully faithful functor $D_{\mathrm{cris}}(-)$ combined with the crystalline comparison theorem of Faltings [18] gives a correspondence between the isomorphism class of ρ' to the isomorphism class of

$$\bigoplus_{i=1}^{\ell}(H^1_{\mathrm{dR}}(E'_{L_{w_i},Q_i'}/L_{w_i}), \phi_i, \text{Hodge filtration}).$$

in $\bigoplus_{i=1}^{\ell} \mathrm{MF}^{\phi}_{L_{w_i}}$. With some abuse of notation, we'll denote this $D_{\mathrm{cris}}(\rho')$.

On account of Proposition 3.1.3, we see that upon forgetting all the L_{w_i}-linear structure of this object, we must recover the filtered F-isocrystal $(H^1_{\mathrm{dR}}\left(E'_{K_v,Q}/K_v\right), \phi, \text{Hodge filtration})$ associated to $\rho_Q|G_{K_v}$. □

Next, we turn towards the period map. Typically, one wishes to identify $H^*_{\mathrm{dR}}(E'_{Q,K_v}/K_v)$ with $H^*_{\mathrm{dR}}(E'_{Q_0,K_v}/K_v)$ in a residue disc (i.e. $Q \in U_{0,L}$), then study the variation of Hodge filtrations in the residue disc as flags of $H^*_{\mathrm{dR}}(E'_{Q_0,K_v}/K_v)$. To make use of the L_{w_i}-linear structure described in Proposition 3.3.3, we should make sure that it is compatible with the Gauss-Manin identification.

Lemma 3.3.4. *The Gauss-Manin identification of $H^1_{\mathrm{dR}}(E'_{Q,K_v}/K_v)$ with $H^1_{\mathrm{dR}}(E'_{Q_0,K_v}/K_v)$ in a residue disc preserves the decomposition L_{w_i}-linear decomposition of Proposition 3.3.3.*

Proof. Indeed, the $\bigoplus_{i=1}^{\ell} L_{w_i}$ linear structure we have just described on $D_{\mathrm{cris}}(\rho_Q)$ also comes naturally from $H^0_{\mathrm{dR}}(E'_{Q,K_v}/K_v)$ and the cup product. Indeed, we have $Y'_{K_v,Q} \cong \bigoplus_{i=1}^{\ell} L_{w_i}$ and the natural morphism

$$\bigoplus_{i=1}^{\ell} L_{w_i} \cong H^0_{\mathrm{dR}}(Y'_{K_v,Q}/K_v) \to H^0_{\mathrm{dR}}(E'_{K_v,Q}/K_v)$$

compatible with $L_{w_i} \cong H^0_{\mathrm{dR}}(Q'_i/K_v) \to H^0_{\mathrm{dR}}(E'_{K_v,Q}/K_v)$. The cup product action then recovers the L_{w_i} structure of each $H^1_{\mathrm{dR}}(E'_{L_{w_i},Q'_i}/L_{w_i})$. The lemma then follows from naturality of the Gauss-Manin connection with the cup product. $\square$

In analogy with the work in [36], the purpose of using the family $E' \to Y' \to Y$ instead of $E \to Y$ is precisely to use the extra structure provided by Proposition 3.3.3 and Lemma 3.3.4. Isomorphism classes in $\bigoplus_{i=1}^{\ell} \mathrm{MF}^{\phi}_{L_{w_i}}$ are smaller than those in $\mathrm{MF}^{\phi}_{K_v}$, which will be useful or us. We first reduce to the case of a fixed isomorphism class using Lemma 3.3.2, then bound the size of a fixed isomorphism class.

Lemma 3.3.5. *There are many finitely possibilities for ρ' up to isomorphism. In particular, to prove Proposition 3.2.9, we may assume ρ' lies in a fixed isomorphism class.*

Proof. For $Q \in U_{0,L}$, the fiber E'_Q has good reduction away from primes in S. If $Q' \in Y'(L)$ is in the fiber over Q, then the G_L representation $\rho_{Q'}$ on $H^1_{\mathrm{et}}\left(E'_{Q'} \times_L \overline{L}, \mathbb{Q}_p\right) = V_p(E'_{Q'})$ is unramified away from primes above S or above p. Furthermore, this representation is pure of weight one, i.e. for primes $\mathfrak{p}$ not above S or p, the eigenvalues of Frobenius for $\mathfrak{p}$ are algebraic with complex absolute value $q_{\mathfrak{p}}^{1/2}$, where $q_{\mathfrak{p}}$ is the size of the residue field of $\mathfrak{p}$. See [12, Lemma 1.7] for a general statement.

Applying Lemma 3.3.2 shows that we may assume the representations $\rho_{P'}|G_L$ are semisimple.

A result of Faltings implies that, up to isomorphism, there are finitely many semisimple representations $G_L \to \mathrm{GL}_d(\mathbb{Q}_p)$ for fixed d, unramified outside a fixed finite set, and pure of a fixed weight. See [16] and the statement of [36, Lemma 2.3]. This applies for our representations $\rho_{Q'_i}|G_L$, so further restricting to local Galois representations and applying Lemma 3.1.1, we may assume ρ' lies in a fixed isomorphism class. $\square$

We will use a linear algebra lemma [36, Lemma 2.1], which we record here for completeness and whose proof we omit.

Lemma 3.3.6. *Let E be a field and $\sigma\colon E \to E$ an automorphism of finite order e with fixed field F. Let V be a dimension d vector space over E and $\phi\colon V \to V$ be a σ-semilinear automorphism.*

Write $Z_{\mathrm{end}}(\phi)$ for

$$Z_{\mathrm{end}}(\phi) = \{f\colon V \to V \text{ an } E\text{-linear map}, f \circ \phi = \phi \circ f\},$$

which is an F vector space. Note $\dim_E Z_{\mathrm{end}}(\phi^e)$ is an E vector space. Then $\dim_F Z_{\mathrm{end}}(\phi) = \dim_E Z_{\mathrm{end}}(\phi^e)$. In particular $\dim_F Z_{\mathrm{end}}(\phi) \leq (\dim_E V)^2$.

Proposition 3.3.7. *There is a subgroup $Z(\phi^{[K_v:\mathbb{Q}_p]})$ of $\mathrm{GL}(H^1_{\mathrm{dR}}(E'_{K_v,Q}/K_v))$ (described in the proof) whose Zariski closure has dimension at most 4ℓ, such that*

$$\Phi_v^{-1}(Z(\phi^{[K_v:\mathbb{Q}_p]}) \cdot h^v) \supseteq \{\Phi_v(Q) : Q \in U_{0,L} \text{ such that } \rho' \text{ lies in fixed isomorphism class }\}$$

for an appropriate $h^v \in \mathcal{H}_{K_v}$.

Proof. Objects isomorphic to $D_{\mathrm{cris}}(\rho')$ in $\bigoplus_{i=1}^{\ell} \mathrm{MF}^{\phi}_{L_{w_i}}$ must differ by an automorphism in

$$Z(\phi) := \bigoplus_{i=1}^{\ell} Z_i(\phi_i) \quad \text{where} \quad Z_i(\phi_i) = \text{ centralizer of } \phi_i \text{ in } \mathrm{Aut}_{L_{w_i}} H^1_{\mathrm{dR}}(E'_{L_{w_i},Q'_i}/L_{w_i}).$$

Note $Z_i(\phi_i)$ is contained in $Z_i(\phi_i^{[K_v:\mathbb{Q}_p]})$, so we'll work with this latter group instead. Since $\phi^{[K_v:\mathbb{Q}_p]}$ is now K_v-linear, we may speak of the dimension of $Z_{i,\mathrm{end}}(\phi_i^{[K_v:\mathbb{Q}_p]})$ as a K_v vector space, and apply Lemma 3.3.6 with $E/F = L_{w_i}/K_v$ to see that

$$\dim_{K_v} Z_{i,\mathrm{end}}(\phi_i^{[K_v:\mathbb{Q}_p]}) \leq (\dim_{L_{w_i}} H^1_{\mathrm{dR}}(E'_{L_{w_i},Q'_i}/L_{w_i}))^2 = 4.$$

Since $Z_{i,\mathrm{end}}(\phi_i^{[K_v:\mathbb{Q}_p]})$ certainly contains $Z_i(\phi_i^{[K_v:\mathbb{Q}_p]})$, we conclude that the Zariski closure of $Z_i(\phi_i^{[K_v:\mathbb{Q}_p]})$ as a subgroup of $\mathrm{Aut}_{K_v} H^1_{\mathrm{dR}}(E'_{L_{w_i},Q'_i}/L_{w_i})$ has dimension at most 4. This is as an algebraic group; we are indeed working in an ambient space of K_v-linear automorphisms, after forgetting L_{w_i}-structure.

The previous computation thus shows that the Zariski closure of $Z(\phi^{[K_v:\mathbb{Q}_p]})$ has dimension at most $\bigoplus_{i=1}^{\ell} \dim_{K_v} Z_i(\phi^{[K_v:\mathbb{Q}_p]}) = 4\ell$, as claimed. □

With the use of Lemma 3.3.1, let us now show that $\Phi_v(\Omega_v)$ is larger in comparison.

Proposition 3.3.8. *Let $h^\iota \in \mathcal{H}_{\mathbb{C}}(\mathbb{C})$ be arbitrary. Then $\overline{\pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0) \cdot h^\iota} = \mathcal{H}_{\mathbb{C}}$, where the left-hand side denotes Zariski closure of a π_1-orbit. In particular, $\dim \overline{\pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0) \cdot h^\iota} = \ell^2$.*

Proof. The fiber Y'_Q splits into ℓ^2 geometric components, so $H^1_{\mathrm{dR}}(E'_{Q_0}/K)$ splits as

$$H^1_{\mathrm{dR}}(E'_{Q_0}/K) \otimes_K \mathbb{C} \cong \bigoplus H^1_{\mathrm{dR}}(E'_{Q'_i}/L) \otimes_K \mathbb{C}$$

where the Q'_i are the preimages of Q_0 in $Y'(L)$ (how many pre-images there are depends on $\mathrm{Gal}(L/K)$ as discussed at the beginning of this proof). The period map and Hodge filtration similarly split, so that

$$\mathcal{H}_{\mathbb{C}} = \bigoplus_{i=1}^{\ell^2} \mathbb{P}^1_{\mathbb{C}}.$$

By Lemma 3.3.1, there is a group G such that the G-orbit of any point in $\mathbb{P}^1_{\mathbb{C}}(\mathbb{C})$ is infinite, i.e. dense, and such that the action of $\pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0)$ contains $\prod_{i=1}^{\ell^2}$. So we conclude $\overline{\pi_1(Y_{\mathbb{C}}(\mathbb{C}), Q_0) \cdot h^{\iota}} = \mathcal{H}_{\mathbb{C}}$ as claimed, and $\mathcal{H}_{\mathbb{C}}$ indeed has dimension ℓ^2. $\square$

Proof of Proposition 3.2.9. Directly apply Lemma 3.3.5, Proposition 3.3.7, Proposition 3.3.8, and Corollary 3.1.5. We have $4\ell < \ell^2$ because we constructed $\ell \geq 5$. $\square$

References

[1] Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius Van de Ven, *Compact complex surfaces*, second ed., 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], vol. 4, Springer-Verlag, Berlin, 2004. MR 2030225

[2] Pierre Berthelot, *Cohomologie cristalline des schémas de caractéristique* $p > 0$, Lecture Notes in Mathematics, Vol. 407, Springer-Verlag, Berlin-New York, 1974. MR 0384804

[3] Pierre Berthelot and Arthur Ogus, *Notes on crystalline cohomology*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978. MR 0491705

[4] Christophe Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) **152** (2000), no. 2, 489–549. MR 1804530

[5] Oliver Brinnon and Brian Conrad, *Cmi summer school notes on p-adic hodge theory*, http://math.stanford.edu/ conrad/papers/notes.pdf, 2009.

[6] Pierre Colmez and Jean-Marc Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), no. 1, 1–43. MR 1779803

[7] Pietro Corvaja, Aaron Levin, and Umberto Zannier, *Integral points on threefolds and other varieties*, Tohoku Math. J. (2) **61** (2009), no. 4, 589–601. MR 2598251

[8] Pietro Corvaja and Umberto Zannier, *A subspace theorem approach to integral points on curves*, C. R. Math. Acad. Sci. Paris **334** (2002), no. 4, 267–271. MR 1891001

[9] P. Deligne, *Théorèmes de finitude en cohomologie ℓ-adique*, Cohomologie étale, Lecture Notes in Math., vol. 569, Springer, Berlin, 1977, Séminaire de Géométrie Algébrique du Bois-Marie (SGA 4.5), pp. 233–261. MR 3727439

[10] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 36, 75–109. MR 0262240

[11] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR 0337993

[12] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. MR 0340258

[13] V. G. Drinfeld, *Two theorems on modular curves*, Funkcional. Anal. i Priložen. **7** (1973), no. 2, 83–84. MR 0318157

[14] David Eisenbud and Joe Harris, *The geometry of schemes*, Graduate Texts in Mathematics, vol. 197, Springer-Verlag, New York, 2000. MR 1730819

[15] ———, *3264 and all that—a second course in algebraic geometry*, Cambridge University Press, Cambridge, 2016. MR 3617981

[16] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935

[17] ———, *A new application of Diophantine approximations*, A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press, Cambridge, 2002, pp. 231–246. MR 1975455

[18] Gerd Faltings, *Crystalline cohomology and p-adic Galois-representations*, Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988), Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 25–80. MR 1463696

[19] ———, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), no. 3, 549–576. MR 1109353

[20] Gerd Fischer, *Plane algebraic curves*, Student Mathematical Library, vol. 15, American Mathematical Society, Providence, RI, 2001, Translated from the 1994 German original by Leslie Kay. MR 1836037

[21] Jean-Marc Fontaine, *Sur certains types de représentations p-adiques de groupe de galois d'un corps local; construction d'un anneau de barsotti-tate*, Annals of Math. **115** (1982), no. 3, 529–577.

[22] Darij Grinberg and Victor Reiner, *Hopf algebras in combinatorics*, Online notes, https://arxiv.org/abs/1409.8356, 2014.

[23] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28, 255. MR 0217086

[24] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361. MR 0238860

[25] Alexander Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. MR 0354656

[26] Gary Harris and Clyde Martin, *The roots of a polynomial vary continuously as a function of the coefficients*, Proc. Amer. Math. Soc. **100** (1987), no. 2, 390–392. MR 884486

[27] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[28] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction. MR 1745599

[29] Naonori Ishii, *Remarks on d-gonal curves*, Tsukuba J. Math. **19** (1995), no. 2, 329–345. MR 1366638

[30] Lena Ji, Li Shizhang, Patrick McFaddin, Drew Moore, and Matthew Stevenson, *Weil restriction for schemes and beyond*, Online notes, http://www-personal.umich.edu/˜stevmatt, 2017.

[31] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR 772569

[32] Mark Kisin, *Crystalline representations and F-crystals*, Algebraic geometry and number theory, Progr. Math., vol. 253, Birkhäuser Boston, Boston, MA, 2006, pp. 459–496. MR 2263197

[33] Finn F. Knudsen, *The projectivity of the moduli space of stable curves. II. The stacks $M_{g,n}$*, Math. Scand. **52** (1983), no. 2, 161–199. MR 702953

[34] ———, *The projectivity of the moduli space of stable curves. III. The line bundles on $M_{g,n}$, and a proof of the projectivity of $\overline{M}_{g,n}$ in characteristic* 0, Math. Scand. **52** (1983), no. 2, 200–212. MR 702954

[35] Finn Faye Knudsen and David Mumford, *The projectivity of the moduli space of stable curves. I. Preliminaries on "det" and "Div"*, Math. Scand. **39** (1976), no. 1, 19–55. MR 0437541

[36] Brian Lawrence and Akshay Venkatesh, *Diophantine problems and p-adic period mappings*, preprint, https://arxiv.org/abs/1807.02721, 2018.

[37] Robert Lazarsfeld, *Positivity in algebraic geometry. I*, 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], vol. 48, Springer-Verlag, Berlin, 2004, Classical setting: line bundles and linear series. MR 2095471

[38] Aaron Levin, *Generalizations of Siegel's and Picard's theorems*, Ann. of Math. (2) **170** (2009), no. 2, 609–655. MR 2552103

[39] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232

[40] Saunders Mack-Crane, *Weil restriction and base change*, Online notes, https://algebrateahousejmath.wordpress.com/2017/02/28/weil-restriction-and-base-change/, 2017.

[41] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. MR 0314846

[42] J.S. Milne, *Lectures on Étale cohomology (v2.21)*, Online notes, https://www.jmilne.org/math/CourseNotes/LEC.pdf, 2013.

[43] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994. MR 1304906

[44] David Mumford, *Stability of projective varieties*, Enseignement Math. (2) **23** (1977), no. 1-2, 39–110. MR 0450272

[45] Makoto Namba, *Families of meromorphic functions on compact Riemann surfaces*, Lecture Notes in Mathematics, vol. 767, Springer, Berlin, 1979. MR 555241

[46] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999,

Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859

[47] A. N. Paršin, *Algebraic curves over function fields*, Dokl. Akad. Nauk SSSR **183** (1968), 524–526. MR 0236180

[48] Igor R. Shafarevich, *Basic algebraic geometry. 1*, third ed., Springer, Heidelberg, 2013, Varieties in projective space. MR 3100243

[49] Goro Shimura, *Reduction of algebraic varieties with respect to a discrete valuation of the basic field*, Amer. J. Math. **77** (1955), 134–176. MR 0066687

[50] Carl L. Siegel, *Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]*, On some applications of Diophantine approximations, Quad./Monogr., vol. 2, Ed. Norm., Pisa, 2014, pp. 81–138. MR 3330350

[51] The Stacks project authors, *The stacks project*, https://stacks.math.columbia.edu, 2019.

[52] Ashvin Swaminathan, *Inflection points in families of algebraic curves*, http://www.math.harvard.edu/theses/senior/swaminathan/swaminathan.pdf, 2017, Undergraduate thesis, Harvard College.

[53] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 8.7)*, 2019, `http://www.sagemath.org`.

[54] Paul Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239, Springer-Verlag, Berlin, 1987. MR 883451

[55] ______, *Integral points on subvarieties of semiabelian varieties. II*, Amer. J. Math. **121** (1999), no. 2, 283–313. MR 1680329

[56] I. R. Šafarevič, *Algebraic number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 163–176. MR 0202709

[57] Robert J. Walker, *Algebraic curves*, Springer-Verlag, New York-Heidelberg, 1978, Reprint of the 1950 edition. MR 513824

[58] André Weil, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser, Boston, Mass., 1982, With appendices by M. Demazure and Takashi Ono. MR 670072

[59] Umberto Zannier, *On the integral points on the complement of ramification-divisors*, J. Inst. Math. Jussieu **4** (2005), no. 2, 317–330. MR 2135140