# $J_1(p)$ Has Connected Fibers

Brian Conrad, Bas Edixhoven, William Stein

Received: November 23, 2002

Communicated by Stephen Lichtenbaum

Abstract. We study resolution of tame cyclic quotient singularities on arithmetic surfaces, and use it to prove that for any subgroup $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ the map $X_H(p) = X_1(p)/H \to X_0(p)$ induces an injection $\Phi(J_H(p)) \to \Phi(J_0(p))$ on mod $p$ component groups, with image equal to that of $H$ in $\Phi(J_0(p))$ when the latter is viewed as a quotient of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$. In particular, $\Phi(J_H(p))$ is always Eisenstein in the sense of Mazur and Ribet, and $\Phi(J_1(p))$ is trivial: that is, $J_1(p)$ has connected fibers. We also compute tables of arithmetic invariants of optimal quotients of $J_1(p)$.

2000 Mathematics Subject Classification: 11F11, 11Y40, 14H40
Keywords and Phrases: Jacobians of modular curves, Component groups, Resolution of singularities

Contents

## 1 INTRODUCTION

Let $p$ be a prime and let $X_1(p)_{/\mathbf{Q}}$ be the projective smooth algebraic curve over $\mathbf{Q}$ that classifies elliptic curves equipped with a point of exact order $p$. Let $J_1(p)_{/\mathbf{Q}}$ be its Jacobian. One of the goals of this paper is to prove:

THEOREM 1.1.1. *For every prime p, the Néron model of* $J_1(p)_{/\mathbf{Q}}$ *over* $\mathbf{Z}_{(p)}$ *has closed fiber with trivial geometric component group.*

This theorem is obvious when $X_1(p)$ has genus 0 (*i.e.*, for $p \leq 7$), and for $p = 11$ it is equivalent to the well-known fact that the elliptic curve $X_1(11)$ has $j$-invariant with a simple pole at 11 (the $j$-invariant is $-2^{12}/11$). The strategy of the proof in the general case is to show that $X_1(p)_{/\mathbf{Q}}$ has a regular proper model $\mathcal{X}_1(p)_{/\mathbf{Z}_{(p)}}$ whose closed fiber is geometrically integral. Once we have such a model, by using the well-known dictionary relating the Néron model of a generic-fiber Jacobian with the relative Picard scheme of a regular proper model (see [9, Ch. 9], esp. [9, 9.5/4, 9.6/1], and the references therein), it follows that the Néron model of $J_1(p)$ over $\mathbf{Z}_{(p)}$ has (geometrically) connected closed fiber, as desired. The main work is therefore to prove the following theorem:

Theorem 1.1.2. *Let $p$ be a prime. There is a regular proper model $\mathcal{X}_1(p)$ of $X_1(p)_{/\mathbf{Q}}$ over $\mathbf{Z}_{(p)}$ with geometrically integral closed fiber.*

What we really prove is that if $X_1(p)^{\mathrm{reg}}$ denotes the minimal regular resolution of the normal (typically non-regular) coarse moduli scheme $X_1(p)_{/\mathbf{Z}_{(p)}}$, then a minimal regular contraction $\mathcal{X}_1(p)$ of $X_1(p)^{\mathrm{reg}}$ has geometrically integral closed fiber; after all the contractions of $-1$-curves are done, the component that remains corresponds to the component of $X_1(p)_{/\mathbf{F}_p}$ classifying étale order-$p$ subgroups. When $p > 7$, so the generic fiber has positive genus, such a minimal regular contraction is the unique minimal regular proper model of $X_1(p)_{/\mathbf{Q}}$.

Theorem 1.1.2 provides natural examples of a finite map $\pi$ between curves of arbitrarily large genus such that $\pi$ does not extend to a morphism of the minimal regular proper models. Indeed, consider the natural map

$$\pi : X_1(p)_{/\mathbf{Q}} \to X_0(p)_{/\mathbf{Q}}.$$

When $p = 11$ or $p > 13$, the target has minimal regular proper model over $\mathbf{Z}_{(p)}$ with reducible geometric closed fiber [45, Appendix], while the source has minimal regular proper model with (geometrically) integral closed fiber, by Theorem 1.1.2. If the map extended, it would be proper and dominant (as source and target have unique generic points), and hence surjective. On the level of closed fibers, there cannot be a surjection from an irreducible scheme onto a reducible scheme. By the valuative criterion for properness, $\pi$ is defined in codimension 1 on minimal regular proper models, so there are finitely many points of $\mathcal{X}_1(p)$ in codimension 2 where $\pi$ cannot be defined.

Note that the fiber of $J_1(p)$ at infinity need not be connected. More specifically, a modular-symbols computation shows that the component group of $J_1(p)(\mathbf{R})$ has order 2 for $p = 17$ and $p = 41$. In contrast, A. Agashe has observed that [47, §1.3] implies that $J_0(p)(\mathbf{R})$ is always connected.

Rather than prove Theorem 1.1.2 directly, we work out the minimal regular model for $X_H(p)$ over $\mathbf{Z}_{(p)}$ for any subgroup $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ and use this to study the mod $p$ component group of the Jacobian $J_H(p)$; note that $J_H(p)$ usually does not have semistable reduction. Our basic method is to use a variant on the classical Jung–Hirzebruch method for complex surfaces, adapted to the case of a proper curve over an arbitrary discrete valuation ring. We refer the reader to Theorem 2.4.1 for the main result in this direction; this is the main new theoretical contribution of the paper. This technique will be applied to prove:

Theorem 1.1.3. *For any prime $p$ and any subgroup $H$ of $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$, the natural surjective map $J_H(p) \to J_0(p)$ of Albanese functoriality induces an injection on geometric component groups of mod-$p$ fibers, with the component* *group* $\Phi(\mathcal{J}_H(p)_{/\overline{\mathbf{F}}_p})$ *being cyclic of order* $|H|/\gcd(|H|,6)$*. In particular, the finite étale component-group scheme* $\Phi(\mathcal{J}_H(p)_{/\mathbf{F}_p})$ *is constant over* $\mathbf{F}_p$*.*

*If we view the constant cyclic component group* $\Phi(\mathcal{J}_0(p)_{/\mathbf{F}_p})$ *as a quotient of the cyclic* $(\mathbf{Z}/p)^\times/\{\pm 1\}$*, then the image of the subgroup* $\Phi(\mathcal{J}_H(p)_{/\mathbf{F}_p})$ *in this quotient is the image of* $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ *in this quotient.*

*Remark* 1.1.4. The non-canonical nature of presenting one finite cyclic group as a quotient of another is harmless when following images of subgroups under maps, so the final part of Theorem 1.1.3 is well-posed.

The constancy in Theorem 1.1.3 follows from the injectivity claim and the fact that $\Phi(\mathcal{J}_0(p)_{/\mathbf{F}_p})$ is constant. Such constancy was proved by Mazur-Rapoport [45, Appendix], where it is also shown that this component group for $J_0(p)$ is cyclic of the order indicated in Theorem 1.1.3 for $H = (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$.

Since the Albanese map is compatible with the natural map $\mathbf{T}_H(p) \to \mathbf{T}_0(p)$ on Hecke rings and Mazur proved [45, §11] that $\Phi(\mathcal{J}_0(p)_{/\overline{\mathbf{F}}_p})$ is Eisenstein as a $\mathbf{T}_0(p)$-module, we obtain:

Corollary 1.1.5. *The Hecke module* $\Phi(\mathcal{J}_H(p)_{/\overline{\mathbf{F}}_p})$ *is Eisenstein as a* $\mathbf{T}_H(p)$*-module* (i.e., $T_\ell$ *acts as* $1+\ell$ *for all* $\ell \neq p$ *and* $\langle d\rangle$ *acts trivially for all* $d \in (\mathbf{Z}/p\mathbf{Z})^\times$*).*

In view of Eisenstein results for component groups due to Edixhoven [18] and Ribet [54], [55] (where Ribet gives examples of non-Eisenstein component groups), it would be of interest to explore the range of validity of Corollary 1.1.5 when auxiliary prime-to-$p$ level structure of $\Gamma_0(N)$-type is allowed. A modification of the methods we use should be able to settle this more general problem. In fact, a natural approach would be to aim to essentially reduce to the Eisenstein results in [54] by establishing a variant of the above injectivity result on component groups when additional $\Gamma_0(N)$ level structure is allowed away from $p$. This would require a new idea in order to avoid the crutch of cyclicity (the case of $\Gamma_1(N)$ seems much easier to treat using our methods because the relevant groups tend to be cyclic, though we have not worked out the details for $N > 1$), and preliminary calculations of divisibility among orders of component groups are consistent with such injectivity.

In order to prove Theorem 1.1.3, we actually first prove a surjectivity result:

Theorem 1.1.6. *The map of Picard functoriality* $J_0(p) \to J_H(p)$ *induces a surjection on mod* $p$ *component groups, with the mod* $p$ *component group for* $J_H(p)$ *having order* $|H|/\gcd(|H|,6)$*.*

*In particular, each connected component of* $\mathcal{J}_H(p)_{/\mathbf{F}_p}$ *contains a multiple of the image of* $(0)-(\infty) \in \mathcal{J}_0(p)(\mathbf{Z}_{(p)})$ *in* $\mathcal{J}_H(p)(\mathbf{F}_p)$*.*

Let us explain how to deduce Theorem 1.1.3 from Theorem 1.1.6. Recall [28, Exposé IX] that for a discrete valuation ring $R$ with fraction field $K$ and an abelian variety $A$ over $K$ over $R$, Grothendieck's biextension pairing sets up a bilinear pairing between the component groups of the closed fibers of the Néron models of $A$ and its dual $A'$. Moreover, under this pairing the component-group map induced by a morphism $f : A \to B$ (to another abelian variety) has as an adjoint the component-group map induced by the dual morphism $f' : B' \to A'$. Since Albanese and Picard functoriality maps on Jacobians are dual to each other, the surjectivity of the Picard map therefore implies the injectivity of the Albanese map provided that the biextension pairings in question are perfect pairings (and then the description of the image of the resulting Albanese injection in terms of $H$ as in Theorem 1.1.3 follows immediately from the order calculation in Theorem 1.1.6).

In general the biextension pairing for an abelian variety and its dual need not be perfect [8], but once it is known to be perfect for the $J_H(p)$'s then surjectivity of the Picard map in Theorem 1.1.6 implies the injectivity of the Albanese map as required in Theorem 1.1.3. To establish the desired perfectness, one can use either that the biextension pairing is always perfect in case of generic characteristic 0 with a perfect residue field [6, Thm. 8.3.3], or that surjectivity of the Picard map ensures that $J_H(p)$ has mod $p$ component group of order prime to $p$, and the biextension pairing is always perfect on primary components prime to the residue characteristic [7, §3, Thm. 7].

It is probable that the results concerning the component groups $\Phi(\mathcal{J}_H(p)_{/\overline{\mathbf{F}}_p})$ and the maps between them that are proved in this article via models of $X_H(p)$ over $\mathbf{Z}_{(p)}$ can also be proved using [20, 5.4, Rem. 1], and the well-known stable model of $X_1(p)$ over $\mathbf{Z}_{(p)}[\zeta_p]$ that one can find for example in [30]. (This observation was prompted by questions of Robert Coleman.) However, such an approach does not give information on regular models of $X_H(p)$ over $\mathbf{Z}_{(p)}$. Hence we prefer the method of this paper.

Acknowledgements. This paper was inspired by the following question of Shuzo Takehashi: "What can be said about component groups of optimal quotients of $J_1(p)$?". Edixhoven was partially supported by the European Research Training Network Contract HPRN-CT-2000-00120 "arithmetic algebraic geometry", while Conrad and Stein are grateful to the NSF for support during work on this paper. Conrad is also grateful to the Sloan Foundation for support and to Henri Darmon, Paul Hacking, and Victor Kac. Dino Lorenzini made a large number of helpful remarks. Stein thanks Ken Ribet and Sheldon Kamienny for discussions about the torsion subgroup of $J_1(p)$, Allan Steel of Magma for computational support, and William R. Hearst III and Sun Microsystems for donating computers that were used for computations in this paper. The authors thank the referee for a thoughtful report.

## 1.2 Outline

Section 1.3 contains a few background notational remarks. In Section 2 we develop the basic Jung–Hirzebruch resolution technique in the context of tame cyclic quotient surface singularities. This includes mod-$p$ singularities on many (coarse) modular curves when $p > 3$ and the $p$-power level structure is only on $p$-torsion. In Section 3, we recall some general results on moduli problems for elliptic curves and coarse moduli schemes for such problems. In Section 4, we use the results of Sections 2 and 3 to locate all the non-regular points on the coarse moduli scheme $X_H(p)_{/\mathbf{Z}_{(p)}}$ (*e.g.*, when $H$ is trivial this is the set of $\mathbf{F}_p$-rational points $(E, 0)$ with $j = 0, 1728$). In Section 5, we use the Jung–Hirzebruch formulas to compute the minimal regular resolution $X_H(p)^{\mathrm{reg}}$ of $X_H(p)_{/\mathbf{Z}_{(p)}}$, and we use use a series of intersection number computations to obtain a regular proper model for $X_H(p)_{/\mathbf{Q}}$; from this, the desired results on component groups follow. We conclude in Section 6 with some computer computations concerning the arithmetic of $J_1(p)$ for small $p$, where (among other things) we propose a formula for the order of the torsion subgroup of $J_1(p)(\mathbf{Q})$.

To avoid using Weierstrass equations in proofs, we have sometimes argued more abstractly than is strictly necessary, but this has the merit of enabling us to treat cusps by essentially the same methods as the other points. We would prefer to avoid mentioning $j$-invariants, but it is more succinct to say "cases with $j = 0$" than it is to say "cases such that $\mathrm{Aut}(E_{/k})$ has order 6."

Because we generally use methods of abstract deformation theory, the same approach should apply to Drinfeld modular curves, as well as to cases with auxiliary level structure away from $p$ (including mod $p$ component groups of suitable Shimura curves associated to indefinite quaternion algebras over $\mathbf{Q}$, with $p$ not dividing the discriminant). However, since a few additional technicalities arise, we leave these examples to be treated at a future time.

### 1.3 Notation and terminology

Throughout this paper, $p$ denotes an arbitrary prime unless otherwise indicated. Although the cases $p \leq 3$ are not very interesting from the point of view of our main results, keeping these cases in mind has often led us to more conceptual proofs. We write $\Phi_p(T) = (T^p - 1)/(T - 1) \in \mathbf{Z}[T]$ to denote the $p$th cyclotomic polynomial (so $\Phi_p(T + 1)$ is $p$-Eisenstein).

We write $V^\vee$ to denote the dual of a vector space $V$, and we write $\mathcal{F}^\vee$ to denote the dual of a locally free sheaf $\mathcal{F}$.

If $X$ and $S'$ are schemes over a scheme $S$ then $X_{/S'}$ and $X_{S'}$ denote $X \times_S S'$. If $S$ is an integral scheme with function field $K$ and $X$ is a $K$-scheme, by a *model* of $X$ (over $S$) we mean a flat $S$-scheme with generic fiber $X$.

By an $S$-*curve* over a scheme $S$ we mean a flat separated finitely presented map $X \to S$ with fibers of pure dimension 1 (the fibral dimension condition need only be checked on generic fibers, thanks to [27, $\mathrm{IV}_3$, 13.2.3] and a reduction to the noetherian case). Of course, when a map of schemes $X \to S$ is proper flat and finitely presented with geometrically connected generic fibers, then the other fibers are automatically geometrically connected (via reduction to the noetherian case and a Stein factorization argument). For purely technical reasons, we do *not* require $S$-curves to be proper or to have geometrically connected fibers. The main reason for this is that we want to use étale localization arguments on $X$ without having to violate running hypotheses. The use of Corollary 2.2.4 in the proof of Theorem 2.4.1 illustrates this point.

## 2 Resolution of singularities

Our eventual aim is to determine the component groups of Jacobians of intermediate curves between $X_1(p)$ and $X_0(p)$. Such curves are exactly the quotient curves $X_H(p) = X_1(p)/H$ for subgroups $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$, where we identify the group $\mathrm{Aut}_{\mathbf{Q}}(X_1(p)/X_0(p)) = \mathrm{Aut}_{\overline{\mathbf{Q}}}(X_1(p)/X_0(p))$ with $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ via the diamond operators (in terms of moduli, $n \in (\mathbf{Z}/p\mathbf{Z})^\times$ sends a pair $(E, P)$ to the pair $(E, n \cdot P)$). The quotient $X_H(p)_{/\mathbf{Z}_{(p)}}$ is an arithmetic surface with tame cyclic quotient singularities (at least when $p > 3$).

After some background review in Section 2.1 and some discussion of generalities in Section 2.2, in Section 2.3 we will describe a class of curves that give rise to (what we call) *tame cyclic quotient singularities*. Rather than work with global quotient situations $X/H$, it is more convenient to require such quotient descriptions only on the level of complete local rings. For example, this is what one encounters when computing complete local rings on coarse modular curves: the complete local ring is a subring of invariants of the universal deformation ring under the action of a finite group, but this group-action might not be induced by an action on the global modular curve. In Section 2.4 we establish the Jung–Hirzebruch continued-fraction algorithm that minimally resolves tame cyclic quotient singularities on curves over an arbitrary discrete valuation ring. The proof requires the Artin approximation theorem, and for this reason we need to define the concept of a *curve* as in Section 1.3 without requiring properness or geometric connectivity of fibers.

We should briefly indicate here why we need to use Artin approximation to compute minimal resolutions. Although the end result of our resolution process is intrinsic and of étale local nature on the curve, the mechanism by which the proof gets there depends on coordinatization and is not intrinsic (*e.g.*, we do not blow-up at points, but rather along certain codimension-1 subschemes). The only way we can relate the general case to a coordinate-dependent calculation in a special case is to use Artin approximation to find a common étale neighborhood over the general case and a special case (coupled with the étale local nature of the intrinsic minimal resolution that we are seeking to describe).

These resolution results are applied in subsequent sections to compute a regular proper model of $X_H(p)_{/\mathbf{Q}}$ over $\mathbf{Z}_{(p)}$ in such a way that we can compute both the mod-$p$ geometric component group of the Jacobian $J_H(p)$ and the map induced by $J_0(p) \to J_H(p)$ on mod-$p$ geometric component-groups. In this way, we will prove Theorem 1.1.6 (as well as Theorem 1.1.2 in the case of trivial $H$).

## 2.1 Background review

Some basic references for intersection theory and resolution of singularities for connected proper flat regular curves over Dedekind schemes are [29, Exposé X], [13], and [41, Ch. 9].

If $S$ is a connected Dedekind scheme with function field $K$ and $X$ is a normal $S$-curve, when $S$ is excellent we can construct a resolution of singularities as follows: blow-up the finitely many non-regular points of $X$ (all in codimension 2), normalize, and then repeat until the process stops. That this process always stops is due to a general theorem of Lipman [40]. For more general (*i.e.*, possibly non-excellent) $S$, and $X_{/S}$ with *smooth* generic fiber, the same algorithm works (including the fact that the non-regular locus consists of only finitely many closed points in closed fibers). Indeed, when $X_{/K}$ is smooth then the non-smooth locus of $X \to S$ is supported on finitely many closed fibers, so we may assume $S = \mathrm{Spec}(R)$ is local. We can then use Lemma 2.1.1 below to bring results down from $X_{/\widehat{R}}$ since $\widehat{R}$ is excellent.

See Theorem 2.2.2 for the existence and uniqueness of a canonical minimal regular resolution $X^{\mathrm{reg}} \to X$ for any connected Dedekind $S$ when $X_{/K}$ smooth. A general result of Lichtenbaum [39] and Shafarevich [61] ensures that when $X_{/S}$ is also proper (with smooth generic fiber if $S$ isn't excellent), by beginning with $X^{\mathrm{reg}}$ (or any regular proper model of $X_{/K}$) we can successively blow down $-1$-curves (see Definition 2.2.1) in closed fibers over $S$ until there are no more such $-1$-curves, at which point we have reached a relatively minimal model among the regular proper models of $X_{/K}$. Moreover, when $X_{/K}$ is in addition geometrically integral with positive arithmetic genus (*i.e.*, $\mathrm{H}^1(X_{/K}, \mathcal{O}) \neq 0$), this is the unique relatively minimal regular proper model, up to unique isomorphism.

In various calculations below with proper curves, it will be convenient to work over a base that is complete with algebraically closed residue field. Since passage from $\mathbf{Z}_{(p)}$ to $W(\overline{\mathbf{F}}_p)$ involves base change to a strict henselization followed by base change to a completion, in order to not lose touch with the situation over $\mathbf{Z}_{(p)}$ it is useful to keep in mind that formation of the minimal regular proper model (when the generic fiber is smooth with positive genus) is compatible with base change to a completion, henselization, and strict henselization on the base. We will not really require these results, but we do need to use the key fact in their proof: certain base changes do not destroy regularity or normality (and so in particular commute with formation of normalizations). This is given by:

Lemma 2.1.1. *Let $R$ be a discrete valuation ring with fraction field $K$ and let $X$ be a locally finite type flat $R$-scheme that has* regular *generic fiber. Let $R \to R'$ be an extension of discrete valuation rings for which $\mathfrak{m}_R R' = \mathfrak{m}_{R'}$ and the residue field extension $k \to k'$ is separable. Assume either that the fraction field extension $K \to K'$ is separable or that $X_{/K}$ is smooth* (*so either way, $X_{/K'}$ is automatically regular*).

*For any $x' \in X' = X \times_R R'$ lying over $x \in X$, the local ring $\mathcal{O}_{X',x'}$ is regular (resp. normal) if and only if the local ring $\mathcal{O}_{X,x}$ is regular (resp. normal).*

*Proof.* Since $\mathfrak{m}_R R' = \mathfrak{m}_{R'}$, the map $\pi : X' \to X$ induces $\pi_k : X_{/k} \times_k k' \to X_{/k}$ upon reduction modulo $\mathfrak{m}_R$. The separability of $k'$ over $k$ implies that $\pi_k$ is a regular morphism. Thus, if $x$ and $x'$ lie in the closed fibers then $\mathcal{O}_{X,x} \to \mathcal{O}_{X',x'}$ is faithfully flat with regular fiber ring $\mathcal{O}_{X',x'}/\mathfrak{m}_x$. Consequently, $X$ is regular at $x$ if and only if $X'$ is regular at $x'$ [44, 23.7]. Meanwhile, if $x$ and $x'$ lie in the generic fibers then they are both regular points since the generic fibers are regular. This settles the regular case.

For the normal case, when $X'$ is normal then the normality of $X$ follows from the faithful flatness of $\pi$ [44, Cor. to 23.9]. Conversely, when $X$ is normal then to deduce normality of $X'$ we use Serre's "$R_1 + S_2$" criterion. The regularity of $X'$ in codimensions $\leq 1$ is clear at points on the regular generic fiber. The only other points of codimension $\leq 1$ on $X'$ are the generic points of the closed fiber, and these lie over the (codimension 1) generic points of the closed fiber of $X$. Such points on $X$ are regular since $X$ is now being assumed to be normal, so the desired regularity on $X'$ follows from the preceding argument. This takes care of the $R_1$ condition. It remains to check that points $x' \in X'$ in codimensions $\geq 2$ contain a regular sequence of length 2 in their local rings. This is clear if $x'$ lies on the regular generic fiber, and otherwise $x'$ is a point of codimension $\geq 1$ on the closed fiber. Thus, $x = \pi(x')$ is either a generic point of $X_{/k}$ or is a point of codimension $\geq 1$ on $X_{/k}$. In the latter case the normal local ring $\mathcal{O}_{X,x}$ has dimension at least 2 and hence contains a regular sequence of length 2; this gives a regular sequence in the faithfully flat extension ring $\mathcal{O}_{X',x'}$. If instead $x$ is a generic point of $X_{/k}$ then $\mathcal{O}_{X,x}$ is a regular ring. It follows that $\mathcal{O}_{X',x'}$ is regular, so we again get the desired regular sequence (since $\dim \mathcal{O}_{X',x'} \geq 2$). □

We wish to record an elementary result in intersection theory that we will use several times later on. First, some notation needs to be clarified: if $X$ is a connected regular proper curve over a discrete valuation ring $R$ with residue field $k$, and $D$ and $D'$ are two *distinct* irreducible and reduced divisors in the closed fiber, then

$$D.D' := \dim_k \mathrm{H}^0(D \cap D', \mathcal{O}) = \sum_{d \in D \cap D'} \dim_k \mathcal{O}_{D \cap D', d}.$$

This is generally larger than the length of the artin ring $\mathrm{H}^0(D \cap D', \mathcal{O})$, and is called the *$k$-length* of $D \cap D'$. If $F = \mathrm{H}^0(D, \mathcal{O}_D)$, then $D \cap D'$ is also an $F$-scheme, and so it makes sense to define

$$D._F D' = \dim_F \mathrm{H}^0(D \cap D', \mathcal{O}) = D.D'/[F : k].$$

We call this the *$F$-length* of $D \cap D'$. We can likewise define $D._{F'} D'$ for the field $F' = \mathrm{H}^0(D', \mathcal{O})$. If $D' = D$, we define the relative self-intersection $D._F D$ to be $(D.D)/[F : k]$ where $D.D$ is the usual self-intersection number on the $k$-fiber.

Theorem 2.1.2. *Let $X$ be a connected regular proper curve over a discrete valuation ring, and let $P \in X$ be a closed point in the closed fiber. Let $C_1$, $C_2$ be two (possibly equal) effective divisors supported in the closed fiber of $X$, with each $C_j$ passing through $P$, and let $C_j'$ be the strict transform of $C_j$ under the blow-up $\pi : X' = \mathrm{Bl}_P(X) \to X$. We write $E \simeq \mathbf{P}^1_{k(P)}$ to denote the exceptional divsor.*

*We have $\pi^{-1}(C_j) = C_j' + m_j E$ where $m_j = \mathrm{mult}_P(C_j)$ is the multiplicity of the curve $C_j$ at $P$. Also, $m_j = (C_j')._{k(P)}E$ and*

$$C_1.C_2 = C_1'.C_2' + m_1 m_2 [k(P) : k].$$

*Proof.* Recall that for a regular local ring $R$ of dimension 2 and any non-zero non-unit $g \in R$, the 1-dimensional local ring $R/g$ has multiplicity (*i.e.*, leading coefficient of its Hilbert-Samuel polynomial) equal to the unique integer $\mu \geq 1$ such that $g \in \mathfrak{m}_R^{\mu}$, $g \notin \mathfrak{m}_R^{\mu+1}$.

We have $\pi^{-1}(C_j) = C_j' + m_j E$ for some positive integer $m_j$ that we must prove is equal to the multiplicity $\mu_j = \mathrm{mult}_P(C_j)$ of $C_j$ at $P$. We have $E._{k(P)}E = -1$, so $E.E = -[k(P) : k]$, and we also have $\pi^{-1}(C_j).E = 0$, so $m_j = (C_j'.E)/[k(P) : k] = (C_j')._{k(P)}E$. The strict transform $C_j'$ is the blow-up of $C_j$ at $P$, equipped with its natural (closed immersion) map into $X'$. The number $m_j$ is the $k(P)$-length of the scheme-theoretic intersection $C_j' \cap E$; this is the fiber of $\mathrm{Bl}_P(C_j) \to C_j$ over $P$. Intuitively, this latter fiber is the scheme of tangent directions to $C_j$ at $P$, but more precisely it is $\mathrm{Proj}(S_j)$, where

$$S_j = \bigoplus_{n \geq 0} \mathfrak{m}_j^n / \mathfrak{m}_j^{n+1},$$

and $\mathfrak{m}_j$ is the maximal ideal of $\mathcal{O}_{C_j,P} = \mathcal{O}_{X,P}/(f_j)$, with $f_j$ a local equation for $C_j$ at $P$. We have $\mathfrak{m}_j = \mathfrak{m}/(f_j)$ with $\mathfrak{m}$ the maximal ideal of $\mathcal{O}_{X,P}$. Since $f_j \in \mathfrak{m}^{\mu_j}$ and $f_j \notin \mathfrak{m}^{\mu_j+1}$,

$$S_j \simeq \mathrm{Sym}_{k(P)}(\mathfrak{m}/\mathfrak{m}^2)/\overline{f}_j = k(P)[u,v]/(\overline{f}_j)$$

with $\overline{f}_j$ denoting the nonzero image of $f_j$ in degree $\mu_j$. We conclude that $\mathrm{Proj}(S_j)$ has $k(P)$-length $\mu_j$, so $m_j = \mu_j$. Thus, we may compute

$$\begin{aligned} C_1.C_2 = \pi^{-1}(C_1).\pi^{-1}(C_2) &= C_1'.C_2' + 2m_1m_2[k(P):k] + m_1m_2 E.E \\ &= C_1'.C_2' + m_1m_2[k(P):k]. \end{aligned}$$

□

## 2.2 Minimal resolutions

It is no doubt well-known to experts that the classical technique of resolution for cyclic quotient singularities on complex surfaces [25, §2.6] can be adapted to the case of tame cyclic quotient singularities on curves over a complete equicharacteristic discrete valuation ring. We want the case of an arbitrary discrete valuation ring, and this seems to be less widely known (it is not addressed in the literature, and was not known to an expert in log-geometry with whom we consulted). Since there seems to be no adequate reference for this more general result, we will give the proof after some preliminary work (*e.g.*, we have to define what we mean by a *tame cyclic quotient singularity*, and we must show that this definition is applicable in many situations. Our first step is to establish the existence and uniqueness of a minimal regular resolution in the case of relative curves over a Dedekind base (the case of interest to us); this will eventually serve to make sense of the *canonical resolution* at a point.

Since we avoid properness assumptions, to avoid any confusion we should explicitly recall a definition.

Definition 2.2.1. Let $X \to S$ be a regular $S$-curve, with $S$ a connected Dedekind scheme. We say that an integral divisor $D \hookrightarrow X$ in a closed fiber $X_s$ is a $-1$-*curve* if $D$ is proper over $k(s)$, $\mathrm{H}^1(D, \mathcal{O}_D) = 0$, and $\deg_k \mathcal{O}_D(D) = -1$, where $k = \mathrm{H}^0(D, \mathcal{O}_D)$ is a finite extension of $k(s)$.

By Castelnuovo's theorem, a $-1$-curve $D \hookrightarrow X$ as in Definition 2.2.1 is $k$-isomorphic to a projective line over $k$, where $k = \mathrm{H}^0(D, \mathcal{O}_D)$.

The existence and uniqueness of minimal regular resolutions is given by:

Theorem 2.2.2. *Let $X \to S$ be a normal $S$-curve over a connected Dedekind scheme $S$. Assume either that $S$ is excellent or that $X_{/S}$ has smooth generic fiber.*

*There exists a birational proper morphism $\pi : X^{\mathrm{reg}} \to X$ such that $X^{\mathrm{reg}}$ is a regular $S$-curve and there are no $-1$-curves in the fibers of $\pi$. Such an $X$-scheme is unique up to unique isomorphism, and every birational proper morphism $X' \to X$ with a regular $S$-curve $X'$ admits a unique factorization through $\pi$. Formation of $X^{\mathrm{reg}}$ is compatible with base change to* $\operatorname{Spec} \mathcal{O}_{S,s}$ *and* $\operatorname{Spec} \widehat{\mathcal{O}}_{S,s}$ *for closed points $s \in S$. For local $S$, there is also compatibility with ind-étale base change $S' \to S$ with local $S'$ whose closed point is residually trivial over that of $S$.*

We remind that reader that, for technical reasons in the proof of Theorem 2.4.1, we avoid requiring curves to be proper and we do not assume the generic fiber to be geometrically connected. The reader is referred to [41, 9/3.32] for an alternative discussion in the proper case.

*Proof.* We first assume $S$ to be excellent, and then we shall use Lemma 2.1.1 and some descent considerations to reduce the general case to the excellent case by passage to completions.

As a preliminary step, we wish to reduce to the proper case (to make the proof of uniqueness easier). By Nagata's compactification theorem [43] and the finiteness of normalization for excellent schemes, we can find a schematically dense open immersion $X \hookrightarrow \overline{X}$ with $\overline{X}_{/S}$ normal, proper, and flat over $S$ (hence a normal $S$-curve). By resolving singularities along $\overline{X} - X$, we may assume the non-regular locus on $\overline{X}$ coincides with that on $X$. Thus, the existence and uniqueness result for $X$ will follow from that for $\overline{X}$. The assertion on regular resolutions (uniquely) factorizing through $\pi$ goes the same way. Hence, we now assume (for excellent $S$) that $X_{/S}$ is proper. We can also assume $X$ to be connected.

By Lemma 2.1.1 and resolution for excellent surfaces, there exists a birational *proper* morphism $X' \to X$ with $X'$ a regular proper $S$-curve. If there is a $-1$-curve in the fiber of $X'$ over some (necessarily closed) point of $X$, then by Castelnuovo we can blow down the $-1$-curve and $X' \to X$ will factor through the blow-down. This blow-down process cannot continue forever, so we get the existence of $\pi : X^{\mathrm{reg}} \to X$ with no $-1$-curves in its fibers.

Recall the Factorization Theorem for birational *proper* morphisms between regular connected $S$-curves: such maps factor as a composite of blow-ups at closed points in closed fibers. Using the Factorization Theorem, to prove uniqueness of $\pi$ and the (unique) factorization through $\pi$ for any regular resolution of $X$ we just have to show that if $X'' \to X' \to X$ is a tower of birational proper morphisms with regular $S$-curves $X'$ and $X''$ such that $X'$ has no $-1$-curves in its fibers over $X$, then any $-1$-curve $C$ in a fiber of $X'' \to X$ is necessarily contracted by $X'' \to X'$. Also, via Stein factorization we can assume that the proper normal connected $S$-curves $X$, $X'$, and $X''$ with common generic fiber over $S$ have geometrically connected fibers over $S$. We may assume that $S$ is local. Since the map $q : X'' \to X'$ is a composite of blow-ups, we may assume that $C$ meets the exceptional fiber $E$ of the first blow-down $q_1 : X'' \to X''_1$ of a factorization of $q$. If $C = E$ we are done, so we may assume $C \neq E$. In this case we will show that $X$ is regular, so again uniqueness holds (by the Factorization Theorem mentioned above).

The image $q_1(C)$ is an irreducible divisor on $X''_1$ with strict transform $C$, so by Theorem 2.1.2 we conclude that $q_1(C)$ has non-negative self-intersection number, so this self-intersection must be zero. Since $X''_1 \to S$ is its own Stein factorization, and hence has geometrically connected closed fiber, $q_1(C)$ must be the entire closed fiber of $X''_1$. Thus, $X''_1$ has irreducible closed fiber, and so the (surjective) proper birational map $X''_1 \to X$ is quasi-finite and hence finite. Since $X$ and $X''_1$ are normal and connected (hence integral), it follows that $X''_1 \to X$ must be an isomorphism. Thus, $X$ is regular, as desired.

With $X^{\mathrm{reg}}$ unique up to (obviously) unique isomorphism, for the base change compatibility we note that the various base changes $S' \to S$ being considered (to completions on $S$, or to local $S'$ ind-étale surjective over local $S$ and residually trivial at closed points), the base change $X^{\mathrm{reg}}_{/S'}$ is regular and proper birational over the normal curve $X_{/S'}$ (see Lemma 2.1.1). Thus, we just have to check that the fibers of $X^{\mathrm{reg}}_{/S'} \to X_{/S'}$ do not contain $-1$-curves. The closed-fiber situation is identical to that before base change, due to the residually trivial condition at closed points, so we are done.

Now suppose we do not assume $S$ to be excellent, but instead assume $X_{/S}$ has smooth generic fiber. In this case all but finitely many fibers of $X_{/S}$ are smooth. Thus, we may reduce to the local case $S = \operatorname{Spec}(R)$ with a discrete valuation ring $R$. Consider $X_{/\widehat{R}}$, a normal $\widehat{R}$-curve by Lemma 2.1.1. Since $\widehat{R}$ is excellent, there is a minimal regular resolution

$$\pi : (X_{/\widehat{R}})^{\mathrm{reg}} \to X_{/\widehat{R}}.$$

By [40, Remark C, p. 155], the map $\pi$ is a blow-up along a 0-dimensional closed subscheme $\widehat{Z}$ physically supported in the non-regular locus of $X_{/\widehat{R}}$. This $\widehat{Z}$ is therefore physically supported in the closed fiber of $X_{/\widehat{R}}$, yet $\widehat{Z}$ is artinian and hence lies in some infinitesimal closed fiber of $X_{/\widehat{R}}$. Since $X \times_R \widehat{R} \to X$ induces isomorphisms on the level of $n$th infinitesimal closed-fibers for all $n$, there is a unique 0-dimensional closed subscheme $Z$ in $X$ with $Z_{/\widehat{R}} = \widehat{Z}$ inside of $X_{/\widehat{R}}$.

Since the blow-up $\mathrm{Bl}_Z(X)$ satisfies

$$\mathrm{Bl}_Z(X)_{/\widehat{R}} \simeq \mathrm{Bl}_{\widehat{Z}}(X_{/\widehat{R}}) = (X_{/\widehat{R}})^{\mathrm{reg}},$$

by Lemma 2.1.1 we see that $\mathrm{Bl}_Z(X)$ is a regular $S$-curve. There are no $-1$-curves in its fibers over $X$ since $\operatorname{Spec}\widehat{R} \to \operatorname{Spec} R$ is an isomorphism over $\operatorname{Spec} R/\mathfrak{m}$. This establishes the existence of $\pi : X^{\mathrm{reg}} \to X$, as well as its compatibility with base change to completions on $S$. To establish uniqueness of $\pi$, or more generally its universal factorization property, we must prove that certain birational maps from regular $S$-curves to $X^{\mathrm{reg}}$ are morphisms. This is handled by a standard graph argument that can be checked after faithfully flat base change to $\widehat{R}$ (such base change preserves regularity, by Lemma 2.1.1). Thus, the uniqueness results over the excellent base $\widehat{R}$ carry over to our original $R$. The same technique of base change to $\widehat{R}$ shows compatibility with ind-étale base change that is residually trivial over closed points.

□

One mild enhancement of the preceding theorem rests on a pointwise definition:

Definition 2.2.3. Let $X_{/S}$ be as in Theorem 2.2.2, and let $\Sigma \subseteq X$ be a finite set of closed points in closed fibers over $S$. Let $U$ be an open in $X$ containing $\Sigma$ such that $U$ does not contain the finitely many non-regular points of $X$ outside of $\Sigma$. We define the *minimal regular resolution along* $\Sigma$ to be the morphism $\pi_\Sigma : X_\Sigma \to X$ obtained by gluing $X - \Sigma$ with the part of $X^{\mathrm{reg}}$ lying over $U$ (note: the choice of $U$ does not matter, and $X_\Sigma$ is not regular if there are non-regular points of $X$ outside of $\Sigma$).

It is clear that the minimal regular resolution along $\Sigma$ is compatible with local residually-trivial ind-étale base change on a local $S$, as well as with base change to a (non-generic) complete local ring on $S$. It is also uniquely characterized among normal $S$-curves $C$ equipped with a proper birational morphism $\varphi : C \to X$ via the following conditions:

- $\pi_\Sigma$ is an isomorphism over $X - \Sigma$,
- $X_\Sigma$ is regular at points over $\Sigma$,
- $X_\Sigma$ has no $-1$-curves in its fibers over $\Sigma$.

This yields the crucial consequence that (under some mild restrictions on residue field extensions) formation of $X_\Sigma$ is étale-local on $X$. This fact is ultimately the reason we did not require properness or geometrically connected fibers in our definition of *$S$-curve*:

Corollary 2.2.4. *Let $X_{/S}$ be a normal $S$-curve over a connected Dedekind scheme $S$, and let $\Sigma \subseteq X$ be a finite set of closed points in closed fibers over $S$. Let $X' \to X$ be étale (so $X'$ is an $S$-curve), and let $\Sigma'$ denote the preimage of $\Sigma$. Assume that $S$ is excellent or $X_{/S}$ has smooth generic fiber.*

*If $X_\Sigma \to X$ denotes the minimal regular resolution along $\Sigma$, and $X' \to X$ is residually trivial over $\Sigma$, then the base change $X_\Sigma \times_X X' \to X'$ is the minimal regular resolution along $\Sigma'$.*

*Remark* 2.2.5. The residual triviality condition over $\Sigma$ is satisfied when $S$ is local with separably closed residue field, as then all points of $\Sigma$ have separably closed residue field (and so the étale $X' \to X$ must induce trivial residue field extensions over such points).

*Proof.* Since $X_\Sigma \times_X X'$ is étale over $X_\Sigma$, we conclude that $X_\Sigma \times_X X'$ is an $S$-curve that is regular along the locus over $\Sigma' \subseteq X'$, and its projection to $X'$ is proper, birational, and an isomorphism over $X' - \Sigma'$. It remains to check that

$$X_\Sigma \times_X X' \to X' \tag{2.2.1}$$

has no $-1$-curves in the proper fibers over $\Sigma'$. Since $X' \to X$ is residually trivial over $\Sigma$ (by hypothesis), so this is clear. □

## 2.3 Nil-semistable curves

In order to compute minimal regular resolutions of the sort that arise on $X_H(p)$'s, it is convenient to study the following concept before we discuss resolution of singularities. Let $S$ be a connected Dedekind scheme and let $X$ be an $S$-curve.

Definition 2.3.1. For a closed point $s \in S$, a closed point $x \in X_s$ is *nil-semistable* if the reduced fiber-curve $X_s^{\mathrm{red}}$ is semistable over $k(s)$ at $x$ and all of the analytic branch multiplicities through $x$ are not divisible by $\mathrm{char}(k(s))$. If $X_s^{\mathrm{red}}$ is semistable for all closed points $s \in S$ and all irreducible components of $X_s$ have multiplicity not divisible by $\mathrm{char}(k(s))$, $X$ is a *nil-semistable curve* over $S$.

Considerations with excellence of the fiber $X_s$ show that the number of analytic branches in Definition 2.3.1 may be computed on the formal completion at a point over $x$ in $X_{s/k'}$ for any separably closed extension $k'$ of $k(s)$. We will use the phrase "analytic branch" to refer to such (formal) branches through a point over $x$ in such a geometric fiber over $s$.

As is well-known from [34], many fine moduli schemes for elliptic curves are nil-semistable.

Fix a closed point $s \in S$. From the theory of semistable curves over fields [24, III, §2], it follows that when $x \in X_s^{\rm red}$ is a semistable non-smooth point then the finite extension $k(x)/k(s)$ is separable. We have the following analogue of the classification of semistable curve singularities:

Lemma 2.3.2. *Let $x \in X_s$ be a closed point and let $\pi_s \in \mathcal{O}_{S,s}$ be a uniformizer.*

*If $x$ is a nil-semistable point at which $X$ is regular, then the underlying reduced scheme of the geometric closed fiber over $s$ has either one or two analytic branches at a geometric point over $x$, with these branches smooth at $x$. When moreover $k(x)/k(s)$ is separable and there is exactly one analytic branch at $x \in X_s$, with multiplicity $m_1$ in $\mathcal{O}_{X_s,x}^{\rm sh}$, then*

$$\widehat{\mathcal{O}_{X,x}^{\rm sh}} \simeq \widehat{\mathcal{O}_{S,s}^{\rm sh}}[\![t_1,t_2]\!]/(t_1^{m_1} - \pi_s). \tag{2.3.1}$$

*If there are two analytic branches (so $k(x)/k(s)$ is automatically separable), say with multiplicities $m_1$ and $m_2$ in $\mathcal{O}_{X_s,x}^{\rm sh}$, then*

$$\widehat{\mathcal{O}_{X,x}^{\rm sh}} \simeq \widehat{\mathcal{O}_{S,s}^{\rm sh}}[\![t_1,t_2]\!]/(t_1^{m_1}t_2^{m_2} - \pi_s). \tag{2.3.2}$$

*Conversely, if $\widehat{\mathcal{O}_{X,x}^{\rm sh}}$ admits one of these two explicit descriptions with the exponents not divisible by* $\mathrm{char}(k(s))$*, then $x$ is a nil-semistable regular point on $X$ with $k(x)/k(s)$ separable.*

In view of this lemma, we call the exponents in the formal isomorphisms (2.3.1) and (2.3.2) the *analytic geometric multiplicities* of $X_s$ at $x$ (this requires $k(x)/k(s)$ to be separable). We emphasize that these exponents can be computed after base change to any separably closed extension of $k(s)$ when $x$ is nil-semistable with $k(x)/k(s)$ separable.

*Proof.* First assume $x \in X_s^{\rm red}$ is a non-smooth semistable point and $X$ is regular at $x$. Since $k(x)$ is therefore finite separable over $k(s)$, we can make a base change to the completion of a strict henselization of $\mathcal{O}_{S,s}$ to reduce to the case $S = \mathrm{Spec}(W)$ with a complete discrete valuation ring $W$ having separably closed residue field $k$ such that $x$ a $k$-rational point. Since $\widehat{\mathcal{O}}_{X,x}$ is a 2-dimensional complete regular local $W$-algebra with residue field $k$, it is a quotient of $W[\![t_1,t_2]\!]$ and hence has the form $W[\![t_1,t_2]\!]/(f)$ where $f$ is a regular parameter. The semistability condition and non-smoothness of $X_{/k}^{\rm red}$ at $x$ imply

$$k[\![t_1,t_2]\!]/\mathrm{rad}(\overline{f}) = (k[\![t_1,t_2]\!]/(\overline{f}))_{\rm red} \simeq \widehat{\mathcal{O}}_{X_{/k}^{\rm red},x} \simeq k[\![u_1,u_2]\!]/(u_1u_2)$$

where $\overline{f} = f \bmod \mathfrak{m}_W$, so $\overline{f}$ has exactly two distinct irreducible factors and these have distinct (non-zero) tangent directions in $X^{\mathrm{red}}_{/k}$ through $x$. We can choose $t_1$ and $t_2$ to lift these tangent directions, so upon replacing $f$ with a unit multiple we may assume $\overline{f} = t_1^{m_1} t_2^{m_2} \bmod \mathfrak{m}_W$ for some $m_1, m_2 \geq 1$ not divisible by $p = \mathrm{char}(k) \geq 0$. Let $\pi$ be a uniformizer of $W$, so $f = t_1^{m_1} t_2^{m_2} - \pi g$ for some $g$, and $g$ must be a unit since $f$ is a regular parameter. Since some $m_j$ is not divisible by $p$, and hence the unit $g$ admits an $m_j$th root, by unit-rescaling of the corresponding $t_j$ we get to the case $g = 1$.

In the case when $X_s^{\mathrm{red}}$ is smooth at $x$ and $k(x)/k(s)$ is separable, we may again reduce to the case in which $S = \mathrm{Spec}\, W$ with complete discrete valuation ring $W$ having separably closed residue field $k$ and $k(x) = k$. In this case, there is just one analytic branch and we see by a variant of the preceding argument that the completion of $\mathcal{O}^{\mathrm{sh}}_{X,x}$ has the desired form.

The converse part of the lemma is clear.

$\square$

In Definition 2.3.6, we shall give a local definition of the class of curve-singularities that we wish to resolve, but we will first work through some global considerations that motivate the relevance of the local Definition 2.3.6.

Assume $X$ is *regular*, and let $H$ be a finite group and assume we are given an action of $H$ on $X_{/S}$ that is free on the scheme of generic points (*i.e.*, no non-identity element of $H$ acts trivially on a connected component of $X$). A good example to keep in mind is the (affine) fine moduli scheme over $S = \mathrm{Spec}(\mathbf{Z}_{(p)})$ of $\Gamma_1(p)$-structures on elliptic curves equipped with auxiliary full level $\ell$-structure for an odd prime $\ell \neq p$, and $H = \mathrm{GL}_2(\mathbf{F}_\ell)$ acting in the usual manner (see Section 3 for a review of these basic level structures).

We wish to work with a quotient $S$-curve $X' = X/H$, so we now also assume that $X$ is quasi-projective Zariski-locally on $S$. Clearly $X \to X'$ is a finite $H$-equivariant map with the expected universal property; in the above modular-curve example, this quotient $X'$ is the coarse moduli scheme $Y_1(p)$ over $\mathbf{Z}_{(p)}$. We also now assume that $S$ is excellent or $X_{/K}$ is smooth, so that there are only finitely many non-regular points (all in codimension 2) and various results centering on resolution of singularities may be applied.

The $S$-curve $X'$ has regular generic fiber (and even smooth generic fiber when $X_{/S}$ has smooth generic fiber), and $X'$ is regular away from finitely many closed points in the closed fibers. Our aim is to understand the *minimal regular resolution* ${X'}^{\mathrm{reg}}$ of $X'$, or rather to describe the geometry of the fibers of ${X'}^{\mathrm{reg}} \to X'$ over non-regular points $x'$ satisfying a mild hypothesis on the structure of $X \to X'$ over $x'$.

We want to compute the minimal regular resolution for $X' = X/H$ at non-regular points $x'$ that satisfy several conditions. Let $s \in S$ be the image of $x'$, and let $p \geq 0$ denote the common characteristic of $k(x')$ and $k(s)$. Pick $x \in X$ over $x'$.

- We assume that $X$ is nil-semistable at $x$ (by the above hypotheses, $X$ is also regular at $x$).

- We assume that the inertia group $H_{x|x'}$ in $H$ at $x$ (*i.e.*, the stablizer in $H$ of a geometric point over $x$) has order not divisible by $p$ (so this group acts semi-simply on the tangent space at a geometric point over $x$).
- When there are two analytic branches through $x$, we assume $H_{x|x'}$ does not interchange them.

These conditions are independent of the choice of $x$ over $x'$ and can be checked at a geometric point over $x$, and when they hold then the number of analytic branches through $x$ coincides with the number of analytic branches through $x'$ (again, we are really speaking about analytic branches on a geometric fiber over $s$).

Since $p$ does not divide $|H_{x|x'}|$, it follows that $k(x')$ is the subring of invariants under the action of $H_{x|x'}$ on $k(x)$, so a classical theorem of Artin ensures that $k(x)/k(x')$ is separable (and even Galois). Thus, $k(x)/k(s)$ is separable if and only if $k(x')/k(s)$ is separable, and such separability holds when the point $x \in X_s^{\mathrm{red}}$ is semistable but not smooth. Happily for us, this separability condition over $k(s)$ is always satisfied (we are grateful to Lorenzini for pointing this out):

LEMMA 2.3.3. *With notation and hypotheses as above, particularly with $x' \in X' = X/H$ a non-regular point, the extension $k(x')/k(s)$ is separable.*

*Proof.* Recall that, by hypothesis, $x \in X_s^{\mathrm{red}}$ is either a smooth point or an ordinary double point. If $x$ is a non-smooth point on the curve $X_s^{\mathrm{red}}$, then the desired separability follows from the theory of ordinary double point singularities. Thus, we may (and do) assume that $x$ is a smooth point on $X_s^{\mathrm{red}}$.

We may also assume $S$ is local and strictly henselian, so $k(s)$ is separably closed and hence $k(x)$ and $k(x')$ are separably closed. Thus, $k(x) = k(x')$ and $H_{x|x'}$ is the physical stabilizer of the point $x \in X$. We need to show that the common residue field $k(x) = k(x')$ is separable over $k(s)$. If we let $X'' = X/H_{x|x'}$, then the image $x''$ of $x$ in $X''$ has complete local ring isomorphic to that of $x' \in X'$, so we may replace $X'$ with $X''$ to reduce to the case when $H$ has order not divisible by $p$ and $x$ is in the fixed-point locus of $H$. By [20, Prop. 3.4], the fixed-point locus of $H$ in $X$ admits a closed-subscheme structure in $X$ that is smooth over $S$. On the closed fiber this smooth scheme is finite and hence étale over $k(s)$, so its residue fields are separable over $k(s)$.

□

The following refinement of Lemma 2.3.2 is adapted to the $H_{x|x'}$-action, and simultaneously handles the cases of one and two (geometric) analytic branches through $x'$.

LEMMA 2.3.4. *With hypotheses as above, there is an $\widehat{\mathcal{O}_{S,s}^{\mathrm{sh}}}$-isomorphism*

$$\widehat{\mathcal{O}_{X,x}^{\mathrm{sh}}} \simeq \widehat{\mathcal{O}_{S,s}^{\mathrm{sh}}}[\![t_1, t_2]\!]/(t_1^{m_1} t_2^{m_2} - \pi_s)$$

*(with $m_1 > 0$, $m_2 \geq 0$) such that the $H_{x|x'}$-action looks like $h(t_j) = \chi_j(h)t_j$ for characters $\chi_1, \chi_2 : H_{x|x'} \to \widehat{\mathcal{O}^{\rm sh}_{S,s}}^{\times}$ that are the Teichmüller lifts of characters giving a decomposition of the semisimple $H_{x|x'}$-action on the 2-dimensional cotangent space at a geometric point over $x$. Moreover, $\chi_1^{m_1}\chi_2^{m_2} = 1$.*

The characters $\chi_j$ also describe the action of $H_{x|x'}$ on the tangent space at (a geometric point over) $x$. There are two closed-fiber analytic branches through $x$ when $m_1$ and $m_2$ are positive, and then the branch with formal parameter $t_2$ has multiplicity $m_1$ since

$$(k[\![t_1, t_2]\!]/(t_1^{m_1} t_2^{m_2}))[1/t_2] = k(\!(t_2)\!)[t_1]/(t_1^{m_1})$$

has length $m_1$. Likewise, when $m_2 > 0$ it is the branch with formal parameter $t_1$ that has multiplicity $m_2$.

*Proof.* We may assume $S = \operatorname{Spec} W$ with $W$ a complete discrete valuation ring having separably closed residue field $k$ and uniformizer $\pi$, so $x$ is $k$-rational. Let $R = \widehat{\mathcal{O}^{\rm sh}_{X,x}} = \widehat{\mathcal{O}}_{X,x}$. We have seen in Lemma 2.3.2 that there is an isomorphism of the desired type as $W$-algebras, but we need to find better such $t_j$'s to linearize the $H_{x|x'}$-action.

We first handle the easier case $m_2 = 0$. In this case there is only one minimal prime $(t_1)$ over $(\pi)$, so $h(t_1) = u_h t_1$ for a unique unit $u_h \in R^\times$. Since $t_1^{m_1} = \pi$ is $H_{x|x'}$ invariant, we see that $u_h \in \mu_{m_1}(R)$ is a Teichmüller lift from $k$ (since $p \nmid m_1$). Thus, $h(t_1) = \chi_1(h)t_1$ for a character $\chi_1 : H_{x|x'} \to R^\times$ that is a lift of a character for $H_{x|x'}$ on $\operatorname{Cot}_x(X)$. Since $H_{x|x'}$ acts semisimply on the 2-dimensional cotangent space $\operatorname{Cot}_x(X)$ and there is a stable line spanned by $t_1 \bmod \mathfrak{m}_x^2$, we can choose $t_2$ to lift an $H_{x|x'}$-stable line complementary to the one spanned by $t_1 \bmod \mathfrak{m}_x^2$. If $\chi_2$ denotes the Teichmüller lift of the character for $H_{x|x'}$ on this complementary line, then

$$h(t_2) = \chi_2(h)(t_2 + \delta_h)$$

with $\delta_h \in \mathfrak{m}_x^i$ for some $i \geq 2$. It is straightfoward to compute that

$$h \mapsto \delta_h \bmod \mathfrak{m}_x^{i+1}$$

is a 1-cocycle with values in the twisted $H_{x|x'}$-module $\chi_2^{-1} \otimes (\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1})$. Changing this 1-cocycle by a 1-coboundary corresponds to adding an element of $\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}$ to $t_2 \bmod \mathfrak{m}_x^{i+1}$. Since

$$\mathrm{H}^1(H_{x|x'}, \chi_2^{-1} \otimes (\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1})) = 0,$$

we can successively increase $i \geq 2$ and pass to the limit to find a choice of $t_2$ such that $H_{x|x'}$ acts on $t_2$ through the character $\chi_2$. That is, $h(t_1) = \chi_1(h)t_1$ and $h(t_2) = \chi_2(h)t_2$ for all $h \in H_{x|x'}$. This settles the case $m_2 = 0$.

Now we turn to the more interesting case when also $m_2 > 0$, so there are two analytic branches through $x$. By hypothesis, the $H_{x|x'}$-action preserves the two minimal primes $(t_1)$ and $(t_2)$ over $(\pi)$ in $R$. We must have $h(t_1) = u_h t_1$, $h(t_2) = v_h t_2$ for unique units $u_h, v_h \in R^\times$. Since $t_1^{m_1} t_2^{m_2} = \pi$, by applying $h$ we get $u_h^{m_1} v_h^{m_2} = 1$.

Consider what happens if we replace $t_2$ with a unit multiple $t_2' = vt_2$, and then replace $t_1$ with the unit multiple $t_1' = v^{-m_2/m_1} t_1$ so as to ensure $t_1'^{m_1} t_2'^{m_2} = \pi$. Note that an $m_1$th root $v^{-m_2/m_1}$ of the unit $v^{-m_2}$ makes sense since $k$ is separably closed and $p \nmid m_1$. The resulting map $W[\![t_1', t_2']\!]/(t_1'^{m_1} t_2'^{m_2} - \pi) \to R$ is visibly surjective, and hence is an isomorphism for dimension reasons. Switching to these new coordinates on $R$ has the effect of changing the 1-cocycle $\{v_h\}$ by a 1-coboundary, and *every* 1-cocycle cohomologous to $\{v_h\}$ is reached by making such a unit multiple change on $t_2$.

By separately treating residue characteristic 0 and positive residue characteristic, an inverse limit argument shows that $\mathrm{H}^1(H_{x|x'}, U)$ vanishes, where $U = \ker(R^\times \twoheadrightarrow k^\times)$. Thus, the natural map $\mathrm{H}^1(H_{x|x'}, R^\times) \to \mathrm{H}^1(H_{x|x'}, k^\times)$ is injective. The $H_{x|x'}$-action on $k^\times$ is trivial since $H_{x|x'}$ acts trivially on $W$, so

$$\mathrm{H}^1(H_{x|x'}, k^\times) = \mathrm{Hom}(H_{x|x'}, k^\times) = \mathrm{Hom}(H_{x|x'}, k^\times_{\mathrm{tors}}),$$

with all elements in the torsion subgroup $k^\times_{\mathrm{tors}}$ of order not divisible by $p$ and hence uniquely multiplicatively lifting into $R$. Thus,

$$\mathrm{H}^1(H_{x|x'}, R^\times) \to \mathrm{H}^1(H_{x|x'}, k^\times)$$

is bijective, and so replacing $t_1$ and $t_2$ with suitable unit multiples allows us to assume $h(t_2) = \chi_2(h) t_2$, with $\chi_2 : H_{x|x'} \to W^\times_{\mathrm{tors}}$ some homomorphism of order not divisible by $p$ (since $H_{x|x'}$ acts trivially on $k^\times$ and $p \nmid |H_{x|x'}|$).

Since

$$1 = u_h^{m_1} v_h^{m_2} = u_h^{m_1} \chi_2(h)^{m_2}$$

and $p \nmid m_1$, we see that $u_h$ is a root of unity of order not divisible by $p$. Viewing $k^\times_{\mathrm{tors}} \subseteq R^\times$ via the Teichmüller lifting, we conclude that $u_h \in k^\times_{\mathrm{tors}} \subseteq R^\times$. Thus, we can write $h(t_1) = \chi_1(h) t_1$ for a homomorphism $\chi_1 : H_{x|x'} \to W^\times_{\mathrm{tors}}$ also necessarily of order not divisible by $p$. The preceding calculation also shows that $\chi_1^{m_1} \chi_2^{m_2} = 1$ since $u_h^{m_1} v_h^{m_2} = 1$.

□

Although Lemma 2.3.4 provides good (geometric) coordinate systems for describing the inertia action, one additional way to simplify matters is to reduce to the case in which the tangent-space characters $\chi_1$ and $\chi_2$ are powers of each other. We wish to explain how this special situation is essentially the general case (in the presence of our running assumption that $H$ acts freely on the scheme of generic points of $X$).

First, observe that $H_{x|x'}$ acts faithfully on the tangent space $T_x(X)$ at $x$. Indeed, if an element in $H_{x|x'}$ acts trivially on the tangent space $T_x(X)$, then by Lemma 2.3.4 it acts trivially on the completion of $\mathcal{O}^{\mathrm{sh}}_{X,x}$ and hence acts trivially on the corresponding connected component of the normal $X$. By hypothesis, $H$ acts freely on the scheme of generic points of $X$, so we conclude that the product homomorphism

$$\chi_1 \times \chi_2 : H_{x|x'} \hookrightarrow k(x)_{\text{sep}}^{\times} \times k(x)_{\text{sep}}^{\times}, \tag{2.3.3}$$

is *injective* (where $k(x)_{\text{sep}}$ is the separable closure of $k(x)$ used when constructing $\mathcal{O}_{X,x}^{\text{sh}}$). In particular, $H_{x|x'}$ is a product of two cyclic groups (one of which might be trivial).

Lemma 2.3.5. *Let $\kappa_j = |\ker(\chi_j)|$. The characters $\chi_1^{\kappa_2}$ and $\chi_2^{\kappa_1}$ factor through a common quotient of $H_{x|x'}$ as faithful characters. When $H_{x|x'}$ is cyclic, this quotient is $H_{x|x'}$.*

*In addition, $\kappa_2|m_1$ and $\kappa_1|m_2$.*

The cyclicity condition on $H_{x|x'}$ will hold in our application to modular curves, as then even $H$ is cyclic.

*Proof.* The injectivity of (2.3.3) implies that $\chi_1$ is faithful on $\ker(\chi_2)$ and $\chi_2$ is faithful on $\ker(\chi_1)$. Since $\chi_1^{m_1}\chi_2^{m_2} = 1$, we get $\kappa_2|m_1$ and $\kappa_1|m_2$ (even if $m_2 = 0$).

For the proof that the indicated powers of the $\chi_j$'s factor as faithful characters of a common quotient of $H_{x|x'}$, it is enough to focus attention on $\ell$-primary parts for a prime $\ell$ dividing $|H_{x|x'}|$ (so $\ell \neq p$). More specifically, if $G$ is an finite $\ell$-group that is either cyclic or a product of two cyclic groups, and $\psi_0, \psi_1 : G \to \mathbf{Z}/\ell^n\mathbf{Z}$ are homomorphisms such that $\psi_0 \times \psi_1$ is injective (*i.e.*, $\ker(\psi_0) \cap \ker(\psi_1) = \{1\}$), then we claim that the $\psi_j^{\kappa_{1-j}}$'s factor as faithful characters on a common quotient of $G$, where $\kappa_j = |\ker(\psi_j)|$. If one of the $\psi_j$'s is faithful (or equivalently, if the $\ell$-group $G$ is cyclic), this is clear. This settles the case in which $G$ is cyclic, so we may assume $G$ is a product of two non-trivial cyclic $\ell$-groups and that both $\psi_j$'s have non-trivial kernel. Since the $\ell$-torsion subgroups $\ker(\psi_j)[\ell]$ must be non-trivial with trivial intersection, these must be distinct lines spanning $G[\ell]$. Passing to group $G/G[\ell]$ and the characters $\psi_j^{\ell}$ therefore permits us to induct on $|G|$. □

By the lemma, we conclude that the characters $\chi_1' = \chi_1^{\kappa_2}$ and $\chi_2' = \chi_1^{\kappa_1}$ both factor faithfully through a common (cyclic) quotient $H'_{x|x'}$ of $H_{x|x'}$. Define $t_1' = t_1^{\kappa_2}$ and $t_2' = t_2^{\kappa_1}$. Since formation of $H_{x|x'}$-invariants commutes with passage to quotients on $\widehat{\mathcal{O}_{S,s}^{\text{sh}}}$-modules, Lemma 2.3.4 shows that in order to compute the $H_{x|x'}$-invariants of $\widehat{\mathcal{O}}_{X',x'}^{\text{sh}}$ it suffices to compute invariants on the level of $\widehat{\mathcal{O}_{S,s}^{\text{sh}}}[\![t_1, t_2]\!]$ and then pass to a quotient. The subalgebra of invariants in $\widehat{\mathcal{O}_{S,s}^{\text{sh}}}[\![t_1, t_2]\!]$ under the subgroup generated by $\ker(\chi_1)$ and $\ker(\chi_2)$ is $\widehat{\mathcal{O}_{S,s}^{\text{sh}}}[\![t_1', t_2']\!]$, and $H_{x|x'}$ acts on this subalgebra through the quotient $H'_{x|x'}$ via the characters $\chi_1'$ and $\chi_2'$. Letting $m_1' = m_1/\kappa_2$ and $m_2' = m_2/\kappa_1$ (so $m_2' = 0$ in the case of one analytic branch), we obtain the description

$$\widehat{\mathcal{O}^{\mathrm{sh}}_{X',x'}} = (\widehat{\mathcal{O}^{\mathrm{sh}}_{S,s}}[\![t'_1, t'_2]\!]/({t'_1}^{m'_1}{t'_2}^{m'_2} - \pi_s))^{H'_{x|x'}} \tag{2.3.4}$$

Obviously $\chi'_2 = {\chi'_1}^{r_{x|x'}}$ for a unique $r_{x|x'} \in (\mathbf{Z}/|H'_{x|x'}|\mathbf{Z})^\times$, as the characters $\chi'_j$ are both faithful on $H'_{x|x'}$.

Since $|H'_{x|x'}|$ and $r_{x|x'} \in (\mathbf{Z}/|H'_{x|x'}|\mathbf{Z})^\times$ are intrinsic to $x' \in X' = X/H$ and do not depend on $x$ (or on a choice of $k(x)_{\mathrm{sep}}$), we may denote these two integers $n_{x'}$ and $r_{x'}$ respectively. We have $m'_1 + m'_2 r'_{x'} \equiv 0 \bmod n_{x'}$ since $1 = {\chi'_1}^{m'_1}{\chi'_2}^{m'_2} = {\chi'_1}^{m'_1+m'_2 r_{x'}}$ with $\chi'_1$ faithful. Theorem 2.3.9 below shows that $n_{x'} > 1$, since $x'$ is the non-regular.

If $S$ were a smooth curve over $\mathbf{C}$, then the setup in (2.3.4) would be the classical cyclic surface quotient-singularity situation whose minimal regular resolution is most readily computed via toric varieties. That case motivates what to expect for minimal regular resolutions with more general $S$ in §2.4, but rather than delve into a relative theory of toric varieties we can just use the classical case as a guide.

To define the class of singularities we shall resolve, let $X'_{/S}$ now be a *normal* (not necessarily connected) curve over a connected Dedekind scheme $S$. Assume moreover that either $S$ is excellent or that $X'_{/S}$ has smooth generic fiber, so there are only finitely many non-regular points (all closed in closed fibers). Consider a closed point $s \in S$ with residue characteristic $p \geq 0$, and pick a closed point $x' \in X'_s$ such that $X'_s$ has one or two (geometric) analytic branches at $x'$.

Definition 2.3.6. We say that a closed point $x'$ in a closed fiber $X'_s$ is a *tame cyclic quotient singularity* if there exists a positive integer $n > 1$ not divisible by $p = \mathrm{char}(k(s))$, a unit $r \in (\mathbf{Z}/n\mathbf{Z})^\times$, and integers $m'_1 > 0$ and $m'_2 \geq 0$ satisfying $m'_1 \equiv -rm'_2 \bmod n$ such that $\widehat{\mathcal{O}^{\mathrm{sh}}_{X',x'}}$ is isomorphic to the subalgebra of $\mu_n(k(s)_{\mathrm{sep}})$-invariants in $\widehat{\mathcal{O}^{\mathrm{sh}}_{S,s}}[\![t'_1, t'_2]\!]/({t'_1}^{m'_1}{t'_2}^{m'_2} - \pi_s)$ under the action $t'_1 \mapsto \zeta t'_1$, $t'_2 \mapsto \zeta^r t'_2$.

*Remark* 2.3.7. Note that when $X'_{/S}$ has a tame cyclic quotient singularity at $x' \in X'_s$, then $k(x')/k(s)$ is separable and $x'$ is non-regular (by Theorem 2.3.9 below). Also, it is easy to check that the exponents $m'_1$ and $m'_2$ are necessarily the analytic branch multiplicities at $x'$. Note that the data of $n$ and $r$ is merely part of a presentation of $\widehat{\mathcal{O}}_{X',x'}$ as a ring of invariants, so it is not clear *a priori* that $n$ and $r$ are intrinsic to $x' \in X'$. The fact that $n$ and $r$ are uniquely determined by $x'$ follows from Theorem 2.4.1 below, where we show that $n$ and $r$ arise from the structure of the minimal regular resolution of $X'$ at $x'$.

Using notation as in the preceding global considerations, there is a very simple criterion for a nil-semistable $x' \in X/H$ to be a non-regular point: there should not be a line in $T_x(X)$ on which the inertia group $H_{x|x'}$ acts trivially. To prove this, we recall Serre's pseudo-reflection theorem [57, Thm. 1′]. This requires a definition:

Definition 2.3.8. Let $V$ be a finite-dimensional vector space over a field $k$. An element $\sigma$ of $\mathrm{Aut}_k(V)$ is called a *pseudo-reflection* if $\mathrm{rank}(1-\sigma) \leq 1$.

Theorem 2.3.9 (Serre). *Let $A$ be a noetherian regular local ring with maximal ideal $\mathfrak{m}$ and residue field $k$. Let $G$ be a finite subgroup of $\mathrm{Aut}(A)$, and let $A^G$ denote the local ring of $G$-invariants of $A$. Suppose that:*

1. *The characteristic of $k$ does not divide the order of $G$,*
2. *$G$ acts trivially on $k$, and*
3. *$A$ is a finitely generated $A^G$-module.*

*Then $A^G$ is regular if and only if the image of $G$ in $\mathrm{Aut}_k(\mathfrak{m}/\mathfrak{m}^2)$ is generated by pseudo-reflections.*

*In fact, the "only if" implication is true without hypotheses on the order of $G$, provided $A^G$ has residue field $k$ (which is automatic when $k$ is algebraically closed).*

*Remark* 2.3.10. By Theorem 3.7($i$) of [44] with $B = A$ and $A = A^G$, hypothesis 3 of Serre's theorem forces $A^G$ to be noetherian. Serre's theorem ensures that $x'$ as in Definition 2.3.6 is necessarily non-regular.

*Proof.* Since this result is not included in Serre's Collected Works, we note that a proof of the "if and only if" assertion can be found in [68, Cor. 2.13, Prop. 2.15]. The proof of the "only if" implication in [68] works without any conditions on the order of $G$ as long as one knows that $A^G$ has the same residue field as $A$. Such equality is automatic when $k$ is algebraically closed. Indeed, the case of characteristic 0 is clear, and for positive characteristic we note that $k$ is a priori finite over the residue field of $A^G$, so if equality were to fail then the residue field of $A^G$ would be of positive characteristic with algebraic closure a finite extension of degree $> 1$, an impossibility by Artin-Schreier.

To see why everything still works without restriction on the order of $G$ when we assume $A^G$ is regular, note first that regularity of $A^G$ ensures that $A^G \to A$ must be finite free, so even without a Reynolds operator we still have $(A \otimes_{A^G} A)^G = A$, where $G$ acts on the left tensor factor. Hence, the proof of [68, Lemma 2.5] still works. Meanwhile, equality of residue fields for $A^G$ and $A$ makes the proof of [68, Prop. 2.6] still work, and then one easily checks that the proofs of [68, Thm. 2.8, Prop. 2.15($i$)⇒($ii$)] go through unchanged. □

The point of the preceding study is that in a *global* quotient situation $X' = X/H$ as considered above, one always has a tame cyclic quotient singularity at the image $x'$ of a nil-semistable point $x \in X_s$ when $x'$ is not regular (by Lemma 2.3.3, both $k(x)$ and $k(x')$ are automatically separable over $k(s)$ when such non-regularity holds). Thus, when computing complete local rings at geometric closed points on a coarse modular curve (in residue characteristic

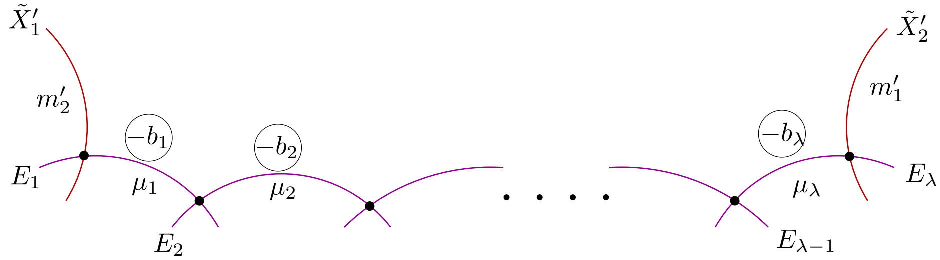


Figure 1: Minimal regular resolution of $x'$

$> 3$), we will naturally encounter a situation such as in Definition 2.3.6. The ability to explicitly (minimally) resolve tame cyclic quotient singularities in general will therefore have immediate applications to modular curves.

### 2.4 Jung–Hirzebruch resolution

As we noted in Remark 2.3.7, it is natural to ask whether the numerical data of $n$ and $r \in (\mathbf{Z}/n\mathbf{Z})^\times$ in Definition 2.3.6 are intrinsic to $x' \in X'$. We shall see in the next theorem that this data is intrinsic, as it can be read off from the minimal regular resolution over $x'$.

Theorem 2.4.1. *Let $X'_{/S}$ be a normal curve over a local Dedekind base $S$ with closed point $s$. Assume either that $S$ is excellent or that $X'_{/S}$ has smooth generic fiber. Assume $X'$ has a tame cyclic quotient singularity at a closed point $x' \in X'_s$ with parameters $n$ and $r$ (in the sense of Definition 2.3.6), where we represent $r \in (\mathbf{Z}/n\mathbf{Z})^\times$ by the unique integer $r$ satisfying $1 \leq r < n$ and $\gcd(r, n) = 1$. Finally, assume either that $k(s)$ is separably closed or that all connected components of the regular compactification $\overline{X}'_K$ of the regular generic-fiber curve $X'_K$ have positive arithmetic genus.*

*Consider the Jung–Hirzebruch continued fraction expansion*

$$\frac{n}{r} = b_1 - \cfrac{1}{b_2 - \cfrac{1}{\cdots - \cfrac{1}{b_\lambda}}} \tag{2.4.1}$$

*with integers $b_j \geq 2$ for all $j$.*

*The minimal regular resolution of $X'$ along $x'$ has fiber over $k(x')_{\mathrm{sep}}$ whose underlying reduced scheme looks like the chain of $E_j$'s as shown in Figure 1, where:*

- *all intersections are transverse, with $E_j \simeq \mathbf{P}^1_{k(x')_{\mathrm{sep}}}$;*
- *$E_j.E_j = -b_j < -1$ for all $j$;*

- $E_1$ *is transverse to the strict transform* $\widetilde{X}'_1$ *of the global algebraic irreducible component* $X'_1$ *through* $x'$ *with multiplicity* $m'_2$ *(along which* $t'_1$ *is a cotangent direction), and similarly for* $E_\lambda$ *and the component* $\widetilde{X}'_2$ *with multiplicity* $m'_1$ *in the case of two analytic branches.*

*Remark* 2.4.2. The case $X'_2 = X'_1$ can happen, and there is no $\widetilde{X}'_1$ in case of one analytic branch (*i.e.*, in case $m'_2 = 0$).

We will also need to know the multiplicities $\mu_j$ of the components $E_j$ in Figure 1, but this will be easier to give after we have proved Theorem 2.4.1; see Corollary 2.4.3.

The labelling of the $E_j$'s indicates the order in which they arise in the resolution process, with each "new" $E_j$ linking the preceding ones to the rest of the closed fiber in the case of one initial analytic branch. Keeping this picture in mind, we see that it is always the strict transform $\widetilde{X}'_2$ of the initial component with formal parameter $t'_2$ that occurs at the end of the chain, and this is the component whose multiplicity is $m'_1$.

*Proof.* We may assume $S$ is local, and if $S$ is not already excellent then (by hypothesis) $X'_K$ is smooth and all connected components of its regular compactification have positive arithmetic genus. We claim that this positivity assumption is preserved by extension of the fraction field $K$. That is, if $\overline{C}$ is a connected regular proper curve over a field $k$ with $\mathrm{H}^1(\overline{C}, \mathcal{O}_{\overline{C}}) \neq 0$ and $C$ is a dense open in $\overline{C}$ that is $k$-smooth, then for any extension $k'/k$ we claim that all connected components $C'_i$ of the regular $k'$-curve $C' = C_{/k'}$ have compactification $\overline{C}'_i$ with $\mathrm{H}^1(\overline{C}'_i, \mathcal{O}_{\overline{C}'_i}) \neq 0$. Since the field $\mathrm{H}^0(\overline{C}, \mathcal{O}_{\overline{C}})$ is clearly finite separable over $k$, by using Stein factorization for $\overline{C}$ we may assume $\overline{C}$ is geometrically connected over $k$. Thus, $\overline{C}' = \overline{C}_{/k'}$ is a connected proper $k'$-curve with $\mathrm{H}^1(\overline{C}', \mathcal{O}_{\overline{C}'}) \neq 0$ and there is a dense open $C'$ that is $k'$-smooth, and we want to show that the normalization of $\overline{C}'_{\mathrm{red}}$ has positive arithmetic genus. Since $\overline{C}'$ is generically reduced, the map from $\mathcal{O}_{\overline{C}'}$ to the normalization sheaf of $\mathcal{O}_{\overline{C}'_{\mathrm{red}}}$ has kernel and cokernel supported in dimension 0, and so the map on $\mathrm{H}^1$'s is an isomorphism. Thus, the normalization of $\overline{C}'_{\mathrm{red}}$ indeed has positive arithmetic genus.

We conclude that Lemma 2.1.1 and the base-change compatibility of Definition 2.2.3 (via Theorem 2.2.2) permit us to base-change to $\widehat{\mathcal{O}}_{S,s}$ without losing any hypotheses. Thus, we may assume $S = \operatorname{Spec} W$ with $W$ a complete (hence excellent) discrete valuation ring. This brings us to the excellent case with all connected components of the regular compactification of $X'_K$ having positive arithmetic genus when the residue field is not separably closed. If in addition $k(s)$ is not separably closed, then we claim that base-change to $\operatorname{Spec} W^{\mathrm{sh}}$ preserves all hypotheses, and so we can always get to the case of a separably closed residue field (in particular, we get to the case with $k(x')$ separably closed); see [24, p. 17] for a proof that strict henselization preserves excellence. We need to show that base change to $W^{\mathrm{sh}}$ commutes with the formation of the minimal regular resolution. This is a refinement on Theorem 2.2.2 because such base change is generally not residually trivial.

From the proof of Theorem 2.2.2 in the excellent case, we see that if $X' \hookrightarrow \overline{X}'$ is a Nagata compactification then the minimal resolution $X \to X'$ of $X'$ is the part of the minimal regular resolution of $\overline{X}'$ that lies over $X'$. Hence, the base-change problem for $W \to W^{\mathrm{sh}}$ is reduced to the proper case. We may assume that $X'$ is connected, so $\widetilde{W} = \mathrm{H}^0(X', \mathcal{O}_{X'})$ is a complete discrete valuation ring finite over $W$. Hence, $\widetilde{W}^{\mathrm{sh}} \simeq \widetilde{W} \otimes_W W^{\mathrm{sh}}$, so we may reduce to the case when $X' \to \operatorname{Spec} W$ is its own Stein factorization. In this proper case, the positivity condition on the arithmetic genus of the generic fiber allows us to use [41, 9/3.28] (which rests on a dualizing-sheaf criterion for minimality) to conclude that formation of the minimal regular resolution of $X'$ is compatible with étale localization on $W$. A standard direct limit argument that chases the property of having a $-1$-curve in a fiber over $X'$ thereby shows that the formation of the minimal regular resolution is compatible with ind-étale base change (such as $W \to W^{\mathrm{sh}}$). Thus, we may finally assume that $W$ is excellent and has a separably closed residue field, and so we no longer need to impose a positivity condition on arithmetic genera of the connected components of the generic-fiber regular compactification.

The intrinsic numerical data for the *unique* minimal resolution (that is, the self-intersection numbers and multiplicities of components in the exceptional divisor for this resolution) may be computed in an étale neighborhood of $x'$, by Corollary 2.2.4 and Remark 2.2.5, and the Artin approximation theorem is the ideal tool for finding a convenient étale neighborhood in which to do such a calculation. We will use the Artin approximation theorem to construct a special case that admits an étale neighborhood that is also an étale neighborhood of our given $x'$, and so it will be enough to carry out the resolution in the special case. The absence of a good theory of minimal regular resolutions for complete 2-dimensional local noetherian rings prevents us from carrying out a proof entirely on $\widehat{\mathcal{O}}_{X',x'}$, and so forces us to use the Artin approximation theorem. It is perhaps worth noting at the outset that the reason we have to use Artin approximation is that the resolution process to be used in the special case will not be intrinsic (we blow up certain codimension-1 subschemes that depend on coordinates).

Here is the special case that we wish to analyze. Let $n > 1$ be a positive integer that is a unit in $W$, and choose $1 \le r < n$ with $\gcd(r, n) = 1$. Pick integers $m_1 \ge 1$ and $m_2 \ge 0$ satisfying $m_1 \equiv -rm_2 \bmod n$. For technical reasons, we do not require either of the $m_j$'s to be units in $W$. To motivate things, let us temporarily assume that the residue field $k$ of $W$ contains a full set of $n$th roots of unity. Let $\mu_n(k)$ act on the *regular domain* $A = W[t_1, t_2]/(t_1^{m_1} t_2^{m_2} - \pi)$ via

$$[\zeta](t_1) = \zeta t_1, \;\; [\zeta](t_2) = \zeta^r t_2. \tag{2.4.2}$$

Since the $\mu_n(k)$-action in (2.4.2) is clearly free away from $t_1 = t_2 = \pi = 0$, the quotient

$$Z = (\mathrm{Spec}(A))/\mu_n(k) = \mathrm{Spec}(B)$$

(with $B = A^{\mu_n(k)}$) is normal and also is regular away from the image point $z \in Z$ of $t_1 = t_2 = \pi = 0$.

To connect up the special situation $(Z, z)$ and the tame cyclic quotient singularity $x' \in X'_{/S}$, note that Lemma 2.3.4 shows that our situation is formally isomorphic to the algebraic $Z = \mathrm{Spec}(B)$ for a suitable such $B$ and $n \in W^\times$. By the Artin approximation theorem, there is a common (residually trivial) connected étale neighborhood $(U, u)$ of $(Z, z)$ and $(X', x')$. That is, there is a pointed connected affine $W$-scheme $U = \mathrm{Spec}(A)$ that is a residually-trivial étale neighborhood of $x'$ and of $z$. In particular, $U$ is a connected normal $W$-curve. We can assume that $u$ is the only point of $U$ over $z$, and also the only point of $U$ over $x'$. Keep in mind (*e.g.*, if $\gcd(m_1, m_2) > 1$) that the field $K$ might not be separably closed in the function fields of $U$ or $Z$, so the generic fibers of $U$ and $Z = \mathrm{Spec}(B)$ over $W$ might not be geometrically connected and $U$ is certainly not proper over $W$ in general.

The étale-local nature of the minimal regular resolution, as provided by Corollary 2.2.4 and Remark 2.2.5, implies that the minimal regular resolutions of $(X', x')$ and $(Z, z)$ have pullbacks to $(U, u)$ that coincide with the minimal regular resolution of $U$ along $\{u\}$. The fibers over $u, x', z$ are all the same due to residual-triviality, so the geometry of the resolution fiber at $x'$ is the same as that over $z$. Hence, we shall compute the minimal regular resolution $Z' \to Z$ at $z$, and will see that the fiber of $Z'$ over $z$ is as in Figure 1.

Let us now study $(Z, z)$. Since $n$ is a unit in $W$, the normal domain $B = A^{\mu_n(k)}$ is a quotient of $W[t_1, t_2]^{\mu_n(k)}$ via the natural map. Since the action of $\mu_n(k)$ as in (2.4.2) sends each monomial $t_1^{e_1} t_2^{e_2}$ to a constant multiple of itself, the ring of invariants $W[t_1, t_2]^{\mu_n(k)}$ is spanned over $W$ by the invariant monomials. Clearly $t_1^{e_1} t_2^{e_2}$ is $\mu_n(k)$-invariant if and only if $e_1 + r e_2 = nf$ for some integer $f$ (so $e_2 \le (n/r)f$), in which case $t_1^{e_1} t_2^{e_2} = u^f v^{e_2}$, where $u = t_1^n$ and $v = t_2/t_1^r$ are $\mu_n(k)$-invariant elements in the fraction field of $W[t_1, t_2]$. Note that even though $v$ does not lie in $W[t_1, t_2]$, for any pair of integers $i, j$ satisfying $0 \le j \le (n/r)i$ we have $u^i v^j \in W[t_1, t_2]$ and

$$W[t_1, t_2]^{\mu_n(k)} = \bigoplus_{0 \le j \le (n/r)i} W u^i v^j.$$

We have $t_1^{m_1} t_2^{m_2} = u^\mu v^{m_2}$ with $m_1 + r m_2 = n\mu$ (so $m_2 \le (n/r)\mu$). Thus,

$$B = \frac{\bigoplus_{0 \le j \le (n/r)i} W u^i v^j}{(u^\mu v^{m_2} - \pi)}. \tag{2.4.3}$$

Observe that (2.4.3) makes sense as a definition of finite-type $W$-algebra, without requiring $n$ to be a unit and without requiring that $k$ contain any non-trivial roots of unity. It is clear that (2.4.3) is $W$-flat, as it has a $W$-module basis given by monomials $u^i v^j$ with $0 \le j \le (n/r)i$ and either $i < \mu$ or $j < m_2$. It is less evident if (2.4.3) is normal for any $n$, but we do not need this fact. We will inductively compute certain blow-ups on (2.4.3) *without restriction on* $n$ or on the residue field, and the process will end at a resolution of singularities for $\operatorname{Spec} B$.

Before we get to the blowing-up, we shall show that $\operatorname{Spec} B$ is a $W$-curve and we will infer some properties of its closed fiber. Note that the map $K(u,v) \to K(t_1,t_2)$ defined by $u \mapsto t_1^n$, $v \mapsto t_2/t_1^r$ induces a $W$-algebra injection

$$\bigoplus_{0\le j\le (n/r)i} Wu^i v^j \to W[t_1,t_2] \tag{2.4.4}$$

that is *finite* because $t_1^n = u$ and $t_2^n = u^r v^n$. Thus, the left side of (2.4.4) is a 3-dimensional noetherian domain and passing to the quotient by $u^\mu v^{m_2} - \pi = t_1^{m_1} t_2^{m_2} - \pi$ yields a finite surjection

$$\operatorname{Spec}(W[t_1,t_2]/(t_1^{m_1}t_2^{m_2} - \pi)) \to \operatorname{Spec}(B). \tag{2.4.5}$$

Passing to the generic fiber and recalling that $B$ is $W$-flat, we infer that $\operatorname{Spec}(B)$ is a $W$-curve with irreducible generic fiber, so $\operatorname{Spec}(B)$ is 2-dimensional and connected. We also have a finite surjection modulo $\pi$,

$$\operatorname{Spec}(k[t_1,t_2]/(t_1^{m_1}t_2^{m_2})) \to \operatorname{Spec}(B/\pi), \tag{2.4.6}$$

so the closed fiber of $\operatorname{Spec}(B)$ consists of at most two irreducible components (or just one when $m_2 = 0$), to be called the images of the $t_1$-axis and $t_2$-axis (where we omit mention of the $t_1$-axis when $m_2 = 0$). Since the $t_2$-axis is the preimage of the zero-scheme of $u = t_1^n$ under (2.4.6), we conclude that when $m_2 > 0$ the closed fiber $\operatorname{Spec}(B/\pi)$ does have two distinct irreducible components.

Inspired by the case of toric varieties, we will now compute the blow-up $Z'$ of the $W$-flat $Z = \operatorname{Spec}(B)$ along the ideal $(u, uv)$. Since

$$\operatorname{Spec}(W[t_1,t_2]/(t_1^{m_1}t_2^{m_2} - \pi, t_1^n, t_1^{n-r}t_2)) \to \operatorname{Spec}(B/(u,uv))$$

is a finite surjection and the source is supported in the $t_2$-axis of the closed fiber over $\operatorname{Spec}(W)$, it follows that $\operatorname{Spec}(B/(u,uv))$ is supported in the image of the $t_2$-axis of the closed fiber of $\operatorname{Spec}(B)$ over $\operatorname{Spec}(W)$. In particular, blowing up $Z$ along $(u,uv)$ does not affect the generic fiber of $Z$ over $W$. Since $Z$ is $W$-flat, it follows that the proper blow-up map $Z' \to Z$ is surjective.

There are two charts covering $Z'$, $D_+(u)$ and $D_+(uv)$, where we adjoin the ratios $uv/u = v$ and $u/uv = 1/v$ respectively. Thus,

$$D_+(u) = \operatorname{Spec}(B[v]) = \operatorname{Spec}(W[u,v]/(u^\mu v^{m_2} - \pi))$$

is visibly regular and connected, and $D_+(uv) = \operatorname{Spec}(B[1/v])$ with

$$B[1/v] = \frac{\bigoplus_{j\le (n/r)i,\, 0\le i} Wu^i v^j}{(u^\mu v^{m_2} - \pi)}.$$

We need to rewrite this latter expression in terms of a more useful set of variables. We begin by writing (as one does when computing the Jung–Hirzebruch continued fraction for $n/r$)

$$n = b_1 r - r'$$

with $b_1 \geq 2$ and either $r = 1$ with $r' = 0$ or else $r' > 0$ with $\gcd(r, r') = 1$ (since $\gcd(n, r) = 1$). We will first treat the case $r' = 0$ (proving that $B[1/v]$ is also regular) and then we will treat the case $r' > 0$. Note that there is no reason to expect that $p$ cannot divide $r$ or $r'$, even if $p \nmid n$, and it is for this reason that we had to recast the definition of $B$ in a form that avoids the assumption that $n$ is a unit in $W$. For similar reasons, we must avoid assuming $m_1$ or $m_2$ is a unit in $W$.

Assume $r' = 0$, so $r = 1$, $b_1 = n$, and $b_1\mu - m_2 = m_1$. Let $i' = b_1 i - j$ and $j' = i$, so $i'$ and $j'$ vary precisely over non-negative integers and $u^i v^j = (1/v)^{i'} (uv^{b_1})^{j'}$. Thus, letting $u' = 1/v$ and $v' = uv^{b_1}$ yields

$$B[1/v] = W[u', v']/({u'}^{b_1\mu - m_2} {v'}^{\mu} - \pi) = W[u', v']/({u'}^{m_1} {v'}^{\mu} - \pi),$$

which is regular. In the closed fiber of $Z' = \mathrm{Bl}_{(u,uv)}(Z)$ over $\mathrm{Spec}(W)$, let $D_1$ denote the $v'$-axis in $D_+(uv) = \mathrm{Spec}\, B[1/v]$ and when $m_2 > 0$ let $D_2$ denote the $u$-axis in $D_+(u)$. The multiplicities of $D_1$ and $D_2$ in $Z'_k$ are respectively $m_1 = b_1\mu - m_2$ and $m_2$ (with multiplicity $m_2 = 0$ being a device for recording that there is no $D_2$). The exceptional divisor $E$ is a projective line over $k$ (with multiplicity $\mu$ and gluing data $u' = 1/v$) and hence the uniformizer $\pi$ has divisor on $Z' = \mathrm{Bl}_{(u,uv)}(Z)$ given by

$$\mathrm{div}_{Z'}(\pi) = (b_1\mu - m_2)D_1 + \mu E + m_2 D_2 = m_1 D_1 + \mu E + m_2 D_2$$

(when $m_2 = 0$, the final term really is omitted).

It is readily checked that the $D_j$'s each meet $E$ transversally at a single $k$-rational point (suppressing $D_2$ when $m_2 = 0$). The intersection product $\mathrm{div}_{Z'}(\pi).E$ makes sense since $E$ is proper over $k$, even though $Z$ is not proper over $W$, and it must vanish because $\mathrm{div}_{Z'}(\pi)$ is principal, so by additivity of intersection products in the first variable (restricted to effective Cartier divisors for a fixed proper second variable such as $E$) we have

$$0 = \mathrm{div}_{Z'}(\pi).E = b_1\mu - m_2 + \mu(E.E) + m_2.$$

Thus, $E.E = -b_1$.

Now assume $r' > 0$. Since $n = b_1 r - r'$, the condition $0 \leq j \leq (n/r)i$ can be rewritten as $0 \leq i \leq (r/r')(b_1 i - j)$. Letting $j' = i$ and $i' = b_1 i - j$, we have $u^i v^j = {u'}^{i'} {v'}^{j'}$ with $u' = 1/v$ and $v' = uv^{b_1}$. In particular, $u^\mu v^{m_2} = {u'}^{b_1\mu - m_2} {v'}^{\mu}$. Thus,

$$B[1/v] = \frac{\bigoplus_{0 \leq j' \leq (r/r')i'} W {u'}^{i'} {v'}^{j'}}{({u'}^{b_1\mu - m_2} {v'}^{\mu} - \pi)}. \tag{2.4.7}$$

Note the similarity between (2.4.3) and (2.4.7) up to modification of parameters: replace $(n, r, m_1, m_2, \mu)$ with $(r, r', m_1, \mu, b_1\mu - m_2)$. The blow-up along $(u', u'v')$ therefore has closed fiber over $\mathrm{Spec}(W)$ with the following irreducible components: the $v'$-axis $D_1$ in $D_+(uv)$ with multiplicity $b_1\mu - m_2$, the $u$-axis $D_2$ in $D_+(u)$ with multiplicity $m_2$ (so this only shows up when $m_2 > 0$), and the exceptional divisor $E$ that is a projective line (via gluing $u' = 1/v$) having multiplicity $\mu$ and meeting $D_1$ (as well as $D_2$ when $m_2 > 0$) transversally at a single $k$-rational point. We will focus our attention on $D_+(uv)$ (as we have already seen that the other chart $D_+(u)$ is regular), and in particular we are interested in the "origin" in the closed fiber of $D_+(uv)$ over $\mathrm{Spec}(W)$ where the projective line $E$ meets $D_1$; near this origin, $D_+(uv)$ is an affine open that is given by the spectrum of (2.4.7).

If $r$ were also a unit in $W$ then $D_+(uv)$ would be the spectrum of the ring of $\mu_r(k)$-invariants in $W[t'_1, t'_2]/({t'_1}^{m_1}{t'_2}^{\mu} - \pi)$ with the action $[\zeta](t'_1) = \zeta t'_1$ and $[\zeta](t'_1) = \zeta^{r'} t'_2$ (this identification uses the identity $m_1 + r'\mu = r(b_1\mu - m_2)$), and without any restriction on $r$ we at least see that (2.4.7) is an instance of the general (2.4.3) and that there is a natural finite surjection

$$\mathrm{Spec}(k[t'_1, t'_2]/({t'_1}^{m_1}{t'_2}^{\mu})) \to D_+(uv)_k.$$

On $D_+(uv)_k$, the component $E$ of multiplicity $\mu$ is the image of the $t'_1$-axis and the component $D_1$ with multiplicity $m_1$ is the image of the $t'_2$-axis. As a motivation for what follows, note also that if $r \in W^\times$ then since $r > 1$ we see that the "origin" in $D_+(uv)_k$ is necessarily a non-regular point in the total space over $\mathrm{Spec}(W)$ (by Serre's Theorem 2.3.9).

We conclude (without requiring any of our integer parameters to be units in $W$) that if we make the change of parameters

$$(n, r, m_1, m_2, \mu) \rightsquigarrow (r, r', m_1, \mu, b_1\mu - m_2) \tag{2.4.8}$$

then $D_+(uv)$ is like the original situation (2.4.3) with a revised set of initial parameters. In particular, $n$ is replaced by the strictly smaller $r > 1$, so the process will eventually end. Moreover, since $\mu > 0$ we see that the case $m_2 = 0$ is now "promoted" to the case $m_2 > 0$. When we make the blow-up at the origin in $D_+(uv)_k$, the strict transform $E_1$ of $E$ plays the same role that $D_2$ played above, so $E_1$ is entirely in the regular locus and the new exceptional divisor $E'$ has multiplicity $b_1\mu - m_2$ (this parameter plays the role for the second blow-up that $\mu$ played for the first blow-up, as one sees by inspecting our change of parameters in (2.4.8)).

As the process continues, nothing more will change around $E_1$, so inductively we conclude from the descriptions of the regular charts that the process ends at a regular connected $W$-curve with closed-fiber Weil divisor

$$\cdots + (b_1\mu - m_2)E' + \mu E_1 + m_2 D_2 + \dots \tag{2.4.9}$$

(where we have abused notation by writing $E'$ to denote the strict transform of $E'$ in the final resolution, and this strict transform clearly has generic multiplicity $b_1\mu - m_2$). The omitted terms in (2.4.9) do not meet $E_1$, so we may form the intersection against $E_1$ to solve

$$0 = (b_1\mu - m_2) + \mu(E_1.E_1) + m_2$$

just as in the case $r' = 0$ (*i.e.*, $r = 1$), so $E_1.E_1 = -b_1$. Since

$$\frac{n}{r} = b_1 - \frac{1}{r/r'},$$

by induction on the length of the continued fraction we reach a regular resolution in the expected manner, with $E_j.E_j = -b_j$ for all $j$ and the final resolution having fiber over $z \in Z$ looking exactly like in Figure 1. Note also that each new blow-up separates all of the previous exceptional lines from the (strict transform of the initial) component through $z$ with multiplicity $m_1$. Since $-b_j \leq -2 < -1$ for all $j$, we conclude that at no stage of the blow-up process before the end did we have a regular scheme (otherwise there would be a $-1$-curve in a fiber over the original base $Z$). Thus, we have computed the minimal regular resolution at $z$.

□

We now compute the multiplicity $\mu_j$ in the closed fiber of $X'^{\text{reg}}$ for each fibral component $E_j$ over $x' \in X'$ in Figure 1. In order to compute the $\mu_j$'s, we introduce some notation. Let $n/r > 1$ be a reduced-form fraction with positive integers $n$ and $r$, so we can write

$$n/r = [b_1, b_2, \ldots, b_\lambda]_{\text{JH}} := b_1 - \cfrac{1}{b_2 - \cfrac{1}{\cdots - \cfrac{1}{b_\lambda}}}$$

as a Jung–Hirzebruch continued fraction, where $b_j \geq 2$ for all $j$. Define $P_j = P_j(b_1, \ldots, b_\lambda)$ and $Q_j = Q_j(b_1, \ldots, b_\lambda)$ by

$$P_{-1} = 0,\ \ Q_{-1} = -1,\ \ P_0 = 1,\ \ Q_0 = 0,$$

$$P_j = b_j P_{j-1} - P_{j-2},\ \ Q_j = b_j Q_{j-1} - Q_{j-2}$$

for all $j \geq 1$. Clearly $P_j$ and $Q_j$ are universal polynomials in $b_1, \ldots, b_j$, and by induction $P_j Q_{j-1} - Q_j P_{j-1} = -1$ and $Q_j > Q_{j-1}$ for all $j \geq 0$, so in particular $Q_j > 0$ for all $j > 0$. Thus,

$$[b_1, \ldots, b_\lambda]_{\text{JH}} = \frac{P_\lambda(b_1, \ldots, b_\lambda)}{Q_\lambda(b_1, \ldots, b_\lambda)}$$

makes sense and $P_\lambda/Q_\lambda$ is in reduced form. Thus, $P_\lambda = n$ and $Q_\lambda = r$ since the $Q_j$'s are necessarily positive.

Corollary 2.4.3. *With hypotheses and notation as in Theorem* 2.4.1, *let* $\mu_j$ *denote the multiplicity of* $E_j$ *in the fiber of* ${X'}^{\mathrm{reg}}$ *over* $k(x')_{\mathrm{sep}}$. *The condition* $r = 1$ *happens if and only if* $\lambda = 1$, *in which case* $\mu_1 = (m'_1 + m'_2)/n$.

*If* $r > 1$ (*so* $\lambda > 1$), *then the* $\mu_j$*'s are the unique solution to the equation*

$$\begin{pmatrix} b_1 & -1 & 0 & 0 & \dots & 0 & 0 & 0 \\ -1 & b_2 & -1 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & b_3 & -1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & b_{\lambda-1} & -1 \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 & b_\lambda \end{pmatrix} \begin{pmatrix} \mu_1 \\ \vdots \\ \vdots \\ \mu_\lambda \end{pmatrix} = \begin{pmatrix} m'_2 \\ 0 \\ \vdots \\ 0 \\ m'_1 \end{pmatrix}. \tag{2.4.10}$$

*Keeping the condition* $r > 1$, *define* $P'_j = P_j(b_{\lambda-j+1}, \dots, b_\lambda)$, *so* $P'_\lambda = n$ *and* $P'_{\lambda-1} = Q_\lambda(b_1, \dots, b_\lambda) = r$. *If we let* $\widetilde{m}_2 = P'_{\lambda-1} m'_2 + m'_1 = r m'_2 + m'_1$, *then the* $\mu_j$*'s are also the unique solution to*

$$\begin{pmatrix} P'_\lambda & 0 & 0 & \dots & 0 & 0 & 0 \\ -P'_{\lambda-2} & P'_{\lambda-1} & 0 & \dots & 0 & 0 & 0 \\ 0 & -P'_{\lambda-3} & P'_{\lambda-2} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -P'_1 & P'_2 & 0 \\ 0 & 0 & 0 & \dots & 0 & -1 & P'_1 \end{pmatrix} \begin{pmatrix} \mu_1 \\ \vdots \\ \vdots \\ \mu_\lambda \end{pmatrix} = \begin{pmatrix} \widetilde{m}_2 \\ m'_1 \\ \vdots \\ m'_1 \\ m'_1 \end{pmatrix}. \tag{2.4.11}$$

*In particular,* $\mu_1 = (r m'_2 + m'_1)/n$.

Note that in the applications with $X' = X/H$ as at the beginning of §2.3, the condition $\chi'_1 \neq \chi'_2$ (*i.e.*, $H'_{x|x'}$ does not act through scalars) is equivalent to the condition $r > 1$ in Corollary 2.4.3.

*Proof.* The value of $\mu_1$ when $r = 1$ was established in the proof of Theorem 2.4.1, so now assume $r > 1$. On ${X'}^{\mathrm{reg}}$ (or rather, its base change to $\mathcal{O}^{\mathrm{sh}}_{S,s}$) we have

$$\operatorname{div}(\pi_s) = m'_1 \widetilde{X}'_2 + \sum_{j=1}^{\lambda} \mu_j E_j + m'_2 \widetilde{X}'_1 + \dots \tag{2.4.12}$$

where

- the $\widetilde{X}'_1$-term does not appear if there is only one analytic branch through $x'$ (recall we also set $m'_2 = 0$ in this case),
- the $\widetilde{X}'_j$-terms are a single term when there are two analytic branches but only one global irreducible (geometric) component (in which case $m'_1 = m'_2$),
- the omitted terms "..." on the right side of (2.4.12) are not in the fiber over $x'$ (and in particular do not intersect the $E_j$'s).

Thus, the equations $E_j.\mathrm{div}(\pi_s) = 0$ and the intersection calculations in the proof of Theorem 2.4.1 (as summarized by Figure 1, including transversalities) immediately yield (2.4.10). By solving this system of equations by working up from the bottom row, an easy induction argument yields the reformulation (2.4.11).

□

To prove Theorems 1.1.2 and 1.1.6, the preceding general considerations will provide the necessary intersection-theoretic information on a minimal resolution. To apply Theorem 2.4.1 and Corollary 2.4.3 to the study of singularities at points $x'$ on modular curves, we need to find the value of the parameter $r_{x'}$ in each case. This will be determined by studying universal deformation rings for moduli problems of elliptic curves.

## 3 The Coarse moduli scheme $X_1(p)$

Let $p$ be a prime number. In this section we review the construction of the coarse moduli scheme $X_1(p)$ attached to $\Gamma_1(p)$ in terms of an auxiliary finite étale level structure which exhibits $X_1(p)$ as the compactification of a quotient of a fine moduli scheme. It is the fine moduli schemes whose completed local rings are well understood through deformation theory (as in [34]), and this will provide the starting point for our subsequent calculations of regular models and component groups.

### 3.1 Some general nonsense

As in [34, Ch. 4], for a scheme $T$ we let $(\mathrm{Ell}/T)$ be the category whose objects are elliptic curves over $T$-schemes and whose morphisms are cartesian diagrams. The moduli problem $[\Gamma_1(p)]$ is the contravariant functor $(\mathrm{Ell}) \to (\mathrm{Sets})$ that to an elliptic curve $E_{/S}$ attaches the set of $P \in E(S)$ such that the relative effective Cartier divisor

$$[0] + [P] + [2P] + \cdots + [(p-1)P],$$

viewed as a closed subscheme of $E$, is a closed subgroup scheme. For any moduli problem $\mathcal{P}$ on $(\mathrm{Ell}/T)$ and any object $E_{/S}$ over a $T$-scheme, we define the functor $\mathcal{P}_{E/S}(S') = \mathcal{P}(E_{/S'})$ to classify "$\mathcal{P}$-structures" on base changes of $E_{/S}$. If $\mathcal{P}_{E/S}$ is representable (with some property $\mathbf{P}$ relative to $S$) for every $E_{/S}$, we say that $\mathcal{P}$ is *relatively representable* (with property $\mathbf{P}$). For example, $[\Gamma_1(p)]$ is relatively representable and finite locally free of degree $p^2-1$ on (Ell) for every prime $p$.

For $p \geq 5$, the moduli problem $[\Gamma_1(p)]_{/\mathbf{Z}[1/p]}$ is representable by a smooth affine curve over $\mathbf{Z}[1/p]$ [34, Cor. 2.7.3, Thm. 3.7.1, and Cor. 4.7.1]. For any elliptic curve $E_{/S}$ over an $\mathbf{F}_p$-scheme $S$, the point $P = 0$ is fixed by the automorphism $-1$ of $E_{/S}$, and is in $[\Gamma_1(p)](E/S)$ because $[0]+[P]+\cdots+[(p-1)P]$ is the kernel of the relative Frobenius morphism $F\colon E \to E^{(p)}$. Thus, $[\Gamma_1(p)]_{/\mathbf{Z}_{(p)}}$ is not rigid, so it is not representable.

As there is no fine moduli scheme associated to $[\Gamma_1(p)]_{/\mathbf{Z}_{(p)}}$ for any prime $p$, we let $X_1(p)$ be the compactified coarse moduli scheme $\overline{M}([\Gamma_1(p)]_{/\mathbf{Z}_{(p)}})$, as constructed in [34, Ch. 8]. This is a proper normal $\mathbf{Z}_{(p)}$-model of a smooth and geometrically connected curve $X_1(p)_{/\mathbf{Q}}$, but $X_1(p)$ is usually not regular. Nevertheless, the complete local rings on $X_1(p)$ are computable in terms of abstract deformation theory. Since $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ acts on isomorphism classes of $\Gamma_1(p)$-structures via

$$(E, P) \mapsto (E, a \cdot P) \simeq (E, -a \cdot P),$$

we get a natural action of this group on $X_1(p)$ which is readily checked to be a faithful action (*i.e.*, non-identity elements act non-trivially). Thus, for any subgroup $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ we get the modular curve $X_H(p) = X_1(p)/H$ which is a normal proper connected $\mathbf{Z}_{(p)}$-curve with smooth generic fiber $X_H(p)_{/\mathbf{Q}}$. When $p > 3$, the curve $X_H(p)$ has tame cyclic quotient singularities at its non-regular points.

In order to compute a minimal regular model for these normal curves, we need more information than is provided by abstract deformation theory: we need to keep track of *global* irreducible components on the geometric fiber mod $p$, whereas deformation theory will only tell us about the analytic branches through a point. Fortunately, in the case of modular curves $X_H(p)$, distinct analytic branches through a closed-fiber geometric point always arise from distinct global (geometric) irreducible components through the point. In order to review this fact, as well as to explain the connection between complete local rings on $X_H(p)$ and rings of invariants in universal deformation rings, we need to recall how $X_1(p)$ can be constructed from fine moduli schemes. Let us briefly review the construction process.

Pick a representable moduli problem $\mathcal{P}$ that is finite, étale, and Galois over $(\mathrm{Ell}/\mathbf{Z}_{(p)})$ with Galois group $G_{\mathcal{P}}$, and for which $M(\mathcal{P})$ is affine. For example (cf. [34, §4.5–4.6]) if $\ell \neq p$ is a prime with $\ell \geq 3$, we can take $\mathcal{P}$ to be the moduli problem $[\Gamma(\ell)]_{/\mathbf{Z}_{(p)}}$ that attaches to $E_{/S}$ the set of isomorphisms of $S$-group schemes

$$\phi\colon (\mathbf{Z}/\ell\mathbf{Z})^2_S \simeq E[\ell];$$

the Galois group $G_{\mathcal{P}}$ is $\mathrm{GL}_2(\mathbf{F}_\ell)$. Let $Y_1(p;\mathcal{P})$ be the fine moduli scheme $M([\Gamma_1(p)]_{/\mathbf{Z}_{(p)}}, \mathcal{P})$ that classifies pairs consisting of a $\Gamma_1(p)$-structure and a $\mathcal{P}$-structure on elliptic curves over variable $\mathbf{Z}_{(p)}$-schemes. The scheme $Y_1(p;\mathcal{P})$ is a flat affine $\mathbf{Z}_{(p)}$-curve. Let $Y_1(p)$ be the quotient of $Y_1(p;\mathcal{P})$ by the $G_{\mathcal{P}}$-action.

We introduce the global $\mathcal{P}$ rather than just use formal deformation theory throughout because on characteristic-$p$ fibers we need to retain a connection between closed fiber irreducible components of global modular curves and closed fiber "analytic" irreducible components of formal deformation rings. The precise connection between global $\mathcal{P}$'s and infinitesimal deformation theory is given by the well-known:

THEOREM 3.1.1. *Let $k$ be an algebraically closed field of characteristic $p$ and let $W = W(k)$ be its ring of Witt vectors. Let $z \in Y_1(p)_{/k}$ be a rational point. Let* $\mathrm{Aut}(z)$ *denote the finite group of automorphisms of the (non-canonically unique) $\Gamma_1(p)$-structure over $k$ underlying $z$. Choose a $\mathcal{P}$-structure on the elliptic curve underlying $z$, with $\mathcal{P}$ as above, and let $z' \in Y_1(p;\mathcal{P})(k)$ be the corresponding point over $z$.*

*The ring $\widehat{\mathcal{O}}_{Y_1(p;\mathcal{P})_W,z'}$ is naturally identified with the formal deformation ring of $z$. Under the resulting natural action of* $\mathrm{Aut}(z)$ *on $\widehat{\mathcal{O}}_{Y_1(p;\mathcal{P})_W,z'}$, the subring of* $\mathrm{Aut}(z)$*-invariants is $\widehat{\mathcal{O}}_{Y_1(p)_W,z}$.*

*For any subgroup $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ equipped with its natural action on $Y_1(p)$, the stabilizer $H_{z'|z}$ of $z'$ in $H$ acts faithfully on the universal deformation ring $\widehat{\mathcal{O}}_{Y_1(p;\mathcal{P})_W,z'}$ of $z$ in the natural way, with subring of invariants $\widehat{\mathcal{O}}_{Y_H(p)_W,z}$.*

*Proof.* Since $\mathcal{P}$ is étale and $Y_1(p;\mathcal{P})_W$ is a fine moduli scheme, the interpretation of $\widehat{\mathcal{O}}_{Y_1(p;\mathcal{P})_W,z'}$ as a universal deformation ring is immediate. Since $Y_1(p)_W$ is the quotient of $Y_1(p;\mathcal{P})_W$ by the action of $G_{\mathcal{P}}$, it follows that $\widehat{\mathcal{O}}_{Y_1(p)_W,z}$ is identified with the subring of invariants in $\widehat{\mathcal{O}}_{Y_1(p;\mathcal{P})_W,z'}$ for the action of the stabilizer of $z'$ for the $G_{\mathcal{P}}$-action on $Y_1(p;\mathcal{P})_W$. We need to compute this stabilizer subgroup.

If $z' = (E_z, P_z, \iota)$ with supplementary $\mathcal{P}$-structure $\iota$, then $g \in G_{\mathcal{P}}$ fixes $z'$ if and only if $(E_z, P_z, \iota)$ is isomorphic to $(E_z, P_z, g(\iota))$. This says exactly that there exists an automorphism $\alpha_g$ of $(E_z, P_z)$ carrying $\iota$ to $g(\iota)$, and such $\alpha_g$ is clearly unique if it exists. Moreover, any two $\mathcal{P}$-structures on $E_z$ are related by the action of a unique $g \in G_{\mathcal{P}}$ because of the definition of $G_{\mathcal{P}}$ as the Galois group of $\mathcal{P}$ (and the fact that $z$ is a geometric point). Thus, the stabilizer of $z$ in $G_{\mathcal{P}}$ is naturally identified with $\mathrm{Aut}(E_z, P_z) = \mathrm{Aut}(z)$ (*compatibly* with actions on the universal deformation ring of $z$). The assertion concerning the $H$-action is clear.

□

Since $Y_1(p;\mathcal{P})$ is a regular $\mathbf{Z}_{(p)}$-curve [34, Thm. 5.5.1], it follows that its quotient $Y_1(p)$ is a normal $\mathbf{Z}_{(p)}$-curve. Moreover, by [34, Prop. 8.2.2] the natural map $j : Y_1(p) \to \mathbf{A}^1_{\mathbf{Z}_{(p)}}$ is finite, and hence it is also *flat* [44, 23.1]. In [34], $X_1(p)$ is *defined* to be the normalization of $Y_1(p)$ over the compactified $j$-line $\mathbf{P}^1_{\mathbf{Z}_{(p)}}$. Both $X_1(p)$ and $Y_1(p)$ are independent of the auxiliary choice of $\mathcal{P}$. The complex analytic theory shows that $X_1(p)$ has geometrically connected fibers over $\mathbf{Z}_{(p)}$, so the same is true for $Y_1(p)$ since the complete local rings at the cusps are analytically irreducible mod $p$ (by the discussion in §4.2, especially the self-contained Lemma 4.2.4 and Lemma 4.2.5).

### 3.2 FORMAL PARAMETERS

To do deformation theory computations, we need to recall some canonical formal parameters in deformation rings. Fix an algebraically closed field $k$ of characteristic $p$ and let $W = W(k)$ denote its ring of Witt vectors. Let

$z \in Y_1(p)_{/k}$ be a $k$-rational point corresponding to an elliptic curve $E_{z/k}$ with $\Gamma_1(p)$-structure $P_z$.

For later purposes, it is useful to give a conceptual description of the 1-dimensional "reduced" cotangent space $\mathfrak{m}/(p, \mathfrak{m}^2)$ of $\mathcal{R}_z^0$, or equivalently the cotangent space to the equicharacteristic formal deformation functor of $E_z$:

Theorem 3.2.1. *The cotangent space to the equicharacteristic formal deformation functor of an elliptic curve $E$ over a field $k$ is canonically isomorphic to* $\mathrm{Cot}_0(E)^{\otimes 2}$.

*Proof.* This is just the dual of the Kodaira-Spencer isomorphism. More specifically, the cotangent space is isomorphic to $\mathrm{H}^1(E, (\Omega^1_{E/k})^\vee)^\vee$, and Serre duality identifies this latter space with

$$\mathrm{H}^0(E, (\Omega^1_{E/k})^{\otimes 2}) \xleftarrow{\simeq} \mathrm{H}^0(E, \Omega^1_{E/k})^{\otimes 2} = \mathrm{Cot}_0(E)^{\otimes 2},$$

the first map being an isomorphism since $\Omega^1_{E/k}$ is (non-canonically) trivial. $\square$

Let

$$\mathbf{E}_z \to \mathrm{Spec}(\mathcal{R}_z^0)$$

denote an algebraization of the universal deformation of $E_z$, so non-canonically $\mathcal{R}_z^0 \simeq W[\![t]\!]$ and (by Theorem 3.1.1) there is a unique local $W$-algebra map $\mathcal{R}_z^0 \to \mathcal{R}_z$ to the universal deformation ring $\mathcal{R}_z$ of $(E_z, P_z)$ such that there is a (necessarily unique) isomorphism of deformations between the base change of $\mathbf{E}_z$ over $\mathcal{R}_z$ and the universal elliptic curve underlying the algebraized universal $\Gamma_1(p)$-structure deformation at $z$.

Now make the additional hypothesis $P_z = 0$, so upon choosing a formal coordinate $\underline{x}$ for the formal group of $\mathbf{E}_z$ it makes sense to consider the coordinate

$$x = \underline{x}(\mathbf{P}_z) \in \mathcal{R}_z$$

of the "point" $\mathbf{P}_z$ in the universal $\Gamma_1(p)$-structure over $\mathcal{R}_z$. We thereby get a natural local $W$-algebra map

$$W[\![x, t]\!] \to \mathcal{R}_z. \tag{3.2.1}$$

Theorem 3.2.2. *The natural map* (3.2.1) *is a surjection with kernel generated by an element $f_z$ that is part of a regular system of parameters of the regular local ring $W[\![x, t]\!]$. Moreover, $x$ and $t$ span the* 2*-dimensional cotangent space of the target ring.*

*Proof.* The surjectivity and cotangent-space claims amount to the assertion that an artinian deformation whose $\Gamma_1(p)$-structure vanishes and whose $t$-parameter vanishes necessarily has $p = 0$ in the base ring (so we then have a constant deformation). The vanishing of $p$ in the base ring is [34, 5.3.2.2]. Since the deformation ring $\mathcal{R}_z$ is a 2-dimensional regular local ring, the kernel of the surjection (3.2.1) is a height-1 prime that must therefore be principal with a generator that is part of a regular system of parameters. $\square$

### 3.3 Closed-fiber description

For considerations in Section 5, we will need some more refined information, particularly a description of $f_z \bmod p$ in Theorem 3.2.2. To this end, we first need to recall some specialized moduli problems in characteristic $p$.

Definition 3.3.1. If $E_{/S}$ is an elliptic curve over an $\mathbf{F}_p$-scheme $S$, and $G \hookrightarrow E$ is a finite locally free closed subgroup scheme of order $p$, we shall say that $G$ is a $(1,0)$-*subgroup* if $G$ is the kernel of the relative Frobenius map $F_{E/S} : E \to E^{(p)}$ and $G$ is a $(0,1)$-*subgroup* if the order $p$ group scheme $E[p]/G \hookrightarrow E/G$ is the kernel of the relative Frobenius for the quotient elliptic curve $E/G$ over $S$.

*Remark* 3.3.2. This is a special case of the more general concept of $(a,b)$-*cyclic subgroup* which is developed in [34, §13.4] for describing the mod $p$ fibers of modular curves. On an ordinary elliptic curve over a field of characteristic $p$, an $(a,b)$-cyclic subgroup has connected-étale sequence with connected part of order $p^a$ and étale part of order $p^b$.

Let $\mathcal{P}$ be a representable moduli problem over $(\mathrm{Ell}/\mathbf{Z}_{(p)})$ that is finite, étale, and Galois with $M(\mathcal{P})$ affine (as in §3.1). For $(a,b) = (1,0),(0,1)$, it makes sense to consider the subfunctor

$$[[\Gamma_1(p)]\text{-}(a,b)\text{-cyclic}, \mathcal{P}] \tag{3.3.1}$$

of points of $[\Gamma_1(p)_{/\mathbf{F}_p}, \mathcal{P}]$ whose $\Gamma_1(p)$-structure generates an $(a,b)$-cyclic subgroup. By [34, 13.5.3, 13.5.4], these subfunctors (3.3.1) are represented by closed subschemes of $Y_1(p;\mathcal{P})_{/\mathbf{F}_p}$ that intersect at exactly the supersingular points and have ordinary loci that give a covering of $Y_1(p;\mathcal{P})^{\mathrm{ord}}_{/\mathbf{F}_p}$ by open subschemes. Explicitly, we have an $\mathbf{F}_p$-scheme isomorphism

$$M([\Gamma_1(p)]\text{-}(0,1)\text{-cyclic}, \mathcal{P}) \simeq M([\mathrm{Ig}(p)], \mathcal{P}) \tag{3.3.2}$$

with a smooth (possibly disconnected) Igusa curve, where $[\mathrm{Ig}(p)]$ is the moduli problem that classifies $\mathbf{Z}/p\mathbf{Z}$-generators of the kernel of the relative Verschiebung $V_{E/S} : E^{(p)} \to E$, and the line bundle $\omega$ of relative 1-forms on the universal elliptic curve over $M(\mathcal{P})_{/\mathbf{F}_p}$ provides the description

$$M([\Gamma_1(p)]\text{-}(1,0)\text{-cyclic}, \mathcal{P}) \simeq \mathrm{Spec}((\mathrm{Sym}_{M(\mathcal{P})_{/\mathbf{F}_p}}\omega)/\omega^{\otimes(p-1)}) \tag{3.3.3}$$

as the cover obtained by locally requiring a formal coordinate of the level-$p$ structure to have $(p-1)$th power equal to zero. The scheme (3.3.3) has generic multiplicity $p-1$ and has smooth underlying reduced curve $M(\mathcal{P})_{/\mathbf{F}_p}$.

We conclude that $Y_1(p;\mathcal{P})$ is $\mathbf{Z}_{(p)}$-smooth at points in

$$M([\Gamma_1(p)]\text{-}(0,1)\text{-cyclic}, \mathcal{P})^{\mathrm{ord}},$$

and near points in $M([\Gamma_1(p)]\text{-}(1,0)\text{-cyclic}, \mathcal{P})$ we can use a local trivialization of $\omega$ to find a nilpotent function $X$ with a moduli-theoretic interpretation as the formal coordinate of the point in the $\Gamma_1(p)$-structure (with $X^{p-1}$ arising as $\Phi_p(X+1) \bmod p$ along the ordinary locus). Thus, we get the "ordinary" part of:

Theorem 3.3.3. *Let $k$ be an algebraically closed field of characteristic $p$, and $z \in Y_1(p)_{/k}$ a rational point corresponding to a $(1,0)$-subgroup of an elliptic curve $E$ over $k$. Choose $z' \in Y_1(p;\mathcal{P})_{/k}$ over $z$. Let $f_z$ be a generator of the kernel of the surjection $W[\![x,t]\!] \twoheadrightarrow \widehat{\mathcal{O}}_{Y_1(p;\mathcal{P}),z'}$ in (3.2.1).*

*We can choose $f_z$ so that*

$$f_z \bmod p = \begin{cases} x^{p-1} & \text{if } E \text{ is ordinary,} \\ x^{p-1}t' & \text{if } E \text{ is supersingular,} \end{cases}$$

*with $p, x, t'$ a regular system of parameters in the supersingular case. In particular, $Y_1(p;\mathcal{P})^{\mathrm{red}}_{/k}$ has smooth irreducible components, ordinary double point singularities at supersingular points, and no other non-smooth points.*

The significance of Theorem 3.3.3 for our purposes is that it ensures the regular $\mathbf{Z}_{(p)}$-curve $Y_1(p;\mathcal{P})_{\mathbf{Z}_{(p)}}$ is nil-semistable in the sense of Definition 2.3.1. In particular, for $p > 3$ and any subgroup $H \subseteq (\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$, the modular curve $X_H(p)$ has tame cyclic quotient singularities away from the cusps.

*Proof.* The geometric irreducible components of $Y_1(p,\mathcal{P})^{\mathrm{red}}_{/k}$ are smooth curves (3.3.2) and (3.3.3) that intersect at exactly the supersingular points, and (3.3.3) settles the description of $f_z \bmod p$ in the ordinary case. It remains to verify the description of $f_z \bmod p$ at supersingular points $z$, for once this is checked then the two minimal primes $(x)$ and $(t')$ in the deformation ring at $z$ must correspond to the $k$-fiber irreducible components of the smooth curves (3.3.2) and $(3.3.3)_{\mathrm{red}}$ through $z'$, and these two primes visibly generate the maximal ideal at $z'$ in the $k$-fiber so (3.3.2) and $(3.3.3)_{\mathrm{red}}$ intersect transversally at $z'$ as desired.

Consider the supersingular case. The proof of [34, 13.5.4] ensures that we can choose $f_z$ so that

$$f_z \bmod p = g_{(1,0)}g_{(0,1)}, \tag{3.3.4}$$

with $k[\![x,t]\!]/g_{(0,1)}$ the complete local ring at $z'$ on the closed subscheme (3.3.2) and likewise for $k[\![x,t]\!]/g_{(1,0)}$ and (3.3.3). By (3.3.3), we can take $g_{(1,0)} = x^{p-1}$, so by (3.3.4) it suffices to check that the formally smooth ring $k[\![x,t]\!]/g_{(0,1)}$ does not have $t$ as a formal parameter. In the proof of [34, 12.8.2], it is shown that there is a natural isomorphism between the moduli stack of Igusa structures and the moduli stack of $(p-1)$th roots of the Hasse invariant of elliptic curves over $\mathbf{F}_p$-schemes. Since the Hasse invariant commutes with base change and the Hasse invariant on the the universal deformation of a supersingular elliptic curve over $k[\![t]\!]$ has a simple zero [34, 12.4.4], by extracting a $(p-1)$th root we lose the property of $t$ being a formal parameter if $p > 2$. We do not need the theorem for the supersingular case when $p = 2$, so we leave this case as an exercise for the interested reader.

∎

## 4 Determination of non-regular points

Since the quotient $X_H(p)$ of the normal proper $\mathbf{Z}_{(p)}$-curve $X_1(p;\mathcal{P})$ is normal, there is a finite set of non-regular points in codimension-2 on $X_H(p)$ that we have to resolve to get a regular model. We will prove that the non-regular points on the nil-semistable $X_H(p)$ are certain *non-cuspidal* $\mathbf{F}_p$-rational points with $j$-invariants 0 and 1728, and that these singularities are tame cyclic quotient singularities when $p > 3$, so Jung–Hirzebruch resolution in Theorem 2.4.1 will tell us everything we need to know about the minimal regular resolution of $X_H(p)$.

### 4.1 Analysis away from cusps

The only possible non-regular points on $X_H(p)$ are closed points in the closed fiber. We will first consider those points that lie in $Y_H(p)$, and then we will study the situation at the cusps. The reason for treating these cases separately is that the deformation theory of generalized elliptic curves is a little more subtle than that of elliptic curves. One can also treat the situation at the cusps by using Tate curves instead of formal deformation theory; this is the approach used in [34].

In order to determine the non-regular points on $Y_H(p)$, by Lemma 2.1.1 we only need to consider geometric points. By Theorem 3.1.1, we need a criterion for detecting when a finite group acting on a regular local ring has regular subring of invariants. The criterion is provided by Serre's Theorem 2.3.9 and leads to:

Theorem 4.1.1. *A geometric point $z = (E_z, P_z) \in Y_1(p)$ has non-regular image in $Y_H(p)$ if and only if it is a point in the closed fiber such that $|\mathrm{Aut}(E_z)| > 2$, $P_z = 0$, and $2|H| \nmid |\mathrm{Aut}(E_z)|$.*

*In particular, when $p > 3$ there are at most two non-regular points on $Y_H(p)$ and such points are $\mathbf{F}_p$-rational, while for $p \leq 3$ (so $H$ is trivial) the unique ($\mathbf{F}_p$-rational) supersingular point is the unique non-regular point.*

*Proof.* Let $k$ be an algebraically closed field of characteristic $p$ and define $W = W(k)$; we may assume that $z$ is a $k$-rational point. By Lemma 2.1.1, we may consider the situation after base change by $\mathbf{Z}_{(p)} \to W$. A non-regular point $z$ must be a closed point on the closed fiber. Let $z'$ be a point over $z$ in $Y_1(p;\mathcal{P})(k)$. Let $(E_z, P_z)$ be the structure arising from $z$.

First suppose $p > 3$ and $H$ is trivial. The group $\mathrm{Aut}_k(E_z)$ is cyclic of order prime to $p$, so the automorphism group $\mathrm{Aut}(z)$ of the $\Gamma_1(p)$-structure underlying $z$ is also cyclic of order prime to $p$. By Theorems 3.1.1 and 2.3.9, the regularity of $\widehat{\mathcal{O}}_{Y_1(p)_W,z}$ is therefore equivalent to the existence of a stable line under the action of $\mathrm{Aut}(z)$ on the 2-dimensional cotangent space to the regular universal deformation ring $\mathcal{R}_z = \widehat{\mathcal{O}}_{Y_1(p;\mathcal{P})_W,z'}$ of the $\Gamma_1(p)$-structure $z$.

When the $\Gamma_1(p)$-structure $z$ is étale (*i.e.*, $P_z \neq 0$), then the formal deformation theory for $z$ is the same as for the underlying elliptic curve $E_z/\langle P_z\rangle$, whence the universal deformation ring is isomorphic to $W[\![t]\!]$. In such cases, $p$ spans an $\mathrm{Aut}(z)$-invariant line in the cotangent space of the deformation ring. Even when $H$ is not assumed to be trivial, this line is stable under the action of the stabilizer of $z'$ the preimage of $H$ in $(\mathbf{Z}/p\mathbf{Z})^\times$). Hence, we get regularity at $z$ for any $H$ when $p > 3$ and $P_z \neq 0$.

Still assuming $p > 3$, now drop the assumption of triviality on $H$ but suppose that the $\Gamma_1(p)$-structure is not étale, so $z = (E_z, 0)$ and $\mathrm{Aut}(z) = \mathrm{Aut}_k(E_z)$. The preimage $H' \subseteq (\mathbf{Z}/p\mathbf{Z})^\times$ of $H$ acts on the deformation ring $\mathcal{R}_z$ since $P_z = 0$. By Theorem 3.1.1 and Theorem 3.2.2, the cotangent space to $\mathcal{R}_z$ is canonically isomorphic to

$$\mathrm{Cot}_0(E_z) \oplus \mathrm{Cot}_0(E_z)^{\otimes 2}, \tag{4.1.1}$$

where this decomposition corresponds to the lines spanned by the images of $x$ and $t$ respectively. Conceptually, the first line in (4.1.1) arises from equicharacterisitc deformations of the point of order $p$ on constant deformations of the elliptic curve $E_z$, and the second line arises from deformations of the elliptic curve without deforming the vanishing level structure $P_z$. These identifications are compatible with the natural actions of $\mathrm{Aut}(z) = \mathrm{Aut}(E_z)$.

Since $p > 3$, the action of $\mathrm{Aut}(E_z) = \mathrm{Aut}(z)$ on the line $\mathrm{Cot}_0(E_z)$ is given by a faithful (non-trivial) character $\overline{\chi}_{\mathrm{id}}$, and the other line in (4.1.1) is acted upon by $\mathrm{Aut}(E_z)$ via the character $\chi_{\mathrm{id}}^2$. The resulting representation of $\mathrm{Aut}(z)$ on $\mathrm{Cot}_0(E_z)^{\otimes 2}$ is trivial if and only if $\overline{\chi}_{\mathrm{id}}^2 = 1$, which is to say (by faithfulness) that $\mathrm{Aut}(E_z)$ has order 2 (*i.e.*, $j(E_z) \neq 0, 1728$). Since the $H'$-action is trivial on the line $\mathrm{Cot}_0(E_z)^{\otimes 2}$ (due to $H'$ only acting on the level structure) and we are passing to invariants by the action of the group $H' \times \mathrm{Aut}(E_{z/k})$, by Serre's theorem we get regularity without restriction on $H$ when $j(E_z) \neq 0, 1728$.

If $j(E_z) \in \{0, 1728\}$ then $|\mathrm{Aut}(E_z)| > 2$ and the cyclic $H'$ acts on (4.1.1) through a representation $\psi \oplus 1$ with $\psi$ a faithful character. The cyclic $\mathrm{Aut}(z)$ acts through a representation $\chi \oplus \chi^2$ with $\chi$ a faithful character, so $\chi^2 \neq 1$. The commutative group of actions on (4.1.1) generated by $H'$ and $\mathrm{Aut}(z)$ is generated by pseudo-reflections if and only if the action of the cyclic $\mathrm{Aut}(z)$ on the first line is induced by the action of a subgroup of $H'$. That is, the order of $\chi$ must divide the order of $\psi$, or equivalently $|\mathrm{Aut}(z)|$ must divide $|H'| = 2|H|$. This yields exactly the desired conditions for non-regularity when $p > 3$.

Now suppose $p \leq 3$, so $H$ is trivial. If $\mathrm{Aut}(E_{z/k}) = \{\pm 1\}$, so $z$ is an ordinary point, then for $p = 3$ we can use the preceding argument to deduce regularity at $z$. Meanwhile, for $p = 2$ we see that $\mathcal{R}_z$ is formally smooth by Theorem 3.3.3, so the subring of invariants at $z$ is formally smooth (by [34, p. 508]). It remains to check non-regularity at the unique (supersingular) point $z \in Y_1(p)_{/k}$ with $j = 0 = 1728$ in $k$.

By Serre's theorem, it suffices to check that the action of $\mathrm{Aut}(z) = \mathrm{Aut}(E_z)$ on (4.1.1) is not generated by pseudo-reflections, where $E_z$ is the unique supersingular elliptic curve over $k$ (up to isomorphism). The action of $\mathrm{Aut}(E_z)$ is through 1-dimensional characters, so the $p$-Sylow subgroup must act trivially. In both cases ($p = 2$ or 3) the group $\mathrm{Aut}(E_z)$ has order divisible by only two primes $p$ and $p'$, with the $p'$-Sylow of order $> 2$. This $p'$-Sylow must act through a faithful character on $\mathrm{Cot}_0(E_z)$ (use [20, Lemma 3.3] or [68, Lemma 2.16]), and hence this group also acts non-trivially on $\mathrm{Cot}_0(E_z)^{\otimes 2}$. It follows that this action is not generated by pseudo-reflections.

□

### 4.2 Regularity along the cusps

Now we check that $X_H(p)$ is regular along the cusps, so we can focus our attention on $Y_H(p)$ when computing the minimal regular resolution of $X_H(p)$. We will again use deformation theory, but now in the case of generalized elliptic curves. Throughout this section, $p$ is an arbitrary prime.

Recall that a *generalized elliptic curve* over a scheme $S$ is a proper flat map $\pi : E \to S$ of finite presentation equipped with a section $e : S \to E^{\mathrm{sm}}$ into the relative smooth locus and a map

$$+ : E^{\mathrm{sm}} \times_S E \to E$$

such that

- the geometric fibers of $\pi$ are smooth genus 1 curves or Néron polygons;
- $+$ restricts to a commutative group scheme structure on $E^{\mathrm{sm}}$ with identity section $e$;
- $+$ is an action of $E^{\mathrm{sm}}$ on $E$ such that on singular geometric fibers with at least two "sides", the translation action by each rational point in the smooth locus induces a rotation on the graph of irreducible components.

Since the much of the basic theory of Drinfeld structures was developed in [34, Ch. 1] for arbitrary smooth separated commutative group schemes of relative dimension 1, it can be applied (with minor changes in proofs) to the smooth locus of a generalized elliptic curve. In this way, one can merge the "affine" moduli-theoretic $\mathbf{Z}$-theory in [34] with the "proper" moduli-theoretic $\mathbf{Z}[1/N]$-theory in [15]. We refer the reader to [21] for further details on this synthesis.

The main deformation-theoretic fact we need is an analogue of Theorem 3.2.1:

THEOREM 4.2.1. *An irreducible generalized elliptic curve $C_1$ over a perfect field $k$ of characteristic $p > 0$ admits a universal deformation ring that is abstractly isomorphic to $W[\![t]\!]$, and the equicharacteristic cotangent space of this deformation ring is canonically isomorphic to* $\mathrm{Cot}_0(C_1^{\mathrm{sm}})^{\otimes 2}$.

*Proof.* The existence and abstract structure of the deformation ring are special cases of [15, III, 1.2]. To describe the cotangent space intrinsically, we wish to put ourselves in the context of deformation theory of proper flat curves. Infinitesimal deformations of $C_1$ admit a unique generalized elliptic curve structure once we fix the identity section [15, II, 2.7], and any two choices of identity section are uniquely related by a translation action. Thus, the deformation theory for $C_1$ as a generalized elliptic (*i.e.*, marked) curve coincides with its deformation theory as a flat (unmarked) curve. In particular, the tangent space to this deformation functor is canonically identified with $\mathrm{Ext}^1_{C_1}(\Omega^1_{C_1/k}, \mathcal{O}_{C_1})$ [56, §4.1.1].

Since the natural map $\Omega^1_{C_1/k} \to \omega_{C_1/k}$ to the invertible relative dualizing sheaf is injective with finite-length cokernel (supported at the singularity),

$$\mathrm{Ext}^1_{C_1}(\omega_{C_1/k}, \mathcal{O}_{C_1}) \simeq \mathrm{Ext}^1_{C_1}(\omega^{\otimes 2}_{C_1/k}, \omega_{C_1/k}) \simeq \mathrm{H}^0(C_1, \omega^{\otimes 2}_{C_1/k})^\vee,$$

with the final isomorphism provided by Grothendieck duality. Thus, the cotangent space to the deformation functor is identified with $\mathrm{H}^0(C_1, \omega^{\otimes 2}_{C_1/k})$. Since $\omega_{C_1/k}$ is (non-canonically) trivial, just as for elliptic curves, we get a canonical isomorphism

$$\mathrm{H}^0(C_1, \omega^{\otimes 2}_{C_1/k}) \simeq \mathrm{H}^0(C_1, \omega_{C_1/k})^{\otimes 2} \simeq \mathrm{Cot}_0(C_1^{\mathrm{sm}})^{\otimes 2}$$

(the final isomorphism defined via pullback along the identity section).

□

DEFINITION 4.2.2. A $\Gamma_1(N)$-*structure* on a generalized elliptic curve $E \to S$ is an "$S$-ample" Drinfeld $\mathbf{Z}/N\mathbf{Z}$-structure on $E^{\mathrm{sm}}$; *i.e.*, a section $P \in E^{\mathrm{sm}}[N](S)$ such that the relative effective Cartier divisor

$$D = \sum_{j \in \mathbf{Z}/N\mathbf{Z}} [jP]$$

in $E^{\mathrm{sm}}$ is a subgroup scheme which meets all irreducible components of all geometric fibers.

If $E_{/S}$ admits a $\Gamma_1(N)$-structure, then the non-smooth geometric fibers must be $d$-gons for various $d|N$. In case $N = p$ is prime, this leaves $p$-gons and 1-gons as the only options. The importance of Definition 4.2.2 is the following analogue of Theorem 3.1.1:

THEOREM 4.2.3. *Let $k$ be an algebraically closed field of characteristic $p > 0$, and $W = W(k)$. The points of $X_1(p)_{/k} - Y_1(p)_{/k}$ correspond to isomorphism classes of $\Gamma_1(p)$-structures on degenerate generalized elliptic curves over $k$ with 1 or $p$ sides.*

*For $z \in X_1(p)_{/k} - Y_1(p)_{/k}$, there exists a universal deformation ring $\mathcal{S}_z$ for the $\Gamma_1(p)$-structure $z$, and $\widehat{\mathcal{O}}_{X_1(p)_W, z}$ is the subring of $\mathrm{Aut}(z)$-invariants in $\mathcal{S}_z$.*

*Proof.* In general, $\Gamma_1(p)$-structures on generalized elliptic curves form a proper flat Deligne-Mumford stack $\overline{M}_{\Gamma_1(p)}$ over $\mathbf{Z}_{(p)}$ of relative dimension 1, and this stack is smooth over $\mathbf{Q}$ and is normal (as one checks via abstract deformation theory). For our purposes, the important point is that if we choose an odd prime $\ell \neq p$ then we can define an evident $[\Gamma_1(p), \Gamma(\ell)]$-variant on Definition 4.2.2 (imposing an ampleness condition on the combined level structure), and the open locus of points with trivial geometric automorphism group is a scheme (as it is an algebraic space quasi-finite over the $j$-line). This locus fills up the entire stack $\overline{M}_{[\Gamma_1(p),\Gamma(\ell)]}$ over $\mathbf{Z}_{(p)}$, so this stack is a scheme.

The resulting normal $\mathbf{Z}_{(p)}$-flat proper scheme $\overline{M}_{[\Gamma_1(p),\Gamma(\ell)]}$ is finite over the $j$-line, whence it must *coincide* with the scheme $X_1(p;[\Gamma(\ell)])$ as constructed in [34] by the *ad hoc* method of normalization of the fine moduli scheme $Y_1(p;[\Gamma(\ell)])$ over the $j$-line. We therefore get a map

$$\overline{M}_{[\Gamma_1(p),\Gamma(\ell)]} = X_1(p;[\Gamma(\ell)]) \to X_1(p)$$

that *must* be the quotient by the natural $\mathrm{GL}_2(\mathbf{F}_\ell)$-action on the source. Since complete local rings at geometric points on a Deligne-Mumford stack coincide with universal formal deformation rings, we may conclude as in the proof of Theorem 3.1.1.

□

We are now in position to argue just as in the elliptic curve case: we shall work out the deformation rings in the various possible cases and for $p \neq 2$ we will use Serre's pseudo-reflection theorem to deduce regularity of $X_1(p)$ along the cusps on the closed fiber. A variant on the argument will also take care of $p = 2$.

As in the elliptic curve case, it will suffice to consider geometric points. Thus, there will be two types of $\Gamma_1(p)$-structures $(E, P)$ to deform: $E$ is either a $p$-gon or a 1-gon.

Lemma 4.2.4. *Let $E_0$ be a $p$-gon over an algebraically closed field $k$ of characteristic $p$, and $P_0 \in E_0^{\mathrm{sm}}(k)$ a $\Gamma_1(p)$-structure. The deformation theory of $(E_0, P_0)$ coincides with the deformation theory of the 1-gon generalized elliptic curve $E_0/\langle P_0\rangle$.*

Note that in the $p$-gon case, the point $P_0 \in E_0^{\mathrm{sm}}(k)$ generates the order-$p$ constant component group of $E_0^{\mathrm{sm}}$, so the group scheme $\langle P_0\rangle$ generated by $P_0$ is visibly étale and the quotient $E_0/\langle P_0\rangle$ makes sense (as a generalized elliptic curve) and is a 1-gon.

*Proof.* For any infinitesimal deformation $(E, P)$ of $(E_0, P_0)$, the subgroup scheme $H$ generated by $P$ is finite étale, and it makes sense to form the quotient $E/H$ as a generalized elliptic curve deformation of the 1-gon $E_0/H_0$ (with $H_0 = \langle P_0\rangle$). Since any finite étale cover of a generalized elliptic curve admits a unique compatible generalized elliptic curve structure once we fix a lift of the identity section and demand geometric connectedness of fibers over the base [15, II, 1.17], we see that the deformation theory of $(E_0, H_0)$ (ignoring $P$) is equivalent to the deformation theory of the 1-gon $E_0/H_0$. The deformation theory of a 1-gon is formally smooth of relative dimension 1 [15, III, 1.2], and upon specifying $(E, H)$ deforming $(E_0, H_0)$ the étaleness of $H$ ensures the existence and uniqueness of the choice of $\Gamma_1(p)$-structure $P$ generating $H$ such that

$P$ lifts $P_0$ on $E_0$. That is, the universal deformation ring for $(E_0, P_0)$ coincides with that of $E_0/H_0$.

□

In the 1-gon case, there is only one (geometric) possibility up to isomorphism: the pair $(C_1, 0)$ where $C_1$ is the standard 1-gon (over an algebraically closed field $k$ of characteristic $p$). For this, we have an analogue of (4.1.1):

LEMMA 4.2.5. *The universal deformation ring of the* $\Gamma_1(p)$*-structure* $(C_1, 0)$ *is isomorphic to the regular local ring* $W[\![t]\!][\![X]\!]/\Phi_p(X+1)$*, with cotangent space canonically isomorphic to*

$$\mathrm{Cot}_0(C_1^{\mathrm{sm}}) \oplus \mathrm{Cot}_0(C_1^{\mathrm{sm}})^{\otimes 2}.$$

*Proof.* Since the $p$-torsion on $C_1^{\mathrm{sm}}$ is isomorphic to $\mu_p$, upon fixing an isomorphism $C_1^{\mathrm{sm}}[p] \simeq \mu_p$ there is a unique compatible isomorphism $C^{\mathrm{sm}}[p] \simeq \mu_p$ for any infinitesimal deformation $C$ of $C_1$. Thus, the deformation problem is that of endowing a $\mathbf{Z}/p\mathbf{Z}$-generator to the $\mu_p$ inside of deformations of $C_1$ (as a generalized elliptic curve). By Theorem 4.2.3, this is the scheme of generators of $\mu_p$ over the universal deformation ring $W[\![t]\!]$ of $C_1$.

The scheme of generators of $\mu_p$ over $\mathbf{Z}$ is $\mathbf{Z}[Y]/\Phi_p(Y)$, so we obtain $W[\![t]\!][Y]/\Phi_p(Y)$ as the desired (regular) deformation ring. Now just set $X = Y - 1$. The description of the cotangent space follows from Theorem 4.2.1.

□

Since $C_1$ has automorphism group (as a generalized elliptic curve) generated by the unique extension $[-1]$ of inversion from $C_1^{\mathrm{sm}}$ to all of $C_1$, we conclude that $\mathrm{Aut}(C_1, 0)$ is generated by $[-1]$. This puts us in position to carry over our earlier elliptic-curve arguments to prove:

THEOREM 4.2.6. *The scheme* $X_H(p)$ *is regular along its cusps.*

*Proof.* As usual, we may work after making a base change by $W = W(k)$ for an algebraically closed field $k$ of characteristic $p > 0$. Let $z \in X_1(p)_{/k}$ be a cusp whose image $z_H$ in $X_H(p)_{/k}$ we wish to study. Let $H'$ be the preimage of $H$ in $(\mathbf{Z}/p\mathbf{Z})^\times$, and let $H'_z$ be the maximal subgroup of $H'$ that acts on the deformation space for $z$ (*e.g.*, $H'_z = H'$ if the level structure $P_z$ vanishes). By Theorem 4.2.3, the ring $\widehat{\mathcal{O}}_{X_H(p), z_H}$ is the subring of invariants under the action of $\mathrm{Aut}(z) \times H'_z$ on the formal deformation ring for $z$. By Theorem 4.2.1 and Lemma 4.2.4 (as well as [34, p. 508]), this deformation ring is regular (even formally smooth) in the $p$-gon case. In the 1-gon case, Lemma 4.2.5 ensures that the deformation ring is regular (and even formally smooth when $p = 2$). Thus, for $p \neq 2$ we may use Theorem 2.3.9 to reduce the problem for $p \neq 2$ to checking that the action of $\mathrm{Aut}(z) \times H'_z$ on the 2-dimensional cotangent space to the deformation functor has an invariant line.

In the $p$-gon case, the deformation ring is $W[\![t]\!]$ and the cotangent line spanned by $p$ is invariant. In the 1-gon case, Lemma 4.2.5 provides a functorial description of the cotangent space to the deformation functor and from this it is clear that the involution $[-1]$ acts with an invariant line $\mathrm{Cot}_0(z)^{\otimes 2}$ when $p \neq 2$ and that $H'_z$ also acts trivially on this line.

To take care of $p = 2$ (for which $H$ is trivial), we just have to check that any non-trivial $W$-algebra involution $\iota$ of $W[\![T]\!]$ has regular subring of invariants. In fact, for $T' = T\iota(T)$ the subring of invariants is $W[\![T']\!]$ by [34, p. 508].

□

## 5 The Minimal resolution

We now are ready to compute the minimal regular resolution $X_H(p)^{\mathrm{reg}}$ of $X_H(p)$. Since $X_H(p)_{/\mathbf{Q}}$ is a projective line when $p \leq 3$, both Theorem 1.1.2 and Theorem 1.1.6 are trivial for $p \leq 3$. Thus, from now on we assume $p > 3$. We have found all of the non-regular points (Theorem 4.1.1): the $\mathbf{F}_p$-rational points of $(1,0)$-type such that $j \in \{0, 1728\}$, provided that $|H|$ is not divisible by 3 (resp. 2) when $j = 0$ (resp. $j = 1728$). Theorem 3.3.3 provides the necessary local description to carry out Jung–Hirzebruch resolution at these points. These are tame cyclic quotient singularities (since $p > 3$). Moreover, the closed fiber of $X_H(p)$ is a nil-semistable curve that consists of two irreducible components that are geometrically irreducible, as one sees by considering the (1,0)-cyclic and (0,1)-cyclic components.

### 5.1 General considerations

There are four cases, depending on $p \equiv \pm 1, \pm 5 \bmod 12$ as this determines the behavior of the $j$-invariants 0 and 1728 in characteristic $p$ (*i.e.*, supersingular or ordinary). This dichotomy between ordinary and supersingular cases corresponds to Jung–Hirzebruch resolution with either one or two analytic branches.

Pick a point $z = \underline{(E, 0)} \in X_1(p)(\mathbf{F}_p)$ with $j = 0$ or 1728 corresponding an elliptic curve $E$ over $\overline{\mathbf{F}}_p$ with automorphism group of order $> 2$. Let $z_H \in X_H(p)(\mathbf{F}_p)$ be the image of $z$. By Theorem 4.1.1, we know that $z_H$ is non-regular if and only if $|H|$ is odd for $j(E) = 1728$, and if and only if $|H|$ is not divisible by 3 for $j(E) = 0$.

There is a single irreducible component through $z_H$ in the ordinary case (arising from either (3.3.2) or (3.3.3)), while there are two such (transverse) components in the supersingular case, and to compute the generic multiplicities of these components in $X_H(p)_{/\overline{\mathbf{F}}_p}$ we may work with completions because the irreducible components through $z_H$ are analytically irreducible (even smooth) at $z_H$.

Let $C'$ and $C$ denote the irreducible components of $X_H(p)_{/\overline{\mathbf{F}}_p}$, with $C'$ corresponding to étale level $p$-structures. Since the preimage of $H$ in $(\mathbf{Z}/p\mathbf{Z})^\times$ (of order $2|H|$) acts generically freely (resp. trivially) on the preimage of $C'$ (resp. of $C$) in a fine moduli scheme over $X_H(p)_{/\overline{\mathbf{F}}_p}$ obtained by adjoining some prime-to-$p$ level structure, ramification theory considerations and Theorem 3.3.3 show that the components $C'$ and $C$ in $X_H(p)_{/\overline{\mathbf{F}}_p}$ have respective multiplicities of 1 and $(p-1)/2|H| = [(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\} : H]$. Moreover, by Theorem 3.3.3 we see that $z_H$ lies on $C$ when it is an ordinary point.

## 5.2 THE CASE $p \equiv -1 \bmod 12$

We are now ready to resolve the singularities on $X_H(p)_{/W}$ with $W = W(\overline{\mathbf{F}}_p)$. We will first carry out the calculation in the case $p \equiv -1 \pmod{12}$, so 0 and 1728 are supersingular $j$-values. In this case $(p-1)/2$ is not divisible by 2 or 3, so $|H|$ is automatically not divisible by 2 or 3 (so we have two non-regular points).

Write $p = 12k-1$ with $k \geq 1$. By the Deuring Mass Formula [34, Cor. 12.4.6] the components $C$ and $C'$ meet in $(p-11)/12 = k-1$ geometric points away from the two supersingular points with $j = 0, 1728$. Consider one of the two non-regular supersingular points $z_H$. The complete local ring at $z_H$ on $X_H(p)_W$ is the subring of invariants for the commuting actions of $\mathrm{Aut}(z)$ and the preimage $H' \subseteq (\mathbf{Z}/p\mathbf{Z})^\times$ of $H$ on the universal deformation ring $\mathcal{R}_z$ of the $\Gamma_1(p)$-structure $z$. Note that the actions of $H'$ and $\mathrm{Aut}(z)$ on $\mathcal{R}_z$ have a common involution. The action of $H'$ on the tangent space fixes one line and acting through a faithful character on the other line (see the proof of Theorem 4.1.1), so by Serre's Theorem 2.3.9 the subring of $H'$-invariants in $\mathcal{R}_z$ is regular. By Lemma 2.3.5 and the subsequent discussion there, the subring of $H'$-invariant has the form $W[\![x', t']\!]/(x'^{(p-1)/|H'|}t' - p)$ with $\mathrm{Aut}(z)/\{\pm 1\}$ acting on the tangent space via $\chi^{|H|} \oplus \chi$ for a faithful character $\chi$ of $\mathrm{Aut}(z)/\{\pm 1\}$. Let $h = |H|$, so $\rho := (p-1)/2h$ is the multiplicity of $C$ in $X_H(p)_{/\overline{\mathbf{F}_p}}$.

When $j(z_H) = 1728$ the character $\chi$ is quadratic, so we apply Theorem 2.4.1 and Corollary 2.4.3 with $n = 2$, $r = 1$, $m_1' = 1$, $m_2' = \rho$. The resolution has a single exceptional fiber $D'$ that is transverse to the strict transforms $\overline{C}$ and $\overline{C}'$, and $D'$ has self-intersection $-2$ and multiplicity $(m_1' + m_2')/2 = (\rho+1)/2$. When $j(z_H) = 0$ the character $\chi$ is cubic, so we apply Theorem 2.4.1 with $n = 3$, $m_1' = 1$, $m_2' = \rho$, and $r = h \bmod 3$. That is, $r = 1$ when $h \equiv 1 \bmod 6$ and $r = 2$ when $h \equiv -1 \bmod 6$. In the case $r = 1$ we get a single exceptional fiber $E'$ in the resolution, transverse to $\overline{C}$ and $\overline{C}'$ with self-intersection $-3$ and multiplicity $(\rho+1)/3$ (by Corollary 2.4.3). This is illustrated in Figure 2(a). In the case $r = 2$ we use the continued fraction $3/2 = 2 - 1/2$ to see that the resolution of $z_H$ has exceptional fiber with two components $E_1'$ and $E_2'$, and these have self-intersection $-2$ and transverse intersections as shown in Figure 2(b) with respective multiplicities $(2\rho+1)/3$ and $(\rho+2)/3$ by Corollary 2.4.3. This completes the computation of the minimal regular resolution $X_H(p)'$ of $X_H(p)$ when $p \equiv -1 \bmod 12$.

To compute the intersection matrix for the closed fiber of $X_H(p)'$, we need to compute some more intersection numbers. For $h \equiv 1 \bmod 6$ we let $\mu$ and $\nu$ denote the multiplicities of $D'$ and $E'$ in $X_H(p)'$, and for $h \equiv -1 \bmod 6$ we

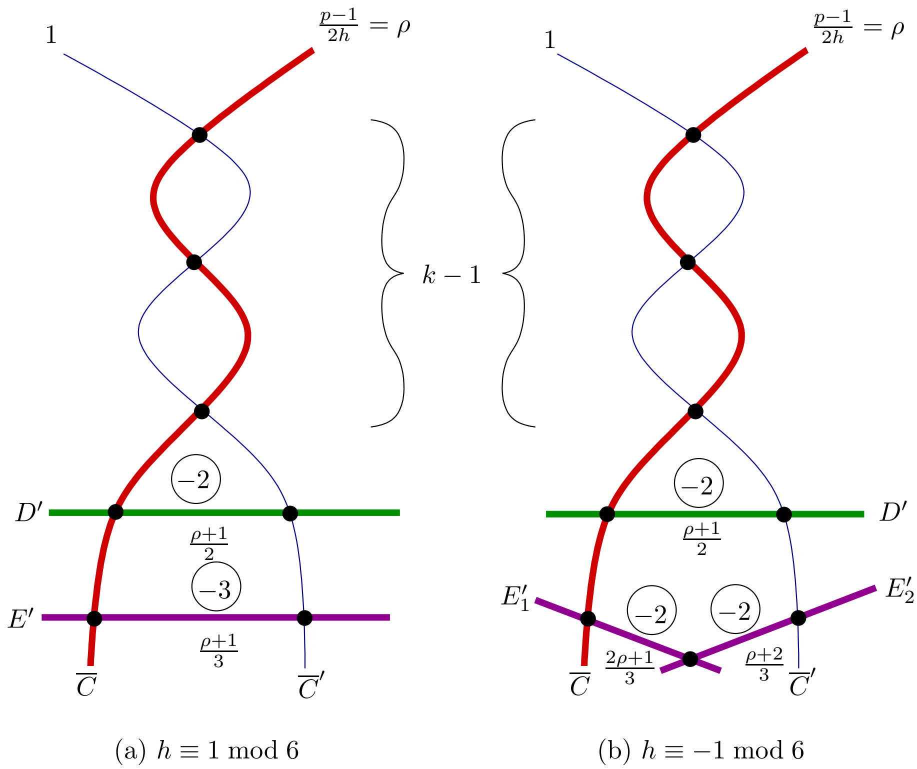


Figure 2: Minimal regular resolution $X_H(p)'$ of $X_H(p)$, $p = 12k-1$, $k \geq 1$, $h = |H|$

define $\mu$ in the same way and let $\nu_j$ denote the multiplicity of $E'_j$ in $X_H(p)'$. In other words,

$$\mu = (\rho+1)/2,\ \nu = (\rho+1)/3,\ \nu_1 = (2\rho+1)/3,\ \nu_2 = (\rho+2)/3.$$

Thus,

$$\overline{C}' + \rho\overline{C} + \mu D' + \nu E' \equiv 0, \tag{5.2.1}$$

so if we intersect (5.2.1) with $\overline{C}$ and use the identities

$$\rho = (6k-1)/h,\ \overline{C}'.\overline{C} = k-1 = (h\rho - 5)/6,$$

we get

$$\overline{C}.\overline{C} = -1 - (h-\varepsilon)/6$$

where $\varepsilon = \pm 1 \equiv h \bmod 6$. In particular, $\overline{C}.\overline{C} < -1$ unless $h = 1$ (*i.e.*, unless $H$ is trivial). We can also compute the self-intersection for $\overline{C}'$, but we do not need it.

When $H$ is trivial, so $\overline{C}$ is a $-1$-curve, we can contract $\overline{C}$ and then by Theorem 2.1.2 and Figure 2 the self-intersection numbers for the components $D'$ and $E'$ drop to $-1$ and $-2$ respectively. Then we may contract $D'$, so $E'$ becomes a $-1$-curve, and finally we end with a single irreducible component (coming from $\overline{C}'$). This proves Theorem 1.1.2 when $p \equiv -1 \bmod 12$.

Returning to the case of general $H$, let us prove Theorem 1.1.6 for $p \equiv -1 \bmod 12$. Since $\overline{C}'$ has multiplicity 1 in the closed fiber of $X_H(p)'$, we can use the following special case of a result of Lorenzini [9, 9.6/4]:

LEMMA 5.2.1 (LORENZINI). *Let $X$ be a regular proper flat curve over a complete discrete valuation ring $R$ with algebraically closed residue field and fraction field $K$. Assume that $X_{/K}$ is smooth and geometrically connected. Let $X_1, \dots, X_m$ be the irreducible components of the closed fiber $\overline{X}$ and assume that some component $X_{i_0}$ occurs with multiplicity 1 in the closed fiber divisor.*

*The component group of the Néron model of the Jacobian $\mathrm{Pic}^0_{X_K/K}$ has order equal to the absolute value of the $(m-1)\times(m-1)$ minor of the intersection matrix $(X_i.X_j)$ obtained by deleting the $i_0$th row and column.*

The intersection submatrices formed by the ordered set $\{\overline{C}, D', E'\}$ for $h \equiv 1 \bmod 6$ and by $\{\overline{C}, D', E'_1, E'_2\}$ for $h \equiv -1 \bmod 6$ are given in Figure 3. The absolute value of the determinant is $h$ in each case, so by Lemma 5.2.1 the order of the component group $\Phi(\mathcal{J}_H(p)_{/\mathbf{F}_p})$ is $h = |H| = |H|/\gcd(|H|, 6)$.

To establish Theorem 1.1.6 for $p \equiv -1 \bmod 12$, it remains to show that the natural Picard map $J_0(p) \to J_H(p)$ induces a surjection on mod-$p$ geometric component groups. We outline a method that works for general $p$ but that we will (for now) carry out only for $p \equiv -1 \bmod 12$, as we have only computed the intersection matrix in this case.

$$\begin{array}{cc}
 & \begin{array}{ccc} \overline{C} & D' & E' \end{array} \\
\begin{array}{c} \overline{C} \\ D' \\ E' \end{array} & \begin{pmatrix} -1-\frac{(h-1)}{6} & 1 & 1 \\ 1 & -2 & 0 \\ 1 & 0 & -3 \end{pmatrix}
\end{array}
\qquad
\begin{array}{cc}
 & \begin{array}{cccc} \overline{C} & D' & E'_1 & E'_2 \end{array} \\
\begin{array}{c} \overline{C} \\ D' \\ E'_1 \\ E'_2 \end{array} & \begin{pmatrix} -1-\frac{(h+1)}{6} & 1 & 1 & 0 \\ 1 & -2 & 0 & 0 \\ 1 & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 \end{pmatrix}
\end{array}$$

(a) $h \equiv 1 \bmod 6$ (b) $h \equiv -1 \bmod 6$

Figure 3: Submatrices of intersection matrix for $X_H(p)'$, $p \equiv -1 \bmod 12$

The component group for $J_0(p)$ is generated by $(0)-(\infty)$, where $(0)$ classifies the 1-gon with standard subgroup $\mu_p \hookrightarrow \mathbf{G}_m$ in the smooth locus, and $(\infty)$ classifies the $p$-gon with subgroup $\mathbf{Z}/p\mathbf{Z} \hookrightarrow (\mathbf{Z}/p\mathbf{Z}) \times \mathbf{G}_m$ in the smooth locus. The generic-fiber Picard map induced by the coarse moduli scheme map

$$X_H(p)_{/\mathbf{Z}_{(p)}} \to X_0(p)_{/\mathbf{Z}_{(p)}}$$

pulls $(0)-(\infty)$ back to a divisor

$$P \;-\; \sum_{j=1}^{(p-1)/2|H|} P'_i \tag{5.2.2}$$

where the $P'_i$'s are $\mathbf{Q}$-rational points whose (cuspidal) reduction lies in the component $\overline{C}'$ classifying étale level-structures and $P$ is a point with residue field $(\mathbf{Q}(\zeta_p)^+)^H$ whose (cuspidal) reduction lies in the component $\overline{C}$ classifying multiplicative level-structures. This description is seen by using the moduli interpretation of cusps (*i.e.*, Néron polygons) and keeping track of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-actions, and it is valid for any prime $p$ (*e.g.*, the $\Gamma_1(p)$-structures on the standard 1-gon consistute a principal homogenous space for the action of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$, so they give a single closed point $P$ on $X_H(p)_{/\mathbf{Q}}$ with residue field $(\mathbf{Q}(\zeta_p)^+)^H$).

To apply (5.2.2), we need to recall some general facts (see [9, 9.5/9, 9.6/1]) concerning the relationship between the closed fiber of a regular proper model $X$ of a smooth geometrically connected curve $X_\eta$ and the component group $\Phi$ of (the Néron model of) the Jacobian of $X_\eta$, with the base equal to the spectrum of a discrete valuation ring $R$ with algebraically closed residue field. If $\{X_i\}_{i\in I}$ is the set of irreducible components in the closed fiber of $X$, then we can form a complex

$$\mathbf{Z}^I \xrightarrow{\alpha} \mathbf{Z}^I \xrightarrow{\beta} \mathbf{Z}$$

where $\mathbf{Z}^I$ is the free group on the $X_i$'s, the map $\alpha$ is defined by the intersection matrix $(X_i.X_j)$, and $\beta$ sends each standard basis vector to the multiplicity of the corresponding component in the closed fiber. The cokernel $\ker(\beta)/\mathrm{im}(\alpha)$

is naturally identified with the component group $\Phi$ via the map $\mathrm{Pic}(X) \to \mathbf{Z}^I$ that assigns to each invertible sheaf $\mathcal{L}$ its tuple of partial degrees $\deg_{X_i}(\mathcal{L})$.

By using [9, 9.1/5] to compute such line-bundle degrees, one finds that the Néron-model integral point associated to the pullback divisor in (5.2.2) has reduction whose image in $\Phi(\mathcal{J}_H(p)_{/\overline{\mathbf{F}}_p})$ is represented by

$$\frac{[\mathbf{Q}(P):\mathbf{Q}]}{\mathrm{mult}(\overline{C})} \cdot \overline{C} - \sum_{i=1}^{(p-1)/2|H|} \overline{C}' = \overline{C} - \frac{p-1}{2|H|} \cdot \overline{C}' \tag{5.2.3}$$

when this component group is computed by using the regular model $X_H(p)'$ that we have found for $p \equiv -1 \bmod 12$ (the same calculation will work for all other $p$'s, as we shall see).

The important property emerging from this calculation is that one of the coefficients in (5.2.3) is $\pm 1$, so an element in $\ker(\beta)$ that is a $\mathbf{Z}$-linear combination of $\overline{C}$ and $\overline{C}'$ *must* be a multiple of (5.2.3) and hence is in the image of $\Phi(\mathcal{J}_0(p))$ under the Picard map. Thus, to prove that the component group for $J_0(p)$ surjects onto the component group for $J_H(p)$, it suffices to check that any element in $\ker(\beta)$ can be modified modulo $\mathrm{im}(\alpha)$ to lie in the $\mathbf{Z}$-span of $\overline{C}$ and $\overline{C}'$.

Since the matrix for $\alpha$ is the intersection matrix, it suffices (and is even necessary) to check that the submatrix $M_{\overline{C},\overline{C}'}$ of the intersection matrix given by the rows labelled by the irreducible components other than $\overline{C}$ and $\overline{C}'$ is a *surjective* matrix over $\mathbf{Z}$. Indeed, such surjectivity ensures that we can always subtract a suitable element of $\mathrm{im}(\alpha)$ from any element of $\ker \beta$ to kill coefficients away from $\overline{C}$ and $\overline{C}'$ in a representative for an element in $\Phi \simeq \ker(\beta)/\mathrm{im}(\alpha)$. The surjectivity assertion over $\mathbf{Z}$ amounts to requiring that the matrix $M_{\overline{C},\overline{C}'}$ have top-degree minors with gcd equal to 1. It is enough to check that those minors that avoid the column coming from $\overline{C}'$ have gcd equal to 1. Thus, it is enough to check that in Figure 3 the matrix of rows beneath the top row has top-degree minors with gcd equal to 1. This is clear in both cases. In particular, this calculation (especially the analysis of (5.2.3)) yields the following result when $p \equiv -1 \bmod 12$:

COROLLARY 5.2.2. *Let $\rho = (p-1)/2|H|$. The degree-0 divisor $\overline{C} - \rho\overline{C}'$ represents a generator of the mod-$p$ component group of $J_H(p)$.*

The other cases $p \equiv 1, \pm 5 \bmod 12$ will behave similarly, with Corollary 5.2.2 being true for all such $p$. The only differences in the arguments are that cases with $|H|$ divisible by 2 or 3 can arise and we will sometimes have to use the "one branch" version of Jung–Hirzebruch resolution to resolve non-regular ordinary points.

## 5.3 THE CASE $p \equiv 1 \bmod 12$.

We have $p = 12k + 1$ with $k \geq 1$, so $(p-1)/2 = 6k$. In this case 0 and 1728 are both ordinary $j$-invariants, so the number of supersingular points is

$(p-1)/12 = k$ by the Deuring Mass Formula. The minimal regular resolution $X_H(p)'$ of $X_H(p)$ is illustrated in Figure 4, depending on the congruence class of $h = |H|$ modulo 6. When $h$ is divisible by 6 there are no non-regular points, so $X_H(p)' = X_H(p)_{/W}$ is as in Figure 4(a). When $h$ is even but not divisible by 3 there is only the non-regularity at $j = 0$ to be resolved, as shown in Figures 4(b),(c). The case of odd $h$ is given in Figures 4(d)–(f), and these are all easy applications of Theorem 2.4.1 and Corollary 2.4.3. We illustrate by working out the case $h \equiv 5 \bmod 6$, for which there are two ordinary singularities to resolve.

Arguing much as in the case $p \equiv -1 \bmod 12$, but now with a "one branch" situation at ordinary points, the ring to be resolved is formally isomorphic to the ring of invariants in $W[\![x', t']\!]/({x'}^{(p-1)/2|H|} - p)$ under an action of the cyclic $\mathrm{Aut}(z)/\{\pm 1\}$ with a tangent-space action of $\chi^{|H|} \oplus \chi$ for a faithful character $\chi$. At a point with $j = 1728$ we have quadratic $\chi$, $n = 2$, $r = 1$. Using the "one branch" version of Theorem 2.4.1 yields the exceptional divisor $D'$ as illustrated in Figure 4(f), transverse to $\overline{C}$ with self-intersection $-2$ and multiplicity $\rho/2$. At a point with $j = 0$ we have a cubic $\chi$, so $n = 3$. Since $h \equiv 2 \bmod 3$ when $h \equiv 5 \bmod 6$, we have $r = 2$. Since $3/2 = 2 - 1/2$, we get exceptional divisors $E_1'$ and $E_2'$ with transverse intersections as shown and self-intersections of $-2$. The "outer" component $E_1'$ has multiplicity $\rho/3$ and the "inner" component $E_2'$ has multiplicity $2\rho/3$. Once again we will suppress the calculation of $\overline{C}'.\overline{C}'$ since it is not needed.

We now proceed to analyze the component group for each value of $h \bmod 6$. Since $\overline{C}'$ has multiplicity 1 in the closed fiber, we can carry out the same strategy that was used for $p \equiv -1 \bmod 12$, resting on Lemma 5.2.1. When $h \equiv 0 \bmod 6$, there are only the components $\overline{C}$ and $\overline{C}'$ in the closed fiber of $X_H(p)' = X_H(p)$, with $\overline{C}.\overline{C} = -h/6$. Thus, the component group has the expected order $|H|/6$ and since there are no additional components we are done in this case.

If $h \equiv 1 \bmod 6$, one finds that the submatrix of the intersection matrix corresponding to the ordered set $\{\overline{C}, D', E'\}$ is

$$\begin{pmatrix} -(h+5)/6 & 1 & 1 \\ 1 & -2 & 0 \\ 1 & 0 & -3 \end{pmatrix}$$

with absolute determinant $h = |H|/\gcd(|H|, 6)$ as desired, and the bottom two rows have $2 \times 2$ minors with gcd equal to 1. Moreover, in the special case $h = 1$ we see that $\overline{C}$ is a $-1$-curve, and after contracting this we contract $D'$ and $E'$ in turn, leaving us with only the component $\overline{C}'$. This proves Theorem 1.1.2 for $p \equiv 1 \bmod 12$.

For $h \equiv 2 \bmod 6$, the submatrix indexed by $\{\overline{C}, E_1', E_2'\}$ is

$$\begin{pmatrix} -(h+4)/6 & 0 & 1 \\ 0 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$$

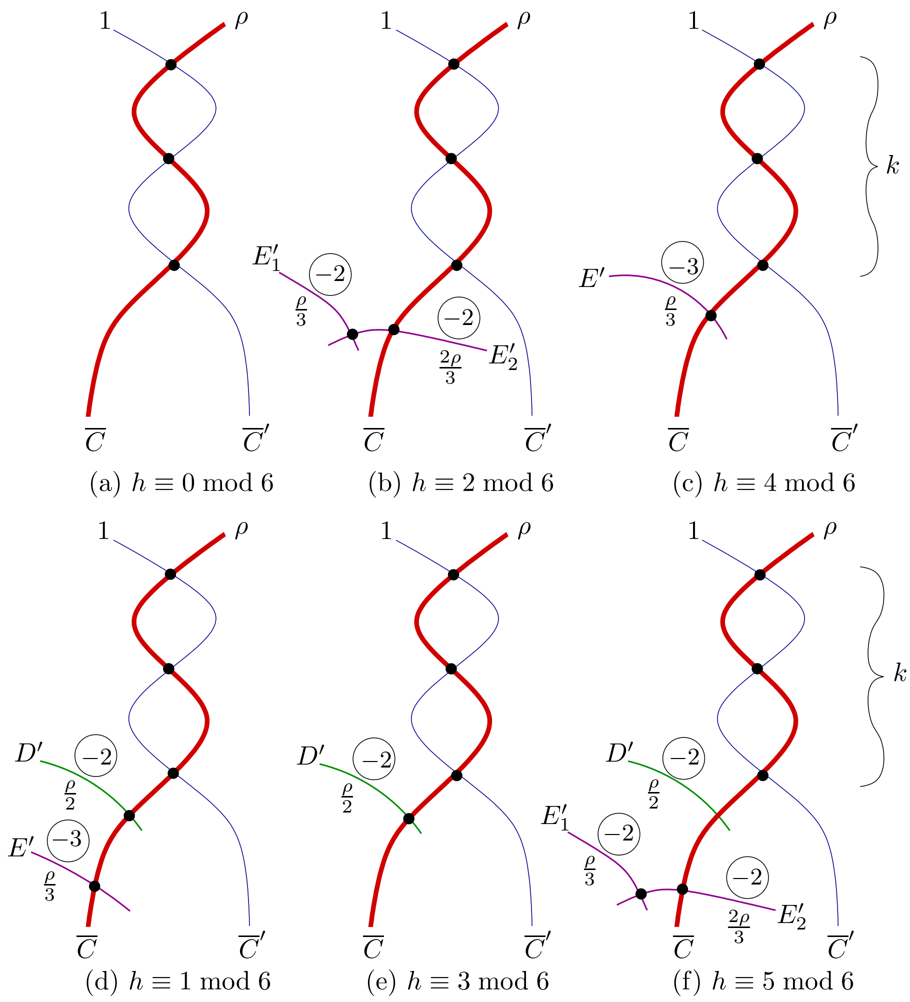


Figure 4: Minimal regular resolution $X_H(p)'$, $p = 12k + 1$, $k \geq 1$, $h = |H|$, $\rho = (p-1)/2h$

with absolute determinant $h/2 = |H|/\gcd(|H|,6)$, and the bottom two rows have $2 \times 2$ minors with gcd equal to 1. The cases $h \equiv 3,4 \bmod 6$ are even easier, since there are just two components to deal with, $\{\overline{C}, D'\}$ and $\{\overline{C}, E'\}$ with corresponding matrices

$$\begin{pmatrix} -(h+3)/6 & 1 \\ 1 & -2 \end{pmatrix}, \qquad \begin{pmatrix} -(h+2)/6 & 1 \\ 1 & -3 \end{pmatrix}$$

that yield the expected results.

For the final case $h \equiv -1 \bmod 6$, the submatrix indexed by the ordered set of components $\{\overline{C}, D', E_1', E_2'\}$ is

$$\begin{pmatrix} -(h+7)/6 & 1 & 0 & 1 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 1 & 0 & 1 & -2 \end{pmatrix}$$

with absolute determinant $h = |H|/\gcd(|H|,6)$ and gcd 1 for the $3 \times 3$ minors along the bottom three rows. The case $p \equiv 1 \bmod 12$ is now settled.

### 5.4 The cases $p \equiv \pm 5 \bmod 12$

With $p = 12k + 5$ for $k \geq 0$, we have $(p-1)/2 = 6k + 2$, so $h = |H|$ is not divisible by 3. Thus, the supersingular $j = 0$ is always non-regular and the ordinary $j = 1728$ is non-regular for even $h$.

Using Theorem 2.4.1 and Corollary 2.4.3, we obtain a minimal regular resolution depending on the possibilities for $h \bmod 6$ not divisible by 3, as given in Figure 5.

From Figure 5 one easily carries out the computations of the absolute determinant and the gcd of minors from the intersection matrix, just as we have done in earlier cases, and in all cases one gets $|H|/\gcd(|H|,6)$ for the absolute determinant and the gcd of the relevant minors is 1. Also, the case $h = 1$ has $\overline{C}$ as a $-1$-curve, and successive contractions end at an integral closed fiber, so we have established Theorems 1.1.2 and 1.1.6 for the case $p \equiv 5 \bmod 12$.

When $p = 12k - 5$ with $k \geq 1$, so $(p-1)/2 = 6k - 3$ is odd, we have that $h = |H|$ is odd. Thus, $j = 1728$ does give rise to a non-regular point, but the behavior at $j = 0$ depends on $h \bmod 6$. The usual applications of Jung–Hirzebruch resolution go through, and the minimal resolution has closed-fiber diagram as in Figure 6, depending on odd $h \bmod 6$, and both Theorem 1.1.2 and Theorem 1.1.6 drop out just as in the preceding cases.

## 6 The Arithmetic of $J_1(p)$

Our theoretical results concerning component groups inspired us to carry out some arithmetic computations in $J_1(p)$, and this section summarizes this work.

In Section 6.1 we recall the Birch and Swinnerton-Dyer conjecture, as this motivates many of our computations, and then we describe some of the theory

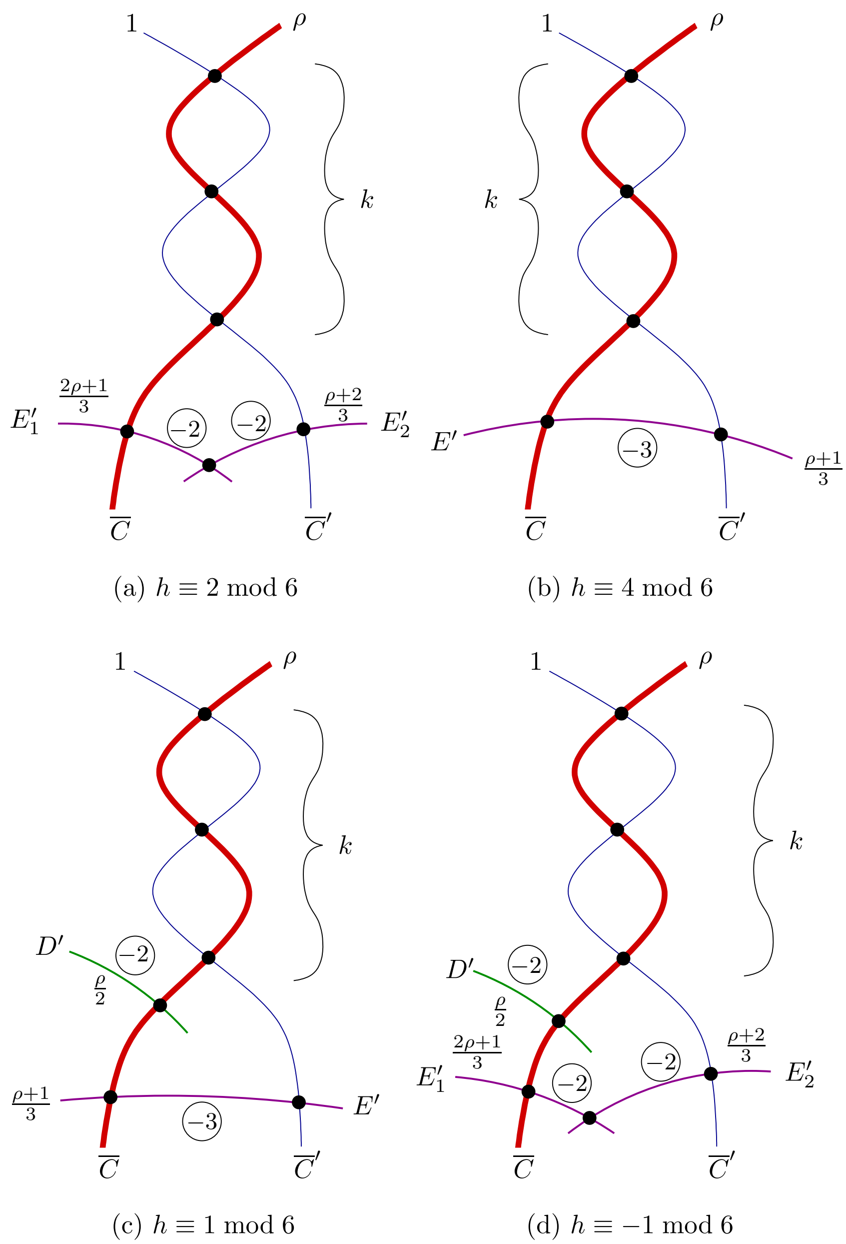


Figure 5: Minimal regular resolution $X_H(p)'$, $p = 12k + 5$, $k \geq 0$, $h = |H|$, $\rho = (p-1)/2h$

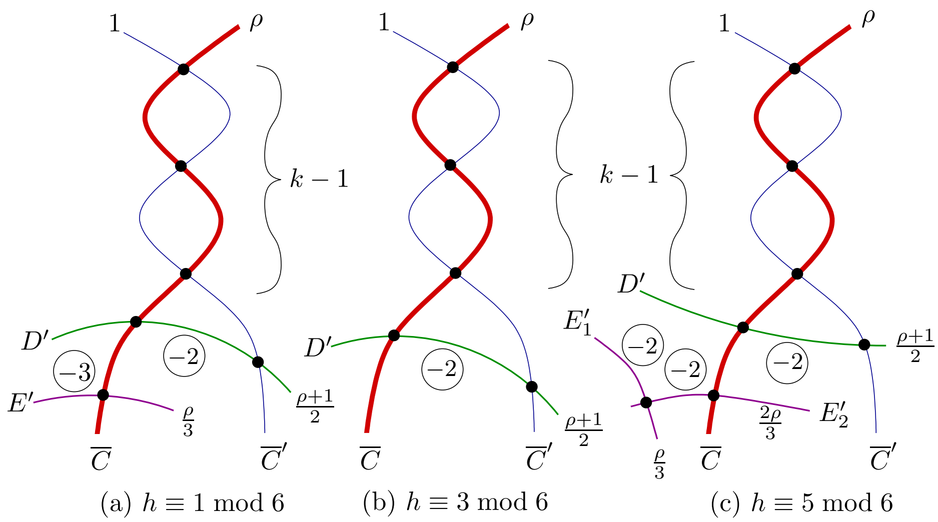


Figure 6: Minimal regular resolution $X_H(p)'$, $p = 12k-5$, $k \geq 1$, $h = |H|$, $\rho = (p-1)/2h$

behind the computations that went into computing the tables of Section 6.6. In Section 6.2 we find all $p$ such that $J_1(p)$ has rank 0. We next discuss tables of certain arithmetic invariants of $J_1(p)$ and we give a conjectural formula for $|J_1(p)(\mathbf{Q})_{\text{tor}}|$, along with some evidence. In Section 6.3 we investigate Jacobians of intermediate curves $J_H(p)$ associated to subgroups of $(\mathbf{Z}/p\mathbf{Z})^\times$, and in Section 6.4 we consider optimal quotients $A_f$ of $J_1(p)$ attached to newforms. In Section 6.4.1 we describe the lowest-level modular abelian variety that (assuming the Birch and Swinnerton-Dyer conjecture) should have infinite Mordell-Weil group but to which the general theorems of Kato, Kolyvagin, *et al.*, do not apply.

## 6.1 Computational methodology

We used the third author's modular symbols package for our computations; this package is part of [10] V2.10-6. See Section 6.5 for a description of how to use Magma to compute the tables. For the general theory of computing with modular symbols, see [14] and [63].

*Remark* 6.1.1. Many of the results of this section assume that a Magma program running on a computer executed correctly. Magma is complicated software that runs on physical hardware that is subject to errors from both programming mistakes and physical processes, such as cosmic radiation. We thus make the running *assumption* for the rest of this section that the computations below were performed correctly. To decrease the chance of hardware errors such as the famous Pentium bug (see [17]), we computed the tables in

Section 6.6 on three separate computers with different CPU architectures (an AMD Athlon 2000MP, a Sun Fire V480 which was donated to the third author by Sun Microsystems, and an Intel Pentium 4-M laptop).

Let $A$ be a modular abelian variety over $\mathbf{Q}$, *i.e.*, a quotient of $J_1(N)$ for some $N$. We will make frequent reference to the following special case of the general conjectures of Birch and Swinnerton-Dyer:

CONJECTURE 6.1.2 (BSD CONJECTURE). *Let $Ш(A)$ be the Shafarevich-Tate group of $A$, let $c_p = |\Phi_{A,p}(\mathbf{F}_p)|$ be the Tamagawa number at $p$ for $A$, and let $\Omega_A$ be the volume of $A(\mathbf{R})$ with respect to a generator of the invertible sheaf of top-degree relative differentials on the Néron model $A_{/\mathbf{Z}}$ of $A$ over $\mathbf{Z}$. Let $A^\vee$ denote the abelian variety dual of $A$. The group $Ш(A)$ is finite and*

$$\frac{L(A,1)}{\Omega_A} = \frac{|Ш(A)| \cdot \prod_{p|N} c_p}{|A(\mathbf{Q})| \cdot |A^\vee(\mathbf{Q})|},$$

*where we interpret the right side as $0$ in case $A(\mathbf{Q})$ is infinite.*

*Remark* 6.1.3. The hypothesis that $A$ is modular implies that $L(A,s)$ has an analytic continuation to the whole complex plane and a functional equation of a standard type. In particular, $L(A,1)$ makes sense. Also, when $L(A,1) \neq 0$, [32, Cor. 14.3] implies that $Ш(A)$ is finite.

Let $\{f_1,\ldots,f_n\}$ be a set of newforms in $S_2(\Gamma_1(N))$ that is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-stable. Let $I$ be the Hecke-algebra annihilator of the subspace generated by $f_1,\ldots,f_n$. *For the rest of Section* 6.1, *we assume that $A = A_I = J_1(N)/IJ_1(N)$ for such an $I$.* Note that $A$ is an *optimal quotient* in the sense that $IJ_1(N) = \ker(J_1(N) \to A)$ is an abelian subvariety of $J_1(N)$.

### 6.1.1 BOUNDING THE TORSION SUBGROUP

To obtain a multiple of the order of the torsion subgroup $A(\mathbf{Q})_{\mathrm{tor}}$, we proceed as follows. For any prime $\ell \nmid N$, the algorithm of [3, §3.5] computes the characteristic polynomial $f \in \mathbf{Z}[X]$ of $\mathrm{Frob}_\ell$ acting on any $p$-adic Tate module of $A$ with $p \neq \ell$. To compute $|A(\mathbf{F}_\ell)|$, we observe that

$$|A(\mathbf{F}_\ell)| = \deg(\mathrm{Frob}_\ell - 1) = \det(\mathrm{Frob}_\ell - 1),$$

and this is the value of the characteristic polynomial of $\mathrm{Frob}_\ell$ at 1. For any prime $\ell \nmid 2N$, the reduction map $A(\mathbf{Q})_{\mathrm{tor}} \to A(\mathbf{F}_\ell)$ is injective, so $|A(\mathbf{Q})_{\mathrm{tor}}|$ divides

$$T = \gcd\{|A(\mathbf{F}_\ell)| : \ \ell < 60 \text{ and } \ell \nmid 2N\}.$$

(If $N$ is divisible by all primes up to 60, let $T = 0$. In all of the examples in this paper, $N$ is prime and so $T \neq 0$.) The injectivity of reduction mod $\ell$ on the finite group $A(\mathbf{Q})_{\mathrm{tor}}$ for any prime $\ell \neq 2$ is well known and follows from the determination of the torsion in a formal group (see, *e.g.*, the appendix to [33] and [59, §IV.6–9]).

The cardinality $|A(\mathbf{F}_\ell)|$ does not change if $A$ is replaced by a $\mathbf{Q}$-isogenous abelian variety $B$, so we do not expect in general that $|A(\mathbf{Q})_{\mathrm{tor}}| = T$. (For much more on relationships between $|A(\mathbf{Q})_{\mathrm{tor}}|$ and $T$, see [33, p. 499].) When we refer to an upper bound on torsion, $T$ is the (multiplicative) upper bound that we have in mind.

The number 60 has no special significance; we had to make some choice to do computations, and in practice the sequence of partial gcd's rapidly stabilizes. For example, if $A = J_1(37)$, then the sequence of partial gcd's is:

$$15249085236272475, 802583433488025, 160516686697605, \ldots$$

where the term 160516686697605 repeats for all $\ell < 1000$.

### 6.1.2 The Manin index

Let $p$ be a prime, let $\Omega_{A/\mathbf{Z}}$ denote the sheaf of relative 1-forms on the Néron model of $A$ over $\mathbf{Z}$, and let $I$ be the annihilator of $A$ in the Hecke algebra $\mathbf{T} \subset \mathrm{End}(J_1(N))$. For a subring $R \subset \mathbf{C}$, let $S_2(\Gamma_1(N), R)$ be the $R$-module of cusp forms whose Fourier expansion at $\infty$ lies in $R[\![q]\!]$. The natural surjective Hecke-equivariant morphism $J_1(N) \to J_1(N)/IJ_1(N) = A$ induces (by pullback) a Hecke-equivariant injection $\Psi_A : \mathrm{H}^0(A_{/\mathbf{Z}}, \Omega_{A/\mathbf{Z}}) \hookrightarrow S_2(\Gamma_1(N), \mathbf{Q})$ whose image lies in $S_2(\Gamma_1(N), \mathbf{Q})[I]$. (Here we identify $S_2(\Gamma_1(N), \mathbf{Q})$ with $\mathrm{H}^0(X_1(N), \Omega_{X_1(N)/\mathbf{Q}}) = \mathrm{H}^0(J_1(N), \Omega_{J_1(N)/\mathbf{Q}})$ in the usual manner.)

Definition 6.1.4 (Manin index). The *Manin index of $A$* is

$$c = [S_2(\Gamma_1(N), \mathbf{Z})[I] : \Psi_A(\mathrm{H}^0(A_{/\mathbf{Z}}, \Omega_{A/\mathbf{Z}}))] \in \mathbf{Q}.$$

*Remark* 6.1.5. We name $c$ after Manin, since he first studied $c$, but only in the context of elliptic curves. When $X_0(N) \to A$ is an optimal elliptic-curve quotient attached to a newform $f$, the usual Manin constant of $A$ is the rational number $c$ such that $\pi^*(\omega_A) = \pm c \cdot f \mathrm{d}q/q$, where $\omega_A$ is a basis for the differentials on the Néron model of $A$. The usual Manin constant equals the Manin index, since $S_2(\Gamma_1(N), \mathbf{Z})[I]$ is generated as a $\mathbf{Z}$-module by $f$.

*A priori*, the index in Definition 6.1.4 is only a generalized lattice index in the sense of [12, Ch. 1, §3], which we interpret as follows. In [12], for any Dedekind domain $R$, the *lattice index* is defined for any two finite free $R$-modules $V$ and $W$ of the same rank $\rho$ that are embedded in a $\rho$-dimensional $\mathrm{Frac}(R)$-vector space $U$. The lattice index is the fractional $R$-ideal generated by the determinant of any automorphism of $U$ that sends $V$ isomorphically onto $W$. In Definition 6.1.4, we take $R = \mathbf{Z}$, $U = S_2(\Gamma_1(N), \mathbf{Q})[I]$, $V = S_2(\Gamma_1(N), \mathbf{Z})[I]$, and $W = \Psi_A(\mathrm{H}^0(A_{/\mathbf{Z}}, \Omega_{A/\mathbf{Z}}))$. Thus, $c$ is the absolute value of the determinant of any linear transformation of $S_2(\Gamma_1(N), \mathbf{Q})[I]$ that sends $S_2(\Gamma_1(N), \mathbf{Z})[I]$ onto $\Psi_A(\mathrm{H}^0(A_{/\mathbf{Z}}, \Omega_{A/\mathbf{Z}}))$. In fact, it is not necessary to consider lattice indexes, as the following lemma shows (note we will use lattices indices later in the statement of Proposition 6.1.10).

Lemma 6.1.6. *The Manin index $c$ of $A$ is an integer.*

*Proof.* Let $X_\mu(N)$ be the coarse moduli scheme over $\mathbf{Z}$ that classifies isomorphism classes of pairs $(E/S, \alpha)$, with $\alpha : \mu_N \hookrightarrow E^{\mathrm{sm}}$ a closed subgroup in the smooth locus of a generalized elliptic curve $E$ with irreducible geometric fibers $E_s$. This is a smooth $\mathbf{Z}$-curve that is not proper, and it is readily constructed by combining the work of Katz-Mazur and Deligne-Rapoport (see §9.3 and §12.3 of [16]). There is a canonical $\mathbf{Z}$-point $\infty \in X_\mu(N)(\mathbf{Z})$ defined by the standard 1-gon equipped with the canonical embedding of $\mu_N$ into the smooth locus $\mathbf{G}_m$, and the theory of the Tate curve provides a canonical isomorphism between $\mathrm{Spf}(\mathbf{Z}[\![q]\!])$ and the formal completion of $X_\mu(N)$ along $\infty$.

There is an isomorphism between the smooth proper curves $X_1(N)$ and $X_\mu(N)$ over $\mathbf{Z}[1/N]$ because the open modular curves $Y_1(N)$ and $Y_\mu(N)$ coarsely represent moduli problems that may be identified over the category of $\mathbf{Z}[1/N]$-schemes via the map

$$(E, P) \mapsto (E/\langle P\rangle, E[N]/\langle P\rangle),$$

where $E[N]/\langle P\rangle$ is identified with $\mu_N$ via the Weil pairing on $E[N]$. For our purposes, the key point (which follows readily from Tate's theory) is that under the moduli-theoretic identification of the analytification of the $\mathbf{C}$-fiber of $X_\mu(N)$ with the analytic modular curve $X_1(N)$ via the trivialization of $\mu_N(\mathbf{C})$ by means of $\zeta_N = e^{\pm 2\pi\sqrt{-1}/N}$, the formal parameter $q$ at the $\mathbf{C}$-point $\infty$ computes the standard analytic $q$-expansion for weight-2 cusp forms on $\Gamma_1(N)$. The reason we consider $X_\mu(N)$ rather than $X_1(N)$ is simply because we want a smooth $\mathbf{Z}$-model in which the analytic cusp $\infty$ descends to a $\mathbf{Z}$-point.

Let $\phi : J_1(N) \to A$ be the Albanese quotient map over $\mathbf{Q}$, and pass to Néron models over $\mathbf{Z}$ (without changing the notation). Since $X_\mu(N)$ is $\mathbf{Z}$-smooth, there is a morphism $X_\mu(N) \to J_1(N)$ over $\mathbf{Z}$ that extends the usual morphism sending $\infty$ to 0. We have a map $\Psi : \mathrm{H}^0(A, \Omega) \to \mathbf{Z}[\![q]\!]\mathrm{d}q/q$ of $\mathbf{Z}$-modules defined by composition

$$\mathrm{H}^0(A, \Omega) \to \mathrm{H}^0(J_1(N), \Omega) \to \mathrm{H}^0(X_\mu(N), \Omega) \xrightarrow{q-\exp} \mathbf{Z}[\![q]\!]\frac{\mathrm{d}q}{q}.$$

The map $\Psi$ is injective, since it is injective after base extension to $\mathbf{Q}$ and each group above is torsion free. The image of $\Psi$ in $\mathbf{Z}[\![q]\!]\mathrm{d}q/q$ is a finite free $\mathbf{Z}$-module, contained in the image of $S = S_2(\Gamma_1(N), \mathbf{Z})$, the sub-$\mathbf{Z}$-module of $S_2(\Gamma_1(N), \mathbf{C})$ of those elements whose analytic $q$-expansion at $\infty$ has coefficients in $\mathbf{Z}$. Since $\Psi$ respects the action of Hecke operators, the image of $\Psi$ is contained in $S[I]$, so the lattice index $c$ is an integer. □

We make the following conjecture:

Conjecture 6.1.7. *If $A = A_f$ is a quotient of $J_1(N)$ attached to a single Galois-conjugacy class of newforms, then $c = 1$.*

Manin made this conjecture for one-dimensional optimal quotients of $J_0(N)$. Mazur bounded $c$ in some cases in [46], Stevens considered $c$ for one-dimensional quotients of $J_1(N)$ in [65], González and Lario considered $c$ for $\mathbf{Q}$-curves in [26], Agashe and Stein considered $c$ for quotients of $J_0(N)$ of dimension bigger than 1 in [4], and Edixhoven proved integrality results in [19, Prop. 2] and [22, §2].

*Remark* 6.1.8. We only make Conjecture 6.1.7 when $A$ is attached to a *single* Galois-conjugacy class of newforms, since the more general conjecture is false. Adam Joyce [31] has recently used failure of multiplicity one for $J_0(p)$ to produce examples of optimal quotients $A$ of $J_1(p)$, for $p = 431$, 503, and 2089, whose Manin indices are divisible by 2. Here, $A$ is isogenous to a product of two elliptic curves, so $A$ is not attached to a single Galois-orbit of newforms.

*Remark* 6.1.9. The question of whether or not $c$ is an isogeny-invariant is not meaningful in the context of this paper because we only define the Manin index for optimal quotients.

### 6.1.3 Computing $L$-ratios

There is a formula for $L(A_f, 1)/\Omega_{A_f}$ in [3, §4.2] when $A_f$ is an optimal quotient of $J_0(N)$ attached to a single Galois conjugacy class of newforms. In this section we describe that formula; it applies to our quotient $A$ of $J_1(N)$.

Recall our running hypothesis that $A = A_I$ is an optimal (new) quotient of $J_1(N)$ attached to a Galois conjugacy class of newforms $\{f_1, \ldots, f_n\}$. Let

$$\Psi : \mathrm{H}_1(X_1(N), \mathbf{Q}) \to \mathrm{Hom}(S_2(\Gamma_1(N))[I], \mathbf{C})$$

be the linear map that sends a rational homology class $\gamma$ to the functional $\int_\gamma$ on the subspace $S_2(\Gamma_1(N))[I]$ in the space of holomorphic 1-forms on $X_1(N)$.

Let $\mathbf{T} \subset \mathrm{End}(\mathrm{H}_1(X_1(N), \mathbf{Q}))$ be the ring generated by all Hecke operators. Since the $\mathbf{T}$-module $H = \mathrm{Hom}(S_2(\Gamma_1(N))[I], \mathbf{C})$ has a natural $\mathbf{R}$-structure (and even a natural $\mathbf{Q}$-structure), it admits a natural $\mathbf{T}$-linear and $\mathbf{C}$-semilinear action by complex conjugation. If $M$ is a $\mathbf{T}$-submodule of $H$, let $M^+$ denote the $\mathbf{T}$-submodule of $M$ fixed by complex conjugation.

Let $c$ be the Manin index of $A$ as in Section 6.1.2, let $c_\infty$ be the number of connected components of $A(\mathbf{R})$, let $\Omega_A$ be the volume of $A(\mathbf{R})$ as in Conjecture 6.1.2, and let $\{0, \infty\} \in \mathrm{H}_1(X_1(N), \mathbf{Q})$ be the rational homology class whose integration functional is integration from 0 to $i\infty$ along the $i$-axis (for the precise definition of $\{0, \infty\}$ and a proof that it lies in the rational homology see [38, Ch. IV §1–2]).

PROPOSITION 6.1.10. *Let $A = A_I$ be an optimal quotient of $J_1(N)$ attached to a Galois-stable collection of newforms. With notation as above, we have*

$$c_\infty \cdot c \cdot \frac{L(A,1)}{\Omega_A} = [\Psi(\mathrm{H}_1(X_1(N), \mathbf{Z}))^+ : \Psi(\mathbf{T}\{0, \infty\})], \tag{6.1.1}$$

*where the index is a lattice index as discussed in Section* 6.1.7 (*in particular,* $L(A, 1) = 0$ *if and only if* $\Psi(\mathbf{T}\{0, \infty\})$ *has smaller rank than* $\mathrm{H}_1(X_1(N), \mathbf{Z})^+$).

*Proof.* It is straightforward to adapt the argument of [3, §4.2] with $J_0(N)$ replaced by $J_1(N)$ (or even $J_H(N)$), but one must be careful when replacing $A_f$ with $A$. The key observation is that if $f_1, \ldots, f_n$ is the unique basis of normalized newforms corresponding to $A$, then $L(A, s) = L(f_1, s) \cdots L(f_n, s)$. □

*Remark* 6.1.11. This equality (6.1.1) need not hold if oldforms are involved, even in the $\Gamma_0(N)$ case. For example, if $A = J_0(22)$, then $L(A, s) = L(J_0(11), s)^2$, but two copies of the newform corresponding to $J_0(11)$ do not form a basis for $S_2(\Gamma_0(22))$.

We finish this section with some brief remarks on how to compute the rational number $c \cdot L(A, 1)/\Omega_A$ using (6.1.1) and a computer. Using modular symbols, one can explicitly compute with $\mathrm{H}_1(X_1(N), \mathbf{Z})$. Though the above lattice index involves two lattices in a complex vector space, the index is unchanged if we replace $\Psi$ with any linear map to a $\mathbf{Q}$-vector space such that the kernel is unchanged (see [3, §4.2]). Such a map may be computed via standard linear algebra by finding a basis for $\mathrm{Hom}(\mathrm{H}_1(X_1(N), \mathbf{Q}), \mathbf{Q})[I]$.

To compute $c_\infty$, use the following well-known proposition; we include a proof for lack of an adequate published reference.

Proposition 6.1.12. *For an abelian variety $A$ over $\mathbf{R}$,*

$$c_\infty = 2^{\dim_{\mathbf{F}_2} A[2](\mathbf{R}) - d},$$

*where $d = \dim A$ and $c_\infty := |A(\mathbf{R})/A^0(\mathbf{R})|$.*

*Proof.* Let $\Lambda = \mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$, so the exponential uniformization of $A(\mathbf{C})$ provides a short exact sequence

$$0 \to \Lambda \to \mathrm{Lie}(A(\mathbf{C})) \to A(\mathbf{C}) \to 0.$$

There is an evident action of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ on all terms via the action on $A(\mathbf{C})$, and this short exact sequence is Galois-equivariant because $A$ is defined over $\mathbf{R}$. Let $\Lambda^+$ be the subgroup of Galois-invariants in $\Lambda$, so we get an exact cohomology sequence

$$0 \to \Lambda^+ \to \mathrm{Lie}(A(\mathbf{R})) \to A(\mathbf{R}) \to \mathrm{H}^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \Lambda) \to 0$$

because higher group cohomology for a finite group vanishes on a $\mathbf{Q}$-vector space (such as the Lie algebra of $A(\mathbf{C})$). The map $\mathrm{Lie}(A(\mathbf{R})) \to A(\mathbf{R})$ is the exponential map for $A(\mathbf{R})$, and so its image is $A(\mathbf{R})^0$. Thus, $\Lambda^+$ has $\mathbf{Z}$-rank equal to $\dim A$ and

$$A(\mathbf{R})/A(\mathbf{R})^0 \simeq \mathrm{H}^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \Lambda).$$

To compute the size of this $\mathrm{H}^1$, consider the short exact sequence

$$0 \to \Lambda \xrightarrow{2} \Lambda \to \Lambda/2\Lambda \to 0$$

of Galois-modules. Since $\Lambda/n\Lambda \simeq A[n](\mathbf{C})$ as Galois-modules for any $n \neq 0$, the long-exact cohomology sequence gives an isomorphism

$$A[2](\mathbf{R})/(\Lambda^+/2\Lambda^+) \simeq \mathrm{H}^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), \Lambda).$$

□

*Remark* 6.1.13. Since the canonical isomorphism

$$A[n](\mathbf{C}) \simeq \mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})/n\mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$$

is $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-equivariant, we can identify $A[2](\mathbf{R})$ with the kernel of $\overline{\tau} - 1$ where $\overline{\tau}$ is the mod-2 reduction of the involution on $\mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$ induced by the action $\tau$ of complex conjugation on $A(\mathbf{C})$. In the special case when $A$ is a quotient of some $J_1(N)$, and we choose a connected component of $\mathbf{C} - \mathbf{R}$ to uniformize $Y_1(N)$ in the usual manner, then via the $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-equivariant isomorphism $\mathrm{H}_1(J_1(N)(\mathbf{C}), \mathbf{Z}) \simeq \mathrm{H}_1(X_1(N)(\mathbf{C}), \mathbf{Z})$ we see that $\mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$ may be computed by modular symbols and that the action of $\tau$ on the modular symbol is $\{\alpha, \beta\} \mapsto \{-\alpha, -\beta\}$. This makes $A[2](\mathbf{R})$, and hence $c_\infty$, readily computable via modular symbols.

## 6.2 Arithmetic of $J_1(p)$

### 6.2.1 The Tables

For $p \leq 71$, the first part of Table 1 (on page 393) lists the dimension of $J_1(p)$ and the rational number $L = c \cdot L(J_1(p), 1)/\Omega_{J_1(p)}$. Table 1 also gives an upper bound $T$ (in the sense of divisibility) on $|J_1(p)(\mathbf{Q})_{\mathrm{tor}}|$ for $p \leq 71$, as discussed in §6.1.1.

When $L \neq 0$, Conjecture 6.1.2 and the assumption that $c = 1$ imply that the numerator of $L$ divides $c_p \cdot |\text{Ш}(A)|$, that in turn divides $T^2L$. For every $p \neq 29$ with $p \leq 71$, we found that $T^2L = 1$. For $p = 29$, we have $T^2L = 2^{12}$; it would be interesting if the isogeny-invariant $T$ overestimates the order of $J_1(29)(\mathbf{Q})_{\mathrm{tor}}$ or if $\text{Ш}(J_1(29))$ is nontrivial.

### 6.2.2 Determination of positive rank

Proposition 6.2.1. *The primes $p$ such that $J_1(p)$ has positive rank are the same as the primes for which $J_0(p)$ has positive rank:*

$$p = 37, 43, 53, 61, 67, \ \textit{and all } p \geq 73.$$

*Proof.* Proposition 2.8 of [45, §III.2.2, p. 147] says: "Suppose $g^+ > 0$ (which is the case for all $N > 73$, as well as $N = 37, 43, 53, 61, 67$). Then the Mordell-Weil group of $J_+$ is a torsion-free group of infinite order (*i.e.* of positive rank)." Here, $N$ is a prime, $g^+$ is the genus of the Atkin-Lehner quotient $X_0(N)^+$ of $X_0(N)$, and $J_+$ is isogenous to the Jacobian of $X_0(N)^+$. This is essentially correct, except for the minor oversight that $g^+ > 0$ also when $N = 73$ (this is stated correctly on page 34 of [45]).

By Mazur's proposition $J_0(p)$ has positive algebraic rank for all $p \geq 73$ and for $p = 37, 43, 53, 61, 67$. The sign in the functional equation for $L(J_+, s)$ is $-1$, so

$$L(J, 1) = L(J_+, 1)L(J_-, 1) = 0 \cdot L(J_-, 1) = 0$$

for all $p$ such that $g^+ > 0$. Using (6.1.1) we see that $L(J, 1) \neq 0$ for all $p$ such that $g^+ = 0$, which by Kato (see [32, Cor. 14.3]) or Kolyvagin–Logachev (see [36]) implies that $J$ has rank 0 whenever $g^+ = 0$. Thus $L(J_0(p), 1) = 0$ if and only if $J_0(p)$ has positive rank.

Work of Kato (see [32, Cor. 14.3]) implies that if $J_1(p)$ has analytic rank 0, then $J_1(p)$ has algebraic rank 0. It thus suffices to check that $L(J_1(p), 1) \neq 0$ for the primes $p$ such that $J_0(p)$ has rank 0. We verify this by computing $c \cdot L(J_1(p), 1)/\Omega_{J_1(p)}$ using (6.1.1), as illustrated in Table 1.

□

If we instead consider composite level, it is not true that $J_0(N)$ has positive analytic rank if and only if $J_1(N)$ has positive analytic rank. For example, using (6.1.1) we find that $J_0(63)$ has analytic rank 0, but $J_1(63)$ has positive analytic rank. Closer inspection using Magma (see the program below) shows that there is a two-dimensional new quotient $A_f$ with positive analytic rank, where $f = q + (\omega - 1)q^2 + (-\omega - 2)q^3 + \cdots$, and $\omega^3 = 1$. It would be interesting to prove that that the algebraic rank of $A_f$ is positive.

```
> M := ModularSymbols(63,2);
> S := CuspidalSubspace(M);
> LRatio(S,1);       // So J_0(63) has rank 0
1/384

> G<a,b> := DirichletGroup(63,CyclotomicField(6));
> e := a^5*b;
> M := ModularSymbols([e],2,+1);
> S := CuspidalSubspace(M);
> LRatio(S,1);     // This step takes some time.
0
> D := NewformDecomposition(S);
> LRatio(D[1],1);
0
> qEigenform(D[1],5);
q + (-2*zeta_6 + 1)*q^2 + (-2*zeta_6 + 1)*q^3 - q^4 + O(q^5)
```

### 6.2.3 Conjectural order of $J_1(\mathbf{Q})_{\rm tor}$

For any Dirichlet character $\varepsilon$ modulo $N$, define Bernoulli numbers $B_{2,\varepsilon}$ by

$$\sum_{a=1}^{N} \frac{\varepsilon(a) t e^{at}}{e^{Nt}-1} = \sum_{k=0}^{\infty} \frac{B_{k,\varepsilon}}{k!} t^k.$$

We make the following conjecture.

Conjecture 6.2.2. *Let $p \geq 5$ be prime. The rational torsion subgroup $J_1(p)(\mathbf{Q})_{\rm tor}$ is generated by the differences of $\mathbf{Q}$-rational cusps on $X_1(p)$. Equivalently (see below), for any prime $p \geq 5$,*

$$|J_1(p)(\mathbf{Q})_{\rm tor}| = \frac{p}{2^{p-3}} \cdot \prod_{\varepsilon \neq 1} B_{2,\varepsilon} \qquad (6.2.1)$$

*where the product is over the nontrivial even Dirichlet characters $\varepsilon$ of conductor dividing $p$.*

Due to how we defined $X_1(p)$, its $\mathbf{Q}$-rational cusps are exactly its cusps lying over the cusp $\infty \in X_0(p)(\mathbf{Q})$ (corresponding to the standard 1-gon equipped with the subgroup $\mu_p$ in its smooth locus $\mathbf{G}_m$) via the second standard degeneracy map

$$(E, P) \mapsto (E/\langle P\rangle, E[p]/\langle P\rangle).$$

In [49] Ogg showed that $|J_1(13)(\mathbf{Q})| = 19$, verifying Conjecture 6.2.2 for $p = 13$. The results of [37] are also relevant to Conjecture 6.2.2, and suggest that the rational torsion of $J_1(p)$ is cuspidal. Let $C(p)$ be the conjectural order of $J_1(p)(\mathbf{Q})_{\rm tor}$ on the right side of (6.2.1). In [37, p. 153], Kubert and Lang prove that $C(p)$ is equal to the order of the group generated by the differences of $\mathbf{Q}$-rational cusps on $X_1(p)$ (in their language, these are viewed as the cusps that lie over $0 \in X_0(p)(\mathbf{Q})$ via the first standard degeneracy map

$$(E, P) \mapsto (E, \langle P\rangle)),$$

and so $C(p)$ is *a priori* an integer that moreover divides $|J_1(p)(\mathbf{Q})_{\rm tor}|$.

Table 1 provides evidence for Conjecture 6.2.2. Let $T(p)$ be the upper bound on $J_1(p)(\mathbf{Q})_{\rm tor}$ (see Table 1). For all $p \leq 157$, we have $C(p) = T(p)$ except for $p = 29$, 97, 101, 109, and 113, where $T(p)/C(p)$ is $2^6$, 17, $2^4$, $3^7$, and $2^{12} \cdot 3^2$, respectively. Thus Conjecture 6.2.2 is true for $p \leq 157$, except possibly in these five cases, where the deviation is consistent with the possibility that $T(p)$ is a nontrivial multiple of the true order of the torsion subgroup (recall that $T(p)$ is an isogeny-invariant, and so it is not surprising that it may be too large).

## 6.3 Arithmetic of $J_H(p)$

For each divisor $d$ of $p-1$, let $H = H_d$ denote the unique subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$ of order $(p-1)/d$. The group of characters whose kernel contains $H_d$ is exactly the group of characters of order dividing $d$. Since the linear fractional transformation associated to $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$ acts trivially on the upper half plane, we lose nothing (for the computations that we will do in this section) if we assume that $-1 \in H$, and so $|H|$ is even.

For any subgroup $H$ of $(\mathbf{Z}/p\mathbf{Z})^\times$ as above, let $J_H$ be the Jacobian of $X_H(p)$, as in Section 1. For each $p \leq 71$, Table 2 lists the dimension of $J_H = J_H(p)$, the rational number $L = c \cdot L(J_H, 1)/\Omega_{J_H}$, an upper bound $T$ on $|J_H(\mathbf{Q})_{\mathrm{tor}}|$, the conjectural multiple $T^2 L$ of $|Ш(J_H)| \cdot c_p$, and $c_p = |\Phi(J_H)|$. We compute $|\Phi(J_H)(\mathbf{F}_p)| = |\Phi(J_H)(\overline{\mathbf{F}}_p)|$ using Theorem 1.1.3. Note that Table 2 omits the data for $d = (p-1)/2$, since $J_H = J_1(p)$ for such $d$, so the corresponding data is therefore already contained in Table 1.

When $L \neq 0$, we have $T^2 L = |\Phi(J_H)|$ in all but one case. The exceptional case is $p = 29$ and $d = 7$, where $T^2 L = 2^6$, but $|\Phi(J_H)| = 1$; probably $T$ overestimates the torsion in this case. In the following proposition we use this observation to deduce that $|Ш(J_H)| = c = 1$ in some cases.

PROPOSITION 6.3.1. *Suppose that $p \leq 71$ is a prime and $d \mid (p-1)$ with $(p-1)/d$ even. Let $J_H$ be the Jacobian of $X_H(p)$, where $H$ is the subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$ of order $(p-1)/d$. Assume that Conjecture* 6.1.2 *is true, and if $p = 29$ then assume that $d \neq 7, 14$. If $L(J_H, 1) \neq 0$, then $|Ш(J_H)| = 1$ and $c = 1$.*

It is not interesting to remove the condition $p \leq 71$ in the statement of the proposition, since when $p > 71$ the quantity $L(J_H, 1)$ automatically vanishes (see Proposition 6.2.1). It is probably not always the case that $|Ш(J_H)| = 1$; for example, Conjecture 6.1.2 and the main result of [1] imply that $7^2$ divides $|Ш(J_0(1091))|$.

*Proof.* We deduce the proposition from Tables 1–3 as follows. Using Conjecture 6.1.2 we have

$$c \cdot |Ш(J_H)| = c \cdot \frac{L(J_H, 1)}{\Omega_{J_H} \cdot |\Phi(J_H)|} \cdot |J_H(\mathbf{Q})_{\mathrm{tor}}|^2. \tag{6.3.1}$$

Let $T$ denote the torsion bound on $J_H(\mathbf{Q})_{\mathrm{tor}}$ as in Section 6.1.1 and let $L = c \cdot L(J_H, 1)/\Omega_{J_H}$, so the right side of (6.3.1) divides $T^2 L/|\Phi(J_H)|$. An inspection of the tables shows that $T^2 L/|\Phi(J_H)| = 1$ for $J_H$ satisfying the hypothesis of the proposition (in the excluded cases $p = 29$ and $d = 7, 14$, the quotient equals $2^6$ and $2^{12}$, respectively). Since $c \in \mathbf{Z}$, we conclude that $c = |Ш(J_H)| = 1$.

$\square$

*Remark* 6.3.2. Theorem 1.1.3 is an essential ingredient in the proof of Proposition 6.3.1 because we used Theorem 1.1.3 to compute the Tamagawa factor $c_p$.

### 6.4 Arithmetic of newform quotients

Tables 4–5 at the end of this paper contain arithmetic information about each newform abelian variety quotient $A_f$ of $J_1(p)$ with $p \leq 71$.

The first column gives a label determining a Galois-conjugacy class of newforms $\{f, \ldots\}$, where **A** corresponds to the first class, **B** to the second, *etc.*, and the classes are ordered first by dimension and then in lexicographical order by the sequence of nonegative integers $|\operatorname{tr}(a_2(f))|, |\operatorname{tr}(a_3(f))|, |\operatorname{tr}(a_5(f))|, \ldots$. (WARNING: This ordering does not agree with the one used by Cremona in [14]; for example, our **37A** is Cremona's **37B**.) The next two columns list the dimension of $A_f$ and the order of the Nebentypus character of $f$, respectively. The fourth column lists the rational number $L = L(A_f, 1)/\Omega_{A_f}$, and the fifth lists the product $T^2L$, where $T$ is an upper bound (as in Section 6.1.1) on the order of $A_f(\mathbf{Q})_{\mathrm{tor}}$. The sixth column, labeled "modular kernel", lists invariants of the group of $\overline{\mathbf{Q}}$-points of the kernel of the polarization $A_f^\vee \hookrightarrow J_1(p) \to A_f$; this kernel is computed by using an algorithm based on Proposition 6.4.1 below. The elementary divisors of the kernel are denoted with notation such as $[2^2 14^2]$ to denote

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/14\mathbf{Z} \times \mathbf{Z}/14\mathbf{Z}.$$

Proposition 6.4.1. *Suppose $A = A_I$ is an optimal quotient of $J = J_1(N)$ attached to the annihilator $I$ of a Galois-stable collection of newforms. The group of $\overline{\mathbf{Q}}$-points of the kernel of the natural map $A^\vee \hookrightarrow J \to A$ is isomorphic to the cokernel of the natural map*

$$\operatorname{Hom}(\mathrm{H}_1(X_1(N), \mathbf{Z}), \mathbf{Z})[I] \to \operatorname{Hom}(\mathrm{H}_1(X_1(N), \mathbf{Z})[I], \mathbf{Z}).$$

*Proof.* The proof is the same as [35, Prop. 1]. □

It is possible to compute the modular kernel by using the formula in this proposition, together with modular symbols and standard algorithms for computing with finitely generated abelian groups.

We do not give $T$ in Tables 4–5, since in all but six cases $T^2L \neq 0$, hence $T^2L$ and $L$ determine $T$. The remaining six cases are **37B**, **43A**, **53A**, **61A**, **61B**, and **67C**, and in all these cases $T = 1$.

*Remark* 6.4.2. If $A = A_f$ is an optimal quotient of $J_1(p)$ attached to a newform, then the tables do not include the toric, additive, and abelian ranks of the closed fiber of the Néron model of $A$ over $\mathbf{F}_p$, since they are easy to determine from other data about $A$ as follows. If $\varepsilon(f) = 1$, then the toric rank is $\dim(A)$, since $A$ is isogenous to an abelian subvariety of $J_0(p)$ and so $A$ has purely toric reduction over $\mathbf{Z}_p$. Now suppose that $\varepsilon(f)$ is nontrivial, so $A$ is isogenous to an abelian subvariety of the abelian variety $J_1(p)/J_0(p)$ that has potentially good reduction at $p$. Hence the toric rank of $A$ is zero, and inertia $I_p \subset G_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts with finite image on the $\mathbf{Q}_\ell$-adic Tate module $V_\ell$ of $A$ for any $\ell \neq p$. Hence $V_\ell$ splits as a nontrivial direct sum of simple representations of $I_p$. Let $V'$ be a factor of $V_\ell$ corresponding to a simple summand $K$

of $\mathbf{T} \otimes \mathbf{Q}_\ell$, where $\mathbf{T}$ is the Hecke algebra. Since the Artin conductor of the 2-dimensional $K$-representation $V'_\ell$ is $p$, the $\overline{\mathbf{Q}}_\ell[I_p]$-module $\overline{\mathbf{Q}}_\ell \otimes_{\mathbf{Q}_\ell} V'$ is the direct sum of the trivial representation and the character $\varepsilon(f) : (\mathbf{Z}/p\mathbf{Z})^\times \to \overline{\mathbf{Q}}_\ell^\times$ viewed as a character of $G_p$ via the identification $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p) = (\mathbf{Z}/p\mathbf{Z})^\times$. This implies that the abelian rank as well as the additive rank are both equal to half of the dimension of $A$.

### 6.4.1 The Simplest example not covered by general theory

The prime $p = 61$ is the only prime $p \leq 71$ such that the maximal quotient of $J_1(p)$ with positive analytic rank is not a quotient of $J_0(p)$. Let $\varepsilon$ be a Dirichlet character of conductor 61 and order 6. Consider the abelian variety $A_f$ attached to the newform

$$f = q + (e^{2\pi i/3} - 1)q^2 - 2q^3 + \cdots$$

that lies in the 6-dimensional $\mathbf{C}$-vector space $S_2(\Gamma_1(61), \varepsilon)$. Using Proposition 6.1.10, we see that $L(f, 1) = 0$.

It would be interesting to show that $A_f$ has positive algebraic rank, since $A_f$ is not covered by the general theorems of Kolyvagin, Logachev, and Kato concerning Conjecture 6.1.2. This example is the simplest example in the following sense: every elliptic curve over $\mathbf{Q}$ is a quotient of some $J_0(N)$, and an inspection of Tables 4–5 for any integer $N < 61$ shows that the maximal quotient of $J_1(N)$ with positive analytic rank is also a quotient of $J_0(N)$.

The following observation puts this question in the context of $\mathbf{Q}$-curves, and may be of some use in a direct computation to show that $A_f$ has positive algebraic rank. Since $\overline{f} = f \otimes \varepsilon^{-1}$, Shimura's theory (see [62, Prop. 8]) supplies an isogeny $\varphi : A_f \to A_f$ defined over the degree-6 abelian extension of $\mathbf{Q}$ cut out by $\ker(\varepsilon)$. Using $\varphi$, one sees that $A_f$ is isogenous to a product of two elliptic curves. According to Enrique Gonzalez-Jimenez (personal communication) and Jordi Quer, if $t^6 + t^5 - 25t^4 + 8t^3 + 123t^2 - 126t + 27 = 0$, so $t$ generates the degree 6 subfield of $\mathbf{Q}(\zeta_{61})$ corresponding to $\varepsilon$, then one of the elliptic-curve factors of $A_f$ has equation $y^2 = x^3 + c_4x + c_6$, where

$$\begin{aligned} c_4 &= \frac{1}{3}(-321 + 738t - 305t^2 - 196t^3 + 47t^4 + 13t^5), \\ c_6 &= \frac{1}{3}(-4647 + 6300t + 996t^2 - 1783t^3 - 432t^4 - 14t^5). \end{aligned}$$

### 6.4.2 Can Optimal Quotients Have Nontrivial Component Group?

Let $p$ be a prime. Component groups of optimal quotients of $J_0(p)$ are well-understood in the sense of the following theorem of Emerton [23]:

Theorem 6.4.3 (Emerton). *If $A_1, \ldots, A_n$ are the distinct optimal quotients of $J_0(p)$ attached the Galois-orbits of newforms, then the product of the orders of the component groups of the $A_i$'s equals the order of the component* *group of* $J_0(p)$, i.e., *the numerator of* $(p-1)/12$. *Moreover, the natural maps* $\Phi(J_0(p)) \to \Phi(A_i)$ *are surjective.*

Shuzo Takehashi asked a related question about $J_1(p)$:

QUESTION 6.4.4 (TAKEHASHI). Suppose $A = A_f$ is an optimal quotient of $J_1(p)$ attached to a newform. What can be said about the component group of $A$? In particular, is the component group of $A$ necessarily trivial?

Since $J_1(p)$ has trivial component group (see Theorem 1.1.1), the triviality of the component group of $A$ is equivalent to the surjectivity of the natural map from $\Phi(J_1(p))$ to $\Phi(A_f)$.

The data in Tables 4–5 sheds little light on Question 6.4.4. The following are the $A_f$'s that have nonzero $L = c \cdot L(A_f, 1)/\Omega$ with numerator divisible by an odd prime: **37D**, **37F**, **43C**, **43F**, **53D**, **61E**, **61F**, **61G**, **61J**, **67D**, **67E**, and **67G**. For each of these, Conjecture 6.1.2 implies that $c \cdot Ш(A_f) \cdot c_p$ is divisible by an odd prime. However, it seems difficult to deduce which factors in the product are not equal to 1. We remark that for each $A_f$ listed above such that the numerator of $L$ is exactly divisible by $p$, there is a rank-1 elliptic curve $E$ over $\mathbf{Q}$ such that $E[p] \subset A$, so methods as in [2] may shed light on this problem.

### 6.5 USING MAGMA TO COMPUTE THE TABLES

In this section, we describe how to use MAGMA V2.10-6 (or later) to compute the entries in Tables 1–5 at the end of this paper.

#### 6.5.1 COMPUTING TABLE 1: ARITHMETIC OF $J_1(p)$

Let $p$ be a prime. The following MAGMA code illustrates how to compute the two rows in Table 1 corresponding to $p$ $(= 19)$. Note that the space of cuspidal modular symbols has dimension $2 \dim J_1(p)$.

```
> p := 19;
> M := ModularSymbols(Gamma1(p));
> S := CuspidalSubspace(M);
> S;
Modular symbols space of level 19, weight 2, and dimension
14 over Rational Field (multi-character)
> LRatio(S,1);
1/19210689
> Factorization(19210689);
[ <3, 4>, <487, 2> ]
> TorsionBound(S,60);
4383
```

*Remark* 6.5.1. It takes less time and memory to compute $c \cdot L(J_1(p), 1)/\Omega$ in $\mathbf{Q}^\times/2^{\mathbf{Z}}$, and this is done by replacing `M:=ModularSymbols(Gamma1(p))` with

`M:=ModularSymbols(Gamma1(p),2,+1)`. A similar remark applies to all computations of $L$-ratios in the sections below.

### 6.5.2 COMPUTING TABLES 2–3: ARITHMETIC OF $J_H(p)$

Let $p$ be a prime, $d$ a divisor of $p-1$ such that $(p-1)/d$ is even, and $H$ the subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ of order $(p-1)/d$. We use Theorem 1.1.3 and commands similar to the ones in Section 6.5.1 to fill in the entries in Tables 2–3. The following code illustrates computation of the second row of Table 2 for $p = 19$.

```
> p := 19;
> [d : d in Divisors(p-1) | IsEven((p-1) div d)];
[ 1, 3, 9 ]
> d := 3;
> M := ModularSymbolsH(p,(p-1) div d, 2, 0);
> S := CuspidalSubspace(M);
> S;
Modular symbols space of level 19, weight 2, and dimension 2
over Rational Field (multi-character)
> L := LRatio(S,1); L;
1/9
> T := TorsionBound(S,60); T;
3
> T^2*L;
1
> Phi := d / GCD(d,6);  Phi;
1
```

It takes about ten minutes to compute all entries in Table 2–3 using an Athlon 2000MP-based computer.

### 6.5.3 COMPUTING TABLES 4–5

Let $p$ be a prime number. To compute the modular symbols factors corresponding to the newform optimal quotients $A_f$ of $J_1(p)$, we use the `NewformDecomposition` command. To compute the modular kernel, we use the command `ModularKernel`. The following code illustrates computation of the second row of Table 4 corresponding to $p = 19$.

```
> p := 19;
> M := ModularSymbols(Gamma1(19));
> S := CuspidalSubspace(M);
> D := NewformDecomposition(S);
> D;
[
    Modular symbols space for Gamma_0(19) of weight 2 and
    dimension 2 over Rational Field,
```

```
    Modular symbols space of level 19, weight 2, and
    dimension 12 over Rational Field (multi-character)
]
> A := D[2];
> Dimension(A) div 2;
6
> Order(DirichletCharacter(A));
9
> L := LRatio(A,1); L;
1/2134521
> T := TorsionBound(A,60);
> T^2*L;
1
> Invariants(ModularKernel(A));
[ 3, 3 ]
```

It takes about 2.5 hours to compute all entries in Tables 4–5, except that the entries corresponding to $p = 71$, using an Athlon 2000MP-based computer. The $p = 71$ entry takes about 3 hours.

### 6.6 Arithmetic tables

The notation in Tables 1–5 below is explained in Section 6.

Table 1: Arithmetic of $J_1(p)$

| $J_1(p)$ | dim | $c \cdot L(J_1(p), 1)/\Omega$ |
|---|---|---|
| 11 | 1 | $1/5^2$ |
| 13 | 2 | $1/19^2$ |
| 17 | 5 | $1/2^6 \cdot 73^2$ |
| 19 | 7 | $1/3^4 \cdot 487^2$ |
| 23 | 12 | $1/11^2 \cdot 37181^2$ |
| 29 | 22 | $1/2^{12} \cdot 3^2 \cdot 7^2 \cdot 43^2 \cdot 17837^2$ |
| 31 | 26 | $1/2^4 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 2302381^2$ |
| 37 | 40 | 0 |
| 41 | 51 | $1/2^8 \cdot 5^2 \cdot 13^2 \cdot 31^4 \cdot 431^2 \cdot 250183721^2$ |
| 43 | 57 | 0 |
| 47 | 70 | $1/23^2 \cdot 139^2 \cdot 82397087^2 \cdot 12451196833^2$ |
| 53 | 92 | 0 |
| 59 | 117 | $1/29^2 \cdot 59^2 \cdot 9988553613691393812358794271^2$ |
| 61 | 126 | 0 |
| 67 | 155 | 0 |
| 71 | 176 | $1/5^2 \cdot 7^2 \cdot 31^2 \cdot 113^2 \cdot 211^2 \cdot 281^2 \cdot 701^4 \cdot 12713^2 \cdot$ $1307084991922565572906 1^2$ |

| $J_1(p)$ | Torsion Bound |
|---|---|
| 11 | 5 |
| 13 | 19 |
| 17 | $2^3 \cdot 73$ |
| 19 | $3^2 \cdot 487$ |
| 23 | $11 \cdot 37181$ |
| 29 | $2^{12} \cdot 3 \cdot 7 \cdot 43 \cdot 17837$ |
| 31 | $2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 2302381$ |
| 37 | $3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73 \cdot 577 \cdot 17209$ |
| 41 | $2^4 \cdot 5 \cdot 13 \cdot 31^2 \cdot 431 \cdot 250183721$ |
| 43 | $2^2 \cdot 7 \cdot 19 \cdot 29 \cdot 463 \cdot 1051 \cdot 416532733$ |
| 47 | $23 \cdot 139 \cdot 82397087 \cdot 12451196833$ |
| 53 | $7 \cdot 13 \cdot 85411 \cdot 96331 \cdot 379549 \cdot 641949283$ |
| 59 | $29 \cdot 59 \cdot 9988553613691393812358794271$ |
| 61 | $5 \cdot 7^2 \cdot 11^2 \cdot 19 \cdot 31 \cdot 2081 \cdot 2801 \cdot 40231 \cdot 411241 \cdot 514216621$ |
| 67 | $11 \cdot 67 \cdot 193 \cdot 661^2 \cdot 2861 \cdot 8009 \cdot 11287 \cdot 9383200455691459$ |
| 71 | $5 \cdot 7 \cdot 31 \cdot 113 \cdot 211 \cdot 281 \cdot 701^2 \cdot 12713 \cdot 13070849919225655729061$ |

Table 2: Arithmetic of $J_H(p)$

| $p$ | $d$ | dim | $L = c \cdot L(J_H, 1)/\Omega$ | $T$ = Torsion Bound | $T^2L$ | $\lvert\Phi(J_H)\rvert$ |
|---|---|---|---|---|---|---|
| 11 | 1 | 1 | $1/5$ | 5 | 5 | 5 |
| 13 | 1 | 0 | 1 | 1 | 1 | 1 |
| | 2 | 0 | 1 | 1 | 1 | 1 |
| | 3 | 0 | 1 | 1 | 1 | 1 |
| 17 | 1 | 1 | $1/2^2$ | $2^2$ | $2^2$ | $2^2$ |
| | 2 | 1 | $1/2^3$ | $2^2$ | 2 | 2 |
| | 4 | 1 | $1/2^4$ | $2^2$ | 1 | 1 |
| 19 | 1 | 1 | $1/3$ | 3 | 3 | 3 |
| | 3 | 1 | $1/3^2$ | 3 | 1 | 1 |
| 23 | 1 | 2 | $1/11$ | 11 | 11 | 11 |
| 29 | 1 | 2 | $1/7$ | 7 | 7 | 7 |
| | 2 | 4 | $1/3^2 \cdot 7$ | $3 \cdot 7$ | 7 | 7 |
| | 7 | 8 | $1/2^6 \cdot 7^2 \cdot 43^2$ | $2^6 \cdot 7 \cdot 43$ | $2^6$ | 1 |
| 31 | 1 | 2 | $1/5$ | 5 | 5 | 5 |
| | 3 | 6 | $1/2^4 \cdot 5 \cdot 7^2$ | $2^2 \cdot 5 \cdot 7$ | 5 | 5 |
| | 5 | 6 | $1/5^4 \cdot 11^2$ | $5^2 \cdot 11$ | 1 | 1 |
| 37 | 1 | 2 | 0 | 3 | 0 | 3 |
| | 2 | 4 | 0 | $3 \cdot 5$ | 0 | 3 |
| | 3 | 4 | 0 | $3 \cdot 7$ | 0 | 1 |
| | 6 | 10 | 0 | $3 \cdot 5 \cdot 7 \cdot 37$ | 0 | 1 |
| | 9 | 16 | 0 | $3^2 \cdot 7 \cdot 19 \cdot 577$ | 0 | 1 |
| 41 | 1 | 3 | $1/2 \cdot 5$ | $2 \cdot 5$ | $2 \cdot 5$ | $2 \cdot 5$ |
| | 2 | 5 | $1/2^6 \cdot 5$ | $2^3 \cdot 5$ | 5 | 5 |
| | 4 | 11 | $1/2^8 \cdot 5 \cdot 13^2$ | $2^4 \cdot 5 \cdot 13$ | 5 | 5 |
| | 5 | 11 | $1/2 \cdot 5^2 \cdot 431^2$ | $2 \cdot 5 \cdot 431$ | 2 | 2 |
| | 10 | 21 | $1/2^6 \cdot 5^2 \cdot 31^4 \cdot 431^2$ | $2^3 \cdot 5 \cdot 31^2 \cdot 431$ | 1 | 1 |

Table 3: Arithmetic of $J_H(p)$ (continued)

| $p$ | $d$ | dim | $L = c \cdot L(J_H, 1)/\Omega$ | $T$ = Torsion Bound | $T^2L$ | $\|\Phi(J_H)\|$ |
|---|---|---|---|---|---|---|
| 43 | 1 | 3 | 0 | 7 | 0 | 7 |
| | 3 | 9 | 0 | $2^2 \cdot 7 \cdot 19$ | 0 | 7 |
| | 7 | 15 | 0 | $7 \cdot 29 \cdot 463$ | 0 | 1 |
| 47 | 1 | 4 | $1/23$ | 23 | 23 | 23 |
| 53 | 1 | 4 | 0 | 13 | 0 | 13 |
| | 2 | 8 | 0 | $7 \cdot 13$ | 0 | 13 |
| | 13 | 40 | 0 | $13 \cdot 96331 \cdot 379549$ | 0 | 1 |
| 59 | 1 | 5 | $1/29$ | 29 | 29 | 29 |
| 61 | 1 | 4 | 0 | 5 | 0 | 5 |
| | 2 | 8 | 0 | $5 \cdot 11$ | 0 | 5 |
| | 3 | 12 | 0 | $5 \cdot 7 \cdot 19$ | 0 | 5 |
| | 5 | 16 | 0 | $5 \cdot 2801$ | 0 | 1 |
| | 6 | 26 | 0 | $5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$ | 0 | 5 |
| | 10 | 36 | 0 | $5 \cdot 11^2 \cdot 2081 \cdot 2801$ | 0 | 1 |
| | 15 | 56 | 0 | $5 \cdot 7 \cdot 19 \cdot 2801 \cdot$ 514216621 | 0 | 1 |
| 67 | 1 | 5 | 0 | 11 | 0 | 11 |
| | 3 | 15 | 0 | $11 \cdot 193$ | 0 | 11 |
| | 11 | 45 | 0 | $11 \cdot 661 \cdot 2861 \cdot 8009$ | 0 | 1 |
| 71 | 1 | 6 | $1/5 \cdot 7$ | $5 \cdot 7$ | $5 \cdot 7$ | $5 \cdot 7$ |
| | 5 | 26 | $1/5^2 \cdot 7 \cdot 31^2 \cdot 211^2$ | $5 \cdot 7 \cdot 31 \cdot 211$ | 7 | 7 |
| | 7 | 36 | $1/5 \cdot 7^2 \cdot 113^2 \cdot 12713^2$ | $5 \cdot 7 \cdot 113 \cdot 12713$ | 5 | 5 |

Table 4: Arithmetic of Optimal Quotients $A_f$ of $J_1(p)$

| $A_f$ | dim | ord($\varepsilon$) | $L = c \cdot L(A_f, 1)/\Omega$ | $T^2L$ | modular kernel |
|---|---|---|---|---|---|
| **11A** | 1 | 1 | $1/5^2$ | 1 | [] |
| **13A** | 2 | 6 | $1/19^2$ | 1 | [] |
| **17A** | 1 | 1 | $1/2^4$ | 1 | $[2^2]$ |
| **17B** | 4 | 8 | $1/2^2 \cdot 73^2$ | 1 | $[2^2]$ |
| **19A** | 1 | 1 | $1/3^2$ | 1 | $[3^2]$ |
| **19B** | 6 | 9 | $1/3^2 \cdot 487^2$ | 1 | $[3^2]$ |
| **23A** | 2 | 1 | $1/11^2$ | 1 | $[11^2]$ |
| **23B** | 10 | 11 | $1/37181^2$ | 1 | $[11^2]$ |
| **29A** | 2 | 2 | $1/3^2$ | 1 | $[14^4]$ |
| **29B** | 2 | 1 | $1/7^2$ | 1 | $[2^2 14^2]$ |
| **29C** | 6 | 7 | $1/2^6 \cdot 43^2$ | $2^6$ | $[2^{10} 14^2]$ |
| **29D** | 12 | 14 | $1/2^6 \cdot 17837^2$ | $2^6$ | $[2^8 14^4]$ |
| **31A** | 2 | 1 | $1/5^2$ | 1 | $[3^2 15^2]$ |
| **31B** | 4 | 5 | $1/5^2 \cdot 11^2$ | 1 | $[3^6 15^2]$ |
| **31C** | 4 | 3 | $1/2^4 \cdot 7^2$ | 1 | $[5^4 15^4]$ |
| **31D** | 16 | 15 | $1/2302381^2$ | 1 | $[15^8]$ |
| **37A** | 1 | 1 | $1/3^2$ | 1 | $[12^2]$ |
| **37B** | 1 | 1 | 0 | 0 | $[36^2]$ |
| **37C** | 2 | 2 | $2/5^2$ | 2 | $[18^4]$ |
| **37D** | 2 | 3 | $3/7^2$ | 3 | $[6^2 18^2]$ |
| **37E** | 4 | 6 | $1/37^2$ | 1 | $[3^4 18^4]$ |
| **37F** | 6 | 9 | $3/577^2$ | 3 | $[2^6 6^2 102^4]$ |
| **37G** | 6 | 9 | $1/3^2 \cdot 19^2$ | 1 | $[2^8 34^2 102^2]$ |
| **37H** | 18 | 18 | $1/73^2 \cdot 17209^2$ | 1 | $[2^{12} 6^{12}]$ |
| **41A** | 2 | 2 | $1/2^4$ | 1 | $[20^4]$ |
| **41B** | 3 | 1 | $1/2^2 \cdot 5^2$ | 1 | $[2^2 20^4]$ |
| **41C** | 6 | 4 | $1/2^2 \cdot 13^2$ | 1 | $[5^2 10^{10}]$ |
| **41D** | 8 | 10 | $1/31^4$ | 1 | $[4^{12} 20^4]$ |
| **41E** | 8 | 5 | $1/431^2$ | 1 | $[4^{12} 20^4]$ |
| **41F** | 24 | 20 | $1/250183721^2$ | 1 | $[2^{20} 10^{12}]$ |
| **43A** | 1 | 1 | 0 | 0 | $[42^2]$ |
| **43B** | 2 | 1 | $2/7^2$ | 2 | $[3^2 42^2]$ |
| **43C** | 2 | 3 | $3/2^4$ | 3 | $[35^2 105^2]$ |
| **43D** | 4 | 3 | $1/19^2$ | 1 | $[7^4 105^4]$ |
| **43E** | 6 | 7 | $1/29^2$ | 1 | $[3^8 39^2 273^2]$ |
| **43F** | 6 | 7 | $7/463^2$ | 7 | $[3^8 39^2 273^2]$ |
| **43G** | 36 | 21 | $1/1051^2 \cdot 416532733^2$ | 1 | $[3^{12} 21^{12}]$ |

Table 5: Arithmetic of Optimal Quotients $A_f$ of $J_1(p)$ (continued)

| $A_f$ | dim | ord($\varepsilon$) | $L = c \cdot L(A_f, 1)/\Omega$ | $T^2L$ | modular kernel |
|---|---|---|---|---|---|
| **47A** | 4 | 1 | $1/23^2$ | 1 | $[23^6]$ |
| **47B** | 66 | 23 | $1/139^2 \cdot 82397087^2 \cdot 12451196833^2$ | 1 | $[23^6]$ |
| **53A** | 1 | 1 | 0 | 0 | $[52^2]$ |
| **53B** | 3 | 1 | $2/13^2$ | 2 | $[2^2 26^2 52^2]$ |
| **53C** | 4 | 2 | $2/7^2$ | 2 | $[26^8]$ |
| **53D** | 36 | 13 | $13/96331^2 \cdot 379549^2$ | 13 | $[2^{66} 26^6]$ |
| **53E** | 48 | 26 | $1/85411^2 \cdot 641949283^2$ | 1 | $[2^{64} 26^8]$ |
| **59A** | 5 | 1 | $1/29^2$ | 1 | $[29^8]$ |
| **59B** | 112 | 29 | $1/59^2 \cdot 99885536136913938123587942712^2$ | 1 | $[29^8]$ |
| **61A** | 1 | 1 | 0 | 0 | $[60^2]$ |
| **61B** | 2 | 6 | 0 | 0 | $[55^4]$ |
| **61C** | 3 | 1 | $2/5^2$ | 2 | $[6^2 30^2 60^2]$ |
| **61D** | 4 | 2 | $2/11^2$ | 2 | $[30^8]$ |
| **61E** | 8 | 3 | $3/7^2 \cdot 19^2$ | 3 | $[10^8 30^8]$ |
| **61F** | 8 | 6 | $11^2/7^2 \cdot 31^2$ | $11^2$ | $[10^8 30^4 330^4]$ |
| **61G** | 12 | 5 | $5/2801^2$ | 5 | $[6^{18} 30^6]$ |
| **61H** | 16 | 10 | $1/11^2 \cdot 2081^2$ | 1 | $[3^8 6^{16} 30^8]$ |
| **61I** | 32 | 15 | $1/514216621^2$ | 1 | $[2^{40} 6^8 30^{16}]$ |
| **61J** | 40 | 30 | $5^2/40231^2 \cdot 411241^2$ | $5^2$ | $[2^{32} 6^{12} 30^{20}]$ |
| **67A** | 1 | 1 | 1 | 1 | $[165^2]$ |
| **67B** | 2 | 1 | $2^2/11^2$ | $2^2$ | $[6^2 330^2]$ |
| **67C** | 2 | 1 | 0 | 0 | $[66^4]$ |
| **67D** | 10 | 11 | $11/2861^2$ | 11 | $[3^{16} 7521^2 82731^2]$ |
| **67E** | 10 | 3 | $3^2/193^2$ | $3^2$ | $[11^{10} 33^{10}]$ |
| **67F** | 10 | 11 | $1/661^2$ | 1 | $[3^{16} 4623^2 50853^2]$ |
| **67G** | 20 | 11 | $11/8009^2$ | 11 | $[3^{36} 240999^4]$ |
| **67H** | 100 | 33 | $1/67^2 \cdot 661^2 \cdot 11287^2 \cdot 9383200455691459^2$ | 1 | $[3^{60} 33^{20}]$ |
| **71A** | 3 | 1 | $1/7^2$ | 1 | $[5^2 35^2 315^2]$ |
| **71B** | 3 | 1 | $1/5^2$ | 1 | $[7^2 35^2 315^2]$ |
| **71C** | 20 | 5 | $1/31^2 \cdot 211^2$ | 1 | $[7^{30} 35^{10}]$ |
| **71D** | 30 | 7 | $1/113^2 \cdot 12713^2$ | 1 | $[5^{50} 35^{10}]$ |
| **71E** | 120 | 35 | $1/281^2 \cdot 701^4 \cdot 13070849919225655729061^2$ | 1 | $[5^{20} 35^{40}]$ |

## References


[1] A. Agashé, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. 328 (1999), no. 5, 369–374.

[2] A. Agashe and W. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory 97 (2002), no. 1, 171–185.

[3] ———, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank* 0, to appear in Math. Comp.

[4] ———, *The Manin constant, congruence primes, and the modular degree*, in progress.

[5] M. Artin, *Algebraic approximation of structures over complete local rings*, Publ. Math. IHES, 36 (1969), 23–58.

[6] L. Bégueri, *Dualité sur un corps local à corps résiduel algébriquement clos*, Mém. Soc. Math. France (1980/81), no. 4.

[7] A. Bertapelle, *On perfectness of Grothendieck's pairing for the $\ell$-parts of component groups*, J. Reine Angew. Math., 538 (2001), 223–236.

[8] A. Bertapelle and S. Bosch, *Weil restriction and Grothendieck's duality conjecture*, Journal of algebraic geometry, 9 (2000), 155–164.

[9] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[10] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[11] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, Cambridge University Press, Cambridge, 1996.

[12] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.

[13] T. Chinburg "Minimal models of curves over Dedekind rings" in *Arithmetic Geometry* (Cornell/Silverman ed.), Springer-Verlag, Berlin, 1986.

[14] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[15] P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques" in *Modular Functions of One Variables II*, Lecture Notes in Mathematics 349, Springer-Verlag, Berlin, 1973.

[16] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133.

[17] A. Edelman, *The mathematics of the Pentium division bug*, SIAM Rev. 39 (1997), no. 1, 54–67.

[18] S. J. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque (1991), no. 196–197, 7–8, 159–170 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[19] ———, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

[20] ———, *Néron models and tame ramification*, Compositio Math., 81 (1992), 291–306.

[21] ———, *Modular parameterizations at primes of bad reduction*, in preparation.

[22] ———, *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod* 2 *of weight one*, preprint.

[23] M. Emerton, *Optimal Quotients of Modular Jacobians*, to appear in Math. Ann.

[24] E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjectures*, Springer-Verlag, Berlin, 1988.

[25] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies 131, Princeton University Press, 1993.

[26] J. González and J.-C. Lario, $\mathbf{Q}$*-curves and their Manin ideals*, Amer. J. Math. 123 (2001), no. 3, 475–503.

[27] A. Grothendieck, *Éléments de géométrie algébrique.* $\mathrm{IV}_4$. Étude locale des schémas et des morphismes de schémas, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28.

[28] ———, *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Lecture Notes in Mathematics, Vol. 288.

[29] ———, *Groupes de monodromie en géométrie algébrique. II*, Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), Dirigé par P. Deligne et N. Katz, Lecture Notes in Mathematics, Vol. 340.

[30] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms* (*mod p*), Duke Math. J. 61 (1990), no. 2, 445–517.

[31] A. Joyce, *The Manin Constant of an Optimal Quotient of* $J_0(431)$, preprint, 2003.

[32] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, 244 page preprint.

[33] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), no. 3, 481–502.

[34] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N.J., 1985.

[35] D. R. Kohel and W. A. Stein, *Component Groups of Quotients of* $J_0(N)$, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000.

[36] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz 1 (1989), no. 5, 171–196.

[37] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981.

[38] S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[39] S. Lichtenbaum, *Curves over discrete valuation rings*, American Journal of Mathematics, 90 (1968), 380–405.

[40] J. Lipman, *Desingularization of two-dimensional schemes*, Annals of Mathematics, 107 (1978), 151–207.

[41] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford University Press, Oxford, 2002.

[42] Q. Liu and D. Lorenzini, *Models of curves and finite covers*, Compositio Math., 118 (1999), 61–102.

[43] W. Lütkebohmert, *On compactification of schemes*, Manuscripta Mathematica, 80 (1993), 95–111.

[44] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986, Translated from the Japanese by M. Reid.

[45] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186.

[46] ______, *Rational isogenies of prime degree* (*with an appendix by D. Goldfeld*), Invent. Math. 44 (1978), no. 2, 129–162.

[47] L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$*, J. Reine Angew. Math. 477 (1996), 71–115.

[48] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462.

[49] ———, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 221–231.

[50] A. P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. 12 (1971), 105–111.

[51] B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. (2) 150 (1999), no. 3, 1109–1149.

[52] D. Popescu, *General Néron desingularization and approximation*, Nagoya Math Journal, 104 (1986), pp. 85–115.

[53] Michel Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France 102 (1974), 241–280.

[54] K. Ribet, "On the component groups and the Shimura subgroup of $J_0(N)$", exposé 6, Sém. Th. Nombres, Université Bordeaux, 1987–88.

[55] ———, "Irreducible Galois representations arising from component groups of Jacobians" in *Elliptic curves, modular forms, and Fermat's Last Theorem*, International Press, 1995.

[56] M. Schlessinger, *Infinitesimal deformations of singularities*, 1964 Harvard Ph.D. thesis, unpublished.

[57] J-P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, Colloque d'Algèbre (Paris, 1967), Exp. 8 (1968), 11.

[58] ———, *Cohomologie des groupes discrets*, Prospects in mathematics (Proc. Sympos., Princeton Univ., Princeton, N.J., 1970), Princeton Univ. Press, Princeton, N.J., 1971, pp. 77–169. Ann. of Math. Studies, No. 70.

[59] ———, *Lie algebras and Lie groups*, second ed., Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 1992, 1964 lectures given at Harvard University.

[60] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000, 1985–1998.

[61] I. Shafarevich, *Lectures on minimal models and birational transformations of two-dimensional schemes*, Tata Institute: Bombay, 1966.

[62] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan 25 (1973), no. 3, 523–544.

[63] ______, *An introduction to computing modular forms using modular symbols*, to appear in an MSRI proceedings.

[64] ______, *Shafarevich-Tate groups of nonsquare order*, to appear in proceedings of MCAV 2002, Progress of Mathematics.

[65] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. 98 (1989), no. 1, 75–106.

[66] R. Swan, *Néron-Popescu desingularization*, Lectures in Algebra and Geometry 2, International Press, Cambridge (1998), pp. 135–192.

[67] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[68] J. Watanabe, *Some remarks on Cohen-Macaulay rings with many zero divisors and an application*, J. Algebra 39 (1976), no. 1, 1–14.

Brian Conrad
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1109
USA
bdconrad@umich.edu

Bas Edixhoven
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands
edix@math.leidenuniv.nl

William A. Stein
Department of Mathematics
Harvard University
Cambridge, MA 02138
USA
was@math.harvard.edu