M.P. Noordman

Gonality and Bad Reduction of Modular Curves

Master Thesis

Thesis Advisors: Prof. S.J. Edixhoven and Dr. M. Derickx

Date Master Examination: June 26, 2017

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

The gonality of a smooth projective curve C over a field is the lowest degree of a finite morphism from C to the projective line $\mathbb{P}^1$. This quantity carries information about the curve, and is of general interest, but is often hard to compute explicitly. In specific cases one can find upper bounds for the gonality by finding functions $C \to \mathbb{P}^1$ of low degree, but proving that a given upper bound is sharp is not so easy.

In [DS17], the authors classify all torsion groups occurring infinitely often as the torsion group of an elliptic curve over a number field of degree d, for $d = 5$ and $d = 6$. This proceeded in several steps, in one of which the authors had to obtain lower bounds for the gonality of some finite set of modular curves over $\mathbb{Q}$. In order to do so, they reduced the curve modulo a prime p chosen such that the reduction was smooth, and then searching the Riemann-Roch spaces of all effective divisors of degree up to d. There are only finitely many of those, so in theory the search terminates, but the running time can become unfeasibly large as d increases. Indeed, the authors state that the the only obstruction to extending their result to $d = 7$ is the running time of the computational verification of the conjectured lower bounds for the gonality of certain curves.

In this thesis, we investigate the possibility of obtaining lower bounds for the gonality of a curve over $\mathbb{Q}$ by looking at reductions that are not smooth. The rationale for doing this is that the primes of bad reduction of a modular curve are usually the characteristics in which the modular interpretation is easiest to translate into geometric properties. We will see examples of this phenomenon in chapter 4.

The structure of the thesis is as follows. In the first chapter, we revise the theory of invertible sheaves and Cartier divisors that we will need in the rest of the thesis. The second chapter contains definitions and theorems on the degrees of such objects. In the third chapter, we give a definition of gonality that is more general than the one stated above, and also a variant of the gonality which we will call the 'divisor gonality' of the curve. We study the relation between these quantities and their behaviour with respect to reduction. More specifically, we will show the following (Theorem 3.16)

Theorem 0.1. *Let $S = \operatorname{Spec} R$ be the spectrum of a discrete valuation ring R, and let $X \to S$ be of relative dimension 1, regular, projective, flat and cohomologically flat. Then the divisor gonality of the generic fiber is at least the divisor gonality of the special fiber.*

In the last section of chapter 3 we will show that the divisor gonality of a geometrically reduced curve over a field is closely related to the gonalities of the partial normalizations of that curve, and how we can use this to bound the divisor gonality in terms of the partial normalizations of the curve (Theorem 3.27).

In the last chapter, we consider two examples that illustrate how these results can be applied to obtain lower bounds on the gonality of modular curves over $\mathbb{Q}$ without using explicit equations for the curves. In the first section we obtain lower bounds for the gonality of $X(2, 2n)$ over $\mathbb{Q}$ for odd $n \geq 5$ in terms of the gonality of $X_1(n)$ over $\mathbb{F}_2$. These gonalities are known for all odd $n \leq 39$. The results of this section imply the following bounds on the occurrence of groups as the torsion group of an elliptic curve over number fields of small degree (Corollary 4.21).

Theorem 0.2. *Let $\Phi^\infty(d)$ denote the set of all pairs (m, mn) such that $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/mn\mathbb{Z})$ occurs infinitely often (up to $\overline{\mathbb{Q}}$-isomorphism) as the torsion subgroup of an elliptic curve over a number field of degree d. Then*

1. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 11, 13, 15$ *and* $d < 8$.
2. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 25$ *and* $d < 10$.
3. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 27$ *and* $d < 12$.
4. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 23$ *and* $d < 13$.
5. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 17, 21$ *and* $d < 16$.
6. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 29$ *and* $d < 18$.
7. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 19$ *and* $d < 19$.
8. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 31, 33$ *and* $d < 20$.
9. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 35$ *and* $d < 24$.
10. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 39$ *and* $d < 26$.
11. $(2, 2n) \notin \Phi^\infty(d)$ *for* $n = 37$ *and* $d < 27$.

In the second section of chapter four, we study the gonality of $X_0(p)/W_p$. We obtain an algorithm that uses Gröbner bases to compute a lower bound for the gonality of these curves over $\mathbb{Q}$, using a simple description of the reduction of $X_0(p)/W_p$ at p. We use this algorithm to compute a lower bound for the gonality of $X_0(p)/W_p$ for all primes between 5 and 500.

Acknowledgements

I would like to thank my two advisors, Bas Edixhoven and Maarten Derickx, for their crucial role in writing this thesis. Maarten introduced me to the topic of the gonality of modular curves, and has since provided many useful insights, both in terms of the mathematics involved and in terms of the exposition of the results. Bas was the one suggesting to study 'bad' reduction of modular curves in order to obtain lower bounds for the gonality. During our weekly meetings he effortlessly managed to clear up any confusion and solve problems that had me stuck for days, while always finding the details in my thesis that needed additional attention. This thesis would not have been written without them.

Chapter 1

Invertible sheaves of modules

In this chapter, we give an overview of the background that we need in the following chapters. We define and give the basic properties of invertible sheaves and of Cartier divisors, and we consider the relation between invertible sheaves and morphisms to projective space. Everything related to degrees of these objects is left for the next chapter. The basic references for this chapter are [Sta17], [Liu02] and [Har77].

In this chapter, we let X be a locally Noetherian scheme.

1.1 Invertible sheaves

Definition 1.1. An *invertible sheaf* or *line bundle* on X is an $\mathcal{O}_X$-module $\mathcal{L}$ such that for every $x \in X$ there is an open neighbourhood U of x such that $\mathcal{L}|_U \cong \mathcal{O}_U$ as $\mathcal{O}_U$-modules.

In other words, an invertible sheaf is a sheaf of modules that is locally free of rank 1. Clearly being invertible is a local property, so to check it we only need to look at open neighbourhoods around each point. The following implies that for a coherent sheaf of modules on X, it is already enough to look at the stalks.

Lemma 1.2. *Let $\mathcal{L}$ be a coherent $\mathcal{O}_X$-module, and $x \in X$ a point. Suppose that $\mathcal{L}_x$ is free of rank $r \in \mathbb{N}$ as an $\mathcal{O}_{X,x}$-module. Then there is some open neighbourhood U of x such that $\mathcal{L}|_U$ is isomorphic to $\mathcal{O}_U^r$ as sheaves over $\mathcal{O}_U$.*

Proof. Let $s_1, \ldots, s_r \in \mathcal{O}_{X,x}$ be a free basis of $\mathcal{O}_{X,x}$. The s_i are locally defined around x, but since the claim is local, we may after shrinking X assume that the s_i are defined on all of X. Then they define a morphism $\varphi\colon \mathcal{O}_X^r \to \mathcal{L}$. Let $\mathcal{K}$ and $\mathcal{C}$ be the kernel and cokernel of this morphism. Then by construction $\mathcal{K}_x = \mathcal{C}_x = 0$. But $\mathcal{K}$ and $\mathcal{C}$ are coherent since X is locally Noetherian, and the support of a coherent sheaf on a locally Noetherian scheme is closed. Hence, there is an open neighbourhood U of x on which $\mathcal{K}$ and $\mathcal{C}$ are zero, and on this neighbourhood, φ is an isomorphism. □

Corollary 1.3. *An $\mathcal{O}_X$-module $\mathcal{L}$ on a locally Noetherian scheme X is invertible if and only if it is coherent and every stalk of $\mathcal{L}$ is free of rank 1.* □

Here are some basic properties of invertible sheaves. The second property justifies the term 'invertible'.

Lemma 1.4.

1. *The tensor product $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{M}$ of two invertible sheaves $\mathcal{L}$, $\mathcal{M}$ on X is an invertible sheaf on X.*
2. *Let $\mathcal{L}$ be a coherent $\mathcal{O}_X$-module. Then $\mathcal{L}$ is invertible if and only if there is a coherent $\mathcal{O}_X$-module $\mathcal{M}$ such that $\mathcal{L} \otimes \mathcal{M} \cong \mathcal{O}_X$ as $\mathcal{O}_X$-modules.*

Proof.

1. Since the tensor product commutes with taking stalks, and the tensor product of free modules of rank 1 is again a free module of rank 1, this follows from Corollary 1.3.

2. Let us first assume that $\mathcal{L}$ is invertible. Set $\mathcal{M} = \mathcal{H}om(\mathcal{L}, \mathcal{O}_X)$. Define a morphism $\mathcal{L} \otimes \mathcal{M} \to \mathcal{O}_X$ on affine open $U \subseteq X$ by $(\mathcal{L} \otimes \mathcal{M})(U) \mapsto \mathcal{O}_X(U)$, $s \otimes f \mapsto f(s)$. By looking at the stalks, one easily verifies that this is an isomorphism.

   The other direction translates after taking stalks into the following claim about commutative algebra: given a local ring A and finitely generated A-modules M and N, if $M \otimes N$ is isomorphic to A (as an A-module) then M is already isomorphic to A. To prove this, let $\mathfrak{m}$ be the maximal ideal of A and $k = A/\mathfrak{m}$ the residue field. From $M \otimes N \cong A$ we get that

   $$(M \otimes_A k) \otimes_k (N \otimes_A k) = (M \otimes_A N) \otimes_A k = A \otimes_A k = k,$$

   so $\dim_k(M \otimes_A k) \leq 1$. By Nakayama's lemma this implies that M is generated over A by a single element $m \in M$. Thus we have a surjection $A \twoheadrightarrow M$. Tensoring with N gives a surjection $N \twoheadrightarrow A$. Switching the roles of M and N, we similarly get a surjective map $M \twoheadrightarrow A$. The composition of the surjective A-module morphisms $A \twoheadrightarrow M$ and $M \twoheadrightarrow A$ gives a surjective A-module morphism $A \twoheadrightarrow A$, which must be an isomorphism. Therefore $M \twoheadrightarrow A$ was already an isomorphism. □

Notice that the above lemma implies that the isomorphism classes of invertible sheaves on X indeed form an abelian group under the tensor product. The inverse $\mathcal{H}om(\mathcal{L}, \mathcal{O}_X)$ of an invertible sheaf $\mathcal{L}$ on X will be denoted $\mathcal{L}^{\otimes -1}$, and in general we denote the k-th power of $\mathcal{L}$ by $\mathcal{L}^{\otimes k}$ for $k \in \mathbb{Z}$.

Definition 1.5. The group of isomorphism classes of invertible sheaves on X under tensor product is called the *Picard group*, denoted $\operatorname{Pic}(X)$.

1.2 Cartier divisors

This section gives the definition and basic properties of Cartier divisors. We follow [Sta17, Section 30.13] and further.

Definition 1.6. An *effective Cartier divisor* on X is a closed subscheme $D \subseteq X$ such that the corresponding ideal sheaf $\mathcal{I}(D)$ is invertible.

It will be useful to make this definition more explicit. Recall that a *regular element* of a ring A is a non-zero element of A that is not a zero-divisor.

Lemma 1.7. *Let $D \subseteq X$ be a closed subscheme. The following are equivalent:*

1. *D is an effective Cartier divisor.*
2. *Every point $x \in X$ has a neighbourhood of the form $U = \operatorname{Spec} A$ such that $D \cap U = \operatorname{Spec} A/fA$ for a regular element $f \in A$.*

Proof. This follows from the observation that an ideal of a ring A is free of rank 1 if and only if it is generated by a single regular element $f \in A$. □

So we should think of effective Cartier divisors as a closed subscheme that is locally the zero set of a single function that is not a zero-divisor.

Definition 1.8. Let D_1 and D_2 be two effective Cartier divisors on X. Then the *sum* of D_1 and D_2, denoted $D_1 + D_2$, is the closed subscheme of X corresponding to the product $\mathcal{I}(D_1)\mathcal{I}(D_2)$ of the sheaves of ideals.

Notice that $D_1 + D_2$ is again an effective Cartier divisor, because the product of two invertible sheaves of ideals is again an invertible sheaf of ideals. In terms of local equations, if D_1 can be locally written as $\operatorname{Spec} A/fA$ and D_2 as $\operatorname{Spec} A/gA$, then $D_1 + D_2$ can be written as $\operatorname{Spec} A/fgA$.

Note that the sum of effective Cartier divisors is associative and commutative, and the empty subscheme of X behaves as an identity. Moreover, we have the following cancellation law.

Lemma 1.9. *Let D_1, D_2 and D_3 be Cartier divisors of X such that $D_1 + D_3 = D_2 + D_3$. Then $D_1 = D_2$.*

Proof. Since the question is local, we can reduce to local equations. Let $x \in X$ arbitrary, and choose an affine neighbourhood $\operatorname{Spec} A$ of x such that there are $f_1, f_2, f_3 \in A$ regular such that $D_i \cap \operatorname{Spec} A = \operatorname{Spec} A/f_iA$ for $i = 1, 2, 3$. Then $D_1 + D_3 = D_2 + D_3$ tells us that $f_1f_3A = f_2f_3A$ as ideals of A. Since the f_i are regular, this means that there is a unit $u \in A$ such that $f_1f_3 = uf_2f_3$, and since f_3 is regular, this implies that $f_1 = uf_2$, hence $f_1A = f_2A$. □

So the collection of effective Cartier divisors is almost a group: we only lack the inverses. Just as one can construct a field from an integral domain by considering formal quotients, we can get a group from a cancellative monoid by considering formal differences.

Definition 1.10. The group of *Cartier divisors* on X, denoted $\operatorname{CaDiv}(X)$ is the collection of differences $D_1 - D_2$, with D_1 and D_2 effective Cartier divisors, modulo the relation

$$D_1 - D_2 \sim E_1 - E_2 \text{ if and only if } D_1 + E_2 = E_1 + D_2.$$

We will identify effective Cartier divisors D with the Cartier divisor $D - \emptyset$. By slight abuse of terminology, we will say that an Cartier divisor $D - E$ is effective if there is an effective Cartier divisor $F \subseteq X$ such that $D - E = F$.

Lemma 1.11. *Let $D, E \subseteq X$ be effective Cartier divisors. Then $D - E$ is effective if and only if $E \subseteq D$ as closed subschemes of X (i.e. the closed immersion $E \to X$ factors via the closed immersion $D \to X$).*

Proof. The statements are local, so we reduce to local equations. Thus we assume that $X = \operatorname{Spec} A$, and that $D = \operatorname{Spec} A/fA$ and $E = \operatorname{Spec} A/gA$ for regular elements $f, g \in A$. If $D - E$ is effective, then there is an effective Cartier divisor F on X such that $D = E + F$. Possibly after shrinking A we may write $F = \operatorname{Spec} A/hA$ for $h \in A$ regular. Since $D = E + F$ we have $fA = ghA \subseteq gA$, so $E \subseteq D$. On the other hand, if $E \subseteq D$, then $fA \subseteq gA$, so there is some $h \in A$ with $f = gh$. If $ah = 0$ for some $a \in A$, then also $af = agh = 0$, and since f is regular, this implies that $a = 0$. Hence, h is regular. Thus letting F be the effective Cartier divisor associated to the ideal hA, we have $D - E = F$. □

Definition 1.12. Let $D = D_1 - D_2$ be a Cartier divisor on X. Then the *invertible sheaf associated to D* is the $\mathcal{O}_X$-module $\mathcal{O}_X(D) = \mathcal{I}(D_1)^{\otimes -1} \otimes \mathcal{I}(D_2)$ (notice the choice of signs).

If D is effective, then $\mathcal{O}_X(D) = \mathcal{H}om(\mathcal{I}(D), \mathcal{O}_X)$ contains a distinguished element, which we call the *canonical section* 1_D, which is given by the inclusion of $\mathcal{I}(D)$ in $\mathcal{O}_X$.

Clearly the association $D \mapsto \mathcal{O}_X(D)$ defines a group homomorphism $\operatorname{CaDiv}(X) \to \operatorname{Pic}(X)$. Note that it is usually not injective, since there are often many different sheaves of ideals that are free of rank 1 (for instance, if $X = \operatorname{Spec} A$, then any regular element that is not a unit gives a non-trivial ideal of that form). It should be noted that the kernel of this association map can be described explicitly in terms of nonzero sections of the sheaf of meromorphic functions on X, but we will not pursue this direction here.

1.3 Regular sections of invertible sheaves

Definition 1.13. Let $\mathcal{L}$ be an invertible sheaf on X. We call a global section $s \in \mathcal{L}(X)$ *regular at a point* $x \in X$ if s_x is a regular element of $\mathcal{L}_x$ (meaning that the map $\mathcal{O}_{X,x} \to \mathcal{L}_x$, $f \mapsto f \cdot s_x$ is injective). We say that s is *regular* if it is regular at every $x \in X$. We call $\mathcal{L}$ *effective* if it has a regular section.

Lemma 1.14. *Let $\mathcal{L}$ be invertible on X and s a global section. Let $\varphi \colon \mathcal{O}_X \to \mathcal{L}$ be the map defined by $f \mapsto f \cdot s$. Then s is a regular section of $\mathcal{L}$ if and only if φ is injective.*

Proof. This follows because a morphism of sheaves is injective if and only if all stalk maps are injective. □

Definition 1.15. Let $\mathcal{L}$ be an invertible sheaf on X and $s \in \mathcal{L}(X)$ a global section. Then we define the *zero scheme* of s (notation $\mathcal{Z}(s)$) to be the closed subscheme of X given by the sheaf of ideals that is the image of the morphism

$$\mathcal{L}^{\otimes -1} \to \mathcal{O}_X, \qquad f \mapsto f(s).$$

We also define the open subset

$$D(s) = \{x \in X : s_x \notin \mathfrak{m}_x \mathcal{L}_x\}.$$

Locally on affine spectra, the zero scheme is what we would expect it to be.

Lemma 1.16. *Suppose $X = \operatorname{Spec} A$ is affine, and let $s \in \mathcal{O}_X(X) = A$ be a global section of the structure sheaf. Then $\mathcal{Z}(s)$ is the closed subscheme associated to the the ideal sA of A.*

Proof. Let $I \subseteq A$ be the ideal associated to $\mathcal{Z}(s)$. By definition, we have

$$I = \{f(s) : f \in \operatorname{Hom}_A(A, A)\}.$$

But the elements of $\operatorname{Hom}_A(A, A)$ are exactly the multiplication-by-a maps for each $a \in A$. So we see that

$$I = \{as : a \in A\} = sA.$$ □

Lemma 1.17. *Let $\mathcal{L}$ be an invertible sheaf on X and $s \in \mathcal{L}(X)$ a global section. For any $x \in X$ we have $x \in \mathcal{Z}(s)$ if and only if $x \notin D(s)$.*

Proof. The statement is local, so may assume that $X = \operatorname{Spec} A$ and $s \in A$. Then the statement follows since $sA \subseteq \mathfrak{m}_x$ if and only if $s \in \mathfrak{m}_x A$. □

Lemma 1.18. *Let $\mathcal{L}$ be an invertible sheaf on X and $s \in \mathcal{L}(X)$ a global section. Then $\mathcal{Z}(s)$ is an effective Cartier divisor of X if and only if s is a regular section of X.*

Proof. The question is local, so we may reduce to the situation where $X = \operatorname{Spec} A$ and $\mathcal{L} = \mathcal{O}_X$ is trivial, and then the statement follows directly from Lemma 1.16. □

Example 1.19. Let $D \subseteq X$ be an effective Cartier divisor. Then the canonical section 1_D of the associated sheaf $\mathcal{O}_X(D)$ is regular, since its zero scheme $\mathcal{Z}(1_D)$ is exactly the Cartier divisor D.

We can also characterize whether a global section is regular by looking at whether it is non-zero at the components of X. If X is not reduced, we need to take into account possible embedded components. We denote the set of associated points of X by $\operatorname{Ass}(X)$.

Lemma 1.20. *Let $\mathcal{L}$ be invertible on X and s a global section of $\mathcal{L}$. Then s is a regular section of $\mathcal{L}$ if and only if $\operatorname{Ass}(X) \subseteq D(s)$.*

Proof. For any open $U \subseteq X$ we have $\operatorname{Ass}(U) = \operatorname{Ass}(X) \cap U$ since restricting to an open subset does not change the local rings. Together with the previous lemma, this shows that the question is local, so we reduce to the situation where $X = \operatorname{Spec} A$ with A Noetherian, and $\mathcal{L} = \mathcal{O}_X$ is trivial. Then the statement follows since the set of zero-divisors of a Noetherian ring A is exactly equal to union of all associated primes of A, by [Sta17, Lemma 10.62.9]. □

Theorem 1.21. *Let $\mathcal{L}$ be an effective invertible sheaf on X and $s \in \mathcal{L}(X)$ a regular section. Let $D = \mathcal{Z}(s)$ be the zero scheme of s. Then D is an effective Cartier divisor on X, and there is a unique isomorphism $\mathcal{O}_X(D) \xrightarrow{\sim} \mathcal{L}$ that maps the canonical section 1_D to s.*

Proof. That D is an effective Cartier divisor is Lemma 1.18. For the isomorphism, we construct it locally.

First suppose that $X = \operatorname{Spec} A$ is affine and $\mathcal{L}$ is free on X. Choose an isomorphism $\varphi\colon \mathcal{O}_X \to \mathcal{L}$, and let $t = \varphi^{-1}(s) \in A$. As before, $\mathcal{Z}(s)$ is the zero scheme associated to the ideal tA of A. Therefore $\mathcal{O}_X(D) = \mathcal{H}om(t\mathcal{O}_X, \mathcal{O}_X)$. The morphism $\operatorname{Hom}_A(tA, A) \to A$ given by $f \mapsto f(t)$ is an isomorphism, since t is regular (the inverse is given by $a \mapsto (tb \mapsto ab)$). This isomorphism induces an isomorphism $\mathcal{O}_X(D) \to \mathcal{O}_X$, which sends 1_D to t. Composing with the isomorphism $\mathcal{O}_X \to \mathcal{L}$, we have an isomorphism $\mathcal{O}_X(D) \to \mathcal{L}$ sending 1_D to s.

To see that this isomorphism is unique, it is enough to show that $\mathcal{O}_X$ has no non-trivial $\mathcal{O}_X$-module automorphisms that keep t fixed. But since $X = \operatorname{Spec} A$ is affine, this is the same as showing that there are no A-module automorphisms of A that keep t fixed. But any such automorphism is given by multiplication by a unit $u \in A^\times$, and from $ut = t$ and the regularity of t we immediately get $u = 1$.

Now we know that the isomorphism we want to construct exists locally, and because of the uniqueness, these locally defined isomorphisms glue to a unique globally defined isomorphism. □

We have now the following characterizations of regular sections.

Corollary 1.22. *Let $\mathcal{L}$ be an invertible sheaf on X and $s \in \mathcal{L}(X)$ a global section. The following are equivalent.*

1. *s is regular.*
2. *The morphism $\mathcal{O}_X \to \mathcal{L}$ defined by s is injective.*
3. $\operatorname{Ass}(X) \subseteq D(s)$.
4. $\operatorname{Ass}(X) \cap |\mathcal{Z}(s)| = \emptyset$.
5. *$\mathcal{Z}(s)$ is an effective Cartier divisor on X.*
6. *There is an isomorphism $\mathcal{O}_X(D) \xrightarrow{\sim} \mathcal{L}$ for some effective Cartier divisor $D \subseteq X$ that maps 1_D to s.*

Proof. The equivalence $1 \Leftrightarrow 2$ is Lemma 1.14, $1 \Leftrightarrow 3$ is Lemma 1.20, $3 \Leftrightarrow 4$ follows from Lemma 1.17, $1 \Leftrightarrow 5$ is Lemma 1.18 and $1 \Leftrightarrow 6$ is Theorem 1.21. □

Corollary 1.23. *An invertible sheaf $\mathcal{L}$ is effective if and only if it is isomorphic to the associated sheaf $\mathcal{O}_X(D)$ of some effective Cartier divisor D.* □

As an application of the above theory, we will prove a statement about inverse images of effective Cartier divisors that we will need in Chapter 3. We first prove a lemma.

Lemma 1.24. *Let Y be a locally Noetherian scheme and $f\colon Y \to X$ an affine morphism (i.e. a morphism such that the inverse image of any affine open subscheme is affine). Let $\mathcal{L}$ be an invertible sheaf on X and $s \in \mathcal{L}(X)$ a section. Then we have an equality*

$$f^{-1}(\mathcal{Z}(s)) = \mathcal{Z}(f^*s)$$

as closed subschemes of Y.

Proof. The statement is local on X, so we may reduce to the situation were $X = \operatorname{Spec} A$ is affine and $\mathcal{L} = \mathcal{O}_X$ is trivial. Then $s \in A$. Since f is assumed to be affine, $Y = \operatorname{Spec} B$ is also affine, and f corresponds to a ring morphism $\varphi\colon A \to B$. Then $\mathcal{Z}(s)$ corresponds to the ideal sA by Lemma 1.16, and $\mathcal{Z}(f^*s)$ to the ideal $\varphi(s)B$ of B. Now the theorem follows from the equality

$$\varphi(sA)B = \varphi(s)B$$

of ideals of B. □

Theorem 1.25. *Let $f\colon Y \to X$ be an affine morphism of locally Noetherian schemes, and $D \subseteq X$ an effective Cartier divisor. Assume that $f(\operatorname{Ass} Y) \subseteq \operatorname{Ass} X$. Then $E = f^{-1}(D)$ is an effective Cartier divisor on Y, and there is a unique isomorphism of $\mathcal{O}_Y$-modules $f^*\mathcal{O}_X(D) \to \mathcal{O}_Y(E)$ that maps f^*1_D to 1_E.*

Proof. Since $D = \mathcal{Z}(1_D)$, we have

$$E = f^{-1}(D) = f^{-1}\mathcal{Z}(1_D) = \mathcal{Z}(f^*1_D),$$

where the last equality follows from Lemma 1.24. By the assumption on the sets of associated points of X and Y, we have

$$|\mathcal{Z}(f^*1_D)| \cap \operatorname{Ass} Y \;\subseteq\; |f^{-1}\mathcal{Z}(1_D)| \cap f^{-1}(\operatorname{Ass} X) \;=\; f^{-1}\big(|\mathcal{Z}(1_D)| \cap \operatorname{Ass} X\big) \;=\; \emptyset,$$

where the last equality follows from Lemma 1.20 and the fact that 1_D is a regular section of $\mathcal{O}_X(D)$. So from the same lemma, we see that f^*1_D is a regular section of $f^*\mathcal{O}_X(D)$. Since the zero scheme of f^*1_D is exactly E, it follows from Theorem 1.21 that E is an effective Cartier divisor and that there is a unique isomorphism of $\mathcal{O}_Y$-modules $f^*\mathcal{O}_X(D) \to \mathcal{O}_Y(E)$ that maps f^*1_D to 1_E. □

1.4 Morphisms to projective space

In this section we investigate the relation between invertible sheaves and morphisms to the $\mathbb{P}^n$.

Definition 1.26. Let $n \geq 1$. We will call an invertible sheaf $\mathcal{L}$ on X *n-generated*[1] if there are global sections $s_1, \ldots, s_n \in \mathcal{L}(X)$ such that for every $x \in X$ the restrictions of the s_i generate the stalk $\mathcal{L}_x$ as an $\mathcal{O}_{X,x}$-module. We say that the collection $s_1, \ldots, s_n$ *generates* $\mathcal{L}$.

[1] This terminology is different from the terminology in [Liu02]. Liu would call this 'generated by n global sections', as he uses the term 'finitely generated' for what I would call 'locally finitely generated', and 'generated by a finite number of global sections' for what I call 'finitely generated'.

More abstractly, one might say that an invertible sheaf is n-generated if it is a quotient of the sheaf $\mathcal{O}_X^n$.

Example 1.27. Let X be a smooth, geometrically irreducible curve and $\mathcal{L}$ an invertible sheaf on X. Then for all $x \in X$ the stalk $\mathcal{O}_{X,x}$ is a discrete valuation ring with maximal ideal $\mathfrak{m}_x$, and any isomorphism between $\mathcal{O}_{X,x}$ and $\mathcal{L}_x$ defines a 'valuation' on $\mathcal{L}_x$. Then a collection $s_1, \ldots, s_n \in \mathcal{L}(X)$ generates $\mathcal{L}$ if and only if for every $x \in X$ there is an index i such that s_i has valuation 0 ('does not vanish') at x.

More generally, we can say the following. We say that s *vanishes* in x if $x \notin D(s)$, otherwise that s *does not vanish* in x.

Lemma 1.28. *Let $\mathcal{L}$ be an invertible sheaf on X, and $s_1, \ldots, s_n \in \mathcal{L}(X)$ a collection of global sections. Then the s_i generate $\mathcal{L}$ if and only if $X = D(s_1) \cup \cdots \cup D(s_n)$.*

Proof. Taking stalks, this is the same as saying that a given collection of elements of a local ring generates the ring (as an ideal) if and only if at least one of them is not in the maximal ideal. □

Lemma 1.29. *Let $f \colon X \to Y$ be a morphism between locally Noetherian schemes, and let $\mathcal{L}$ be an n-generated invertible sheaf on Y. Then also $f^*\mathcal{L}$ is n-generated.*

Proof. It is clear that $f^*\mathcal{L}$ is an invertible sheaf on X, since pulling back commutes with localization and the pullback of the structure sheaf on Y is the structure sheaf on X. Moreover, from a surjective morphism $\mathcal{O}_Y^n \to \mathcal{L}$ we get a surjective morphism $\mathcal{O}_X^n \to f^*\mathcal{L}$ since the functor f^* is right exact and $f^*\mathcal{O}_Y^n = \mathcal{O}_X^n$. □

We will show that $(n+1)$-generated invertible sheaves correspond to maps to $\mathbb{P}^n_{\mathbb{Z}}$. Recall that the invertible sheaf $\mathcal{O}(1)$ (*Serre's twisting sheaf*) on $\mathbb{P}^n_{\mathbb{Z}}$ is the sheaf associated to the homogeneous degree 1 part of $\mathbb{Z}[X_0, \ldots, X_n]$ (see [Har77, Definition II.5.12] or [Liu02, Section 5.1.4] for the details).

Theorem 1.30. *Let $n \geq 1$. Then an invertible sheaf $\mathcal{L}$ on X is $(n+1)$-generated if and only if $\mathcal{L}$ is isomorphic to $f^*\mathcal{O}(1)$ for some morphism $f \colon X \to \mathbb{P}^n_{\mathbb{Z}}$. More precisely, if $s_0, \ldots, s_n \in \mathcal{L}(X)$ are generators for $\mathcal{L}$, and $x_0, \ldots, x_n \in \mathcal{O}(1)(\mathbb{P}^n_{\mathbb{Z}})$ are the standard coordinates, then there is a unique morphism $f \colon X \to \mathbb{P}^n_{\mathbb{Z}}$ and a unique isomorphism $\mathcal{L} \cong f^*\mathcal{O}(1)$ such that s_i maps to f^*x_i.*

Proof. Notice that $\mathcal{O}(1)$ on $\mathbb{P}^n$ is $(n+1)$-generated, namely by the standard coordinates. Hence, by the previous lemma, $f^*\mathcal{O}(1)$ is $(n+1)$-generated as well for any morphism $f \colon X \to \mathbb{P}^n_{\mathbb{Z}}$.

Suppose now that $\mathcal{L}$ is $(n+1)$-generated. We sketch the construction of a morphism $f \colon X \to \mathbb{P}^n$ as above. Note that we only need to prove the claim for X affine and $\mathcal{L}$ trivial, since then a standard gluing argument proves the claim for arbitrary X and $\mathcal{L}$.

So assume $X = \operatorname{Spec} A$ is affine and $\mathcal{L}$ is trivial on X. Fix an identification $\mathcal{L} = \mathcal{O}_X$. Fix generators $s_0, \ldots, s_n \in \mathcal{L}(X) = A$. We first construct for every $0 \leq i \leq n$ a morphism $D(s_i) \to U_i$, where U_i is the affine open in $\mathbb{P}^n_{\mathbb{Z}}$ where the i-th coordinate is non-zero. Notice that

$$U_i = \operatorname{Spec} \mathbb{Z}[x_0, \ldots, \widehat{x_i}, \ldots, x_n] = \operatorname{Spec} \mathbb{Z}[x_0, \ldots, x_n]/(x_i - 1),$$

(the hat denotes omission), so to give a morphism $D(s_i) \to U_i$ is the same as giving $n+1$ global sections of the structure sheaf $\mathcal{O}_{D(s_i)}$, the i-th of which equals 1. Moreover, notice that by definition of $D(s_i)$, s_i is a unit in $\mathcal{O}_X(D(s_i))$. Hence, we can define a map $f_i \colon D(s_i) \to \mathbb{P}^n_{\mathbb{Z}}$ by the sections $s_0/s_i, s_1/s_i, \ldots, s_n/s_i$ (i.e. dual to the ring morphism $\mathbb{Z}[x_0, \ldots, x_n]/(x_i - 1) \to A$ given by $X_j \mapsto s_j/s_i$). Notice that the element $s_j/s_i \in A$ does not depend on our identification of $\mathcal{L}$ and $\mathcal{O}_X$, since any other isomorphism differs from the fixed one by multiplication by an element of $A^\times$.

One easily sees that f_i and f_j coincide on $D(s_i) \cap D(s_j)$. Since $X = D(s_0) \cup \cdots \cup D(s_n)$, the f_i glue to a morphism $f\colon X \to \mathbb{P}^n_{\mathbb{Z}}$, and the construction makes clear that $f^* x_i = s_i$ for each i. Uniqueness comes from running the argument in reverse: from $f^* x_i = s_i$ one obtains that $D(s_i)$ must map to $D(x_i) = U_i$, and then we have no choice but to send x_j/x_i to s_j/s_i. □

We can state the above theorem as a universal property for $\mathbb{P}^n$. To do this, we consider pairs $(\mathcal{L}, p)$, where $\mathcal{L}$ is an invertible sheaf on X and p is a surjective $\mathcal{O}_X$-module morphism $\mathcal{O}_X^{n+1} \twoheadrightarrow \mathcal{L}$. We shall consider two such pairs $(\mathcal{L}_1, p_1)$ and $(\mathcal{L}_2, p_2)$ equivalent if there is an isomorphism $\varphi\colon \mathcal{L}_1 \xrightarrow{\sim} \mathcal{L}_2$ such that $p_2 = \varphi \circ p_1$.

Corollary 1.31. *Let $n \geq 1$. There is a bijection between the set of morphisms $X \to \mathbb{P}^n$ and the collection of pairs $(\mathcal{L}, p)$ as above up to equivalence.*

Proof. Note that giving $n+1$ global sections $s_0, \ldots, s_n$ of an invertible sheaf $\mathcal{L}$ is the same as giving a morphism $\mathcal{O}_X^{n+1} \to \mathcal{L}$, and that the s_i generate $\mathcal{L}$ if and only if the corresponding morphism $\mathcal{O}_X^{n+1} \to \mathcal{L}$ is surjective. Hence, to any such pair $(\mathcal{L}, p)$, the theorem above associates a unique morphism $f\colon X \to \mathbb{P}^n$, and one checks that two pairs $(\mathcal{L}_1, p_1)$ and $(\mathcal{L}_2, p_2)$ induce the same morphism if and only if they are equivalent. □

Corollary 1.32. *Let X be a locally Noetherian scheme over a base scheme S. Then there is a bijection between the set of morphisms $X \to \mathbb{P}^n_S$ over S and the collection of pairs $(\mathcal{L}, p)$ as above up to equivalence.*

Proof. Indeed, we have $\mathbb{P}^n_S = \mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S$. So to give a morphism $X \to \mathbb{P}^n_S$ is the same as giving a morphism $X \to \mathbb{P}^n_{\mathbb{Z}}$ and a morphism $X \to S$ (they are automatically compatible with the maps to $\operatorname{Spec} \mathbb{Z}$). But for an S-scheme there is only one S-morphism to S. Hence, there is a bijection between morphisms $X \to \mathbb{P}^n_{\mathbb{Z}}$ and S-morphisms $X \to \mathbb{P}^n_S$. The rest now follows from the previous corollary. □

Remark 1.33. It should be noted that in the above theorems, the condition that X be locally Noetherian is not really necessary. In fact, Theorem 1.30 holds for any locally ringed space X, and the proof is essentially the same.

It is interesting to consider the case $X = \operatorname{Spec} k$ for a field k. In this case there is only one invertible sheaf on X, namely $\mathcal{O}_X$ itself (because an invertible sheaf by definition needs to be trivial on an open neighbourhood of the single point of $\operatorname{Spec} k$). Therefore, we are considering surjective k-linear maps $k^{n+1} \to k$ up to multiplication by a non-zero element (since these are the automorphisms of k). Clearly, such a map is uniquely determined by its kernel in k^{n+1}, which is a n-dimensional subspace. So by the above corollaries, the set $\mathbb{P}^n(k)$ of k-valued points of $\mathbb{P}^n$ (i.e. the collection of morphisms $\operatorname{Spec} k \to \mathbb{P}^n$) is naturally in bijection with the set of n-dimensional subspaces of k^{n+1}, as expected.

Chapter 2

Degrees

The purpose of this chapter is to study the degrees of morphisms, Cartier divisors and invertible sheaves. We will define the degrees for each, and study the relations between them. Again, references for this chapter are [Sta17], [Liu02] and [Har77].

In this chapter, we cannot work in as much generality as the previous chapter. We will therefore mostly be concerned with curves. Usually, we work over a field, but later we will need to work over discrete valuation rings as well. In order to fix notation, we use the following definition for curves.

Definition 2.1. A scheme X over a Noetherian base scheme S will be called a *curve over S* if X is projective and flat over S and if the irreducible components of the fiber X_s have dimension 1 for all $s \in S$. If A is a ring, then a curve over A is a curve over $\operatorname{Spec} A$.

2.1 Degree of a morphism

Definition 2.2. Let X and Y be integral schemes and $f\colon X \to Y$ a finite flat morphism. Then we define the *degree* of f (notation $\deg f$) to be the degree of the field extension $K(Y) \hookrightarrow K(X)$ induced by f. Additionally, for a morphism $f : X \to Y$ where the fiber over the generic point of Y is empty we set $\deg f = 0$.

The degree of a finite flat morphism is related to the size of the fibers. The precise statement is the following.

Proposition 2.3. *Let X and Y be Noetherian integral schemes and $f\colon X \to Y$ a finite flat morphism. Then for any point $y \in Y$ we have*

$$\deg f = \dim_{\kappa(y)} H^0(X_y, \mathcal{O}_{X_y}).$$

Proof. Let $U = \operatorname{Spec} A$ be an open affine neighbourhood of y. Then $f^{-1}U$ is open affine in X, say $\operatorname{Spec} B$ for some finite A-algebra. Replacing A with the localization of $A_{\mathfrak{p}}$ at the prime $\mathfrak{p}$ corresponding to y, and B with $B \otimes_A A_{\mathfrak{p}}$, we may assume that A is local. Then B is a finitely generated, flat module over a local ring, and therefore free by [Sta17, Lemma 10.77.4], say of rank r. Then $B = A^r$ as A-modules, hence

$$\dim_{A/\mathfrak{p}} B \otimes_A A/\mathfrak{p} = r = \dim_{Q(A)} B \otimes_A Q(A)$$

(where $Q(A)$ denotes the field of fractions of A). The statement follows since $B \otimes_A Q(A) = Q(B)$ for a finite integral A-algebra B. □

2.2 Degree of a Cartier divisor

We start by defining the degree for effective Cartier divisors.

Definition 2.4. Let X be a curve over a field k, and $D \subseteq X$ an effective Cartier divisor. Then we define the *degree* of D over k to be

$$\deg_k D = \dim_k H^0(D, \mathcal{O}_D).$$

Notice that D is closed and of codimension 1 in the Noetherian (because it is projective over a field) 1-dimensional scheme X, so D is finite. Hence, $\deg_k D$ is finite.

It turns out that degrees are additive, in the following sense.

Proposition 2.5. *Let $D, E \subseteq X$ be effective Cartier divisors on a curve X over k. Then* $\deg_k(D+E) = \deg_k D + \deg_k E$.

Proof. Since D and E are finite and zero-dimensional, they are discrete. Hence, we have $H^0(D, \mathcal{O}_D) = \bigoplus_{x \in D} \mathcal{O}_{D,x}$, so

$$\deg_k D = \sum_{x \in D} \dim_k \mathcal{O}_{D,x},$$

and similarly for E. Hence, it is enough to show that for any $x \in D \cap E$,

$$\dim_k \mathcal{O}_{D,x} + \dim_k \mathcal{O}_{E,x} = \dim_k \mathcal{O}_{D+E,x}.$$

To do this, we can take an affine open $U = \operatorname{Spec} A$ around x and regular elements $f, g \in A$ such that $D \cap U = \operatorname{Spec} A/fA$ and $E \cap U = \operatorname{Spec} A/gA$ (Lemma 1.7). Let $\mathfrak{p}$ denote the prime ideal of A corresponding to x. Then we have

$$\mathcal{O}_{D,x} = (A/fA)_{\overline{\mathfrak{p}}} = (A/fA) \otimes_A A_{\mathfrak{p}}$$

and similarly for E. Since f and g are regular in A, we have an exact sequence

$$0 \to A/fA \xrightarrow{g\cdot} A/fgA \to A/gA \to 0.$$

Localizing this exact sequence at $\mathfrak{p}$ and considering the dimensions of the resulting k-vector spaces then gives the result. □

The above proposition allows us to extend the notion of degree to arbitrary Cartier divisors.

Definition 2.6. Let X be a curve over a field k, and $D = E - F$ a Cartier divisor on X. Then we set $\deg_k D = \deg_k E - \deg_k F$.

Then Proposition 2.5 immediately extends to arbitrary Cartier divisors.

Corollary 2.7. *Let D, E be Cartier divisors on a curve X over k. Then* $\deg_k(D+E) = \deg_k D + \deg_k E$. □

2.3 Degree of an invertible sheaf

Definition 2.8. Let X be a projective scheme over a field k and $\mathcal{F}$ a coherent sheaf. Then we define the *Euler characteristic* of $\mathcal{F}$ to be the number

$$\chi(\mathcal{F}) = \sum_{i=0}^{\infty}(-1)^i h^i(X, \mathcal{F}).$$

Here $h^i(X, \mathcal{F}) = \dim_k H^i(X, \mathcal{F})$.

Notice that if X is a curve over a field k and $\mathcal{F}$ a coherent sheaf on X, then $h^i(X, \mathcal{F}) = 0$ for all $i > 1$, so in that case we just have $\chi(\mathcal{F}) = h^0(X, \mathcal{F}) - h^1(X, \mathcal{F})$.

The following is Proposition 5.3.28 in [Liu02]. It states that the Euler characteristic is constant among fibers.

Theorem 2.9. *Let $S = \operatorname{Spec} A$ be the spectrum of a discrete valuation ring A, with generic point η and closed point s. Let X be a projective scheme over S, and $\mathcal{F}$ a coherent sheaf on X which is flat over S. Then*

$$\chi_{\kappa(\eta)}(\mathcal{F}_\eta) = \chi_{\kappa(s)}(\mathcal{F}_s). \qquad \square$$

Definition 2.10. Let X be a curve over a field k. Let $\mathcal{L}$ be an invertible sheaf on X. Then the *degree of* $\mathcal{L}$ over k is defined to be

$$\deg_k \mathcal{L} = \chi_k(\mathcal{L}) - \chi_k(\mathcal{O}_X).$$

Now Theorem 2.9 translates to constancy of the degree of invertible sheaves among fibers.

Proposition 2.11. *Let $S = \operatorname{Spec} A$ be the spectrum of a discrete valuation ring A, with generic point η and closed point s. Let X be a curve over S, and $\mathcal{L}$ an invertible sheaf over X. Then*

$$\deg_{\kappa(\eta)} \mathcal{L}_\eta = \deg_{\kappa(s)} \mathcal{L}_s.$$

Proof. Notice that $\mathcal{L}$ is flat on X, since it is locally free. Since the structure map $X \to S$ is flat by our definition of curve, $\mathcal{L}$ and $\mathcal{O}_X$ are flat over S. Thus the statement follows from Theorem 2.9 after noting that $(\mathcal{O}_X)_\eta = \mathcal{O}_{X_\eta}$ and $(\mathcal{O}_X)_s = \mathcal{O}_{X_s}$. $\square$

We have now defined degrees for Cartier divisors and for invertible sheaves. Since every Cartier divisor comes with an invertible sheaf, we would hope that these degrees coincide.

Theorem 2.12. *Let X be a curve over a field k and D a Cartier divisor on X. Then*

$$\deg_k D = \deg_k \mathcal{O}_X(D).$$

Proof. We first consider the case where D is effective. We consider D as a subscheme of X, and the structure sheaf $\mathcal{O}_D$ of X as a $\mathcal{O}_X$-module via the embedding $D \to X$. Consider the natural sequence of $\mathcal{O}_X$-modules

$$0 \to \mathcal{I}(D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0.$$

It is exact, since locally this is of the form $0 \to fA \to A \to A/fA \to 0$. The sequence stays flat after tensoring with $\mathcal{O}_X(D)$, since $\mathcal{O}_X(D)$ is locally free and therefore flat. This gives us the short exact sequence

$$0 \to \mathcal{O}_X \to \mathcal{O}_X(D) \to \mathcal{O}_X(D)|_D \to 0.$$

Now we note that D is a finite zero-dimensional scheme and therefore discrete. Therefore, $\mathcal{O}_X(D)|_D$ is just the direct sum of its stalks, and those are free of rank 1. Hence, we find that $\mathcal{O}_X(D)|_D \cong O_D$. In particular this shows that $H^0(X, \mathcal{O}_X(D)|_D) \cong H^0(D, \mathcal{O}_D)$ and $H^1(X, \mathcal{O}_X(D)|_D) = 0$.

Now we take cohomology and find the exact sequence

$$0 \to H^0(X, \mathcal{O}_X) \to H^0(X, \mathcal{O}_X(D)) \to H^0(D, \mathcal{O}_D) \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X(D)) \to 0.$$

Considering the dimensions of these k-vector spaces, we obtain

$$h^0(X, \mathcal{O}_X) - h^0(X, \mathcal{O}_X(D)) + h^0(D, \mathcal{O}_D) - h^1(X, \mathcal{O}_X) + h^1(X, \mathcal{O}_X(D)) = 0,$$

and rearranging gives

$$\deg_k D = \chi(\mathcal{O}_X(D)) - \chi(\mathcal{O}_X) = \deg_k \mathcal{O}_X(D).$$

Now we consider the general case. Let $D = E - F$, with E and F effective Cartier divisors. Similar to the above, we have an exact sequence

$$0 \to \mathcal{I}(F) \to \mathcal{O}_X \to \mathcal{O}_F \to 0,$$

which gives after tensoring with $\mathcal{O}_X(E)$ the exact sequence

$$0 \to \mathcal{O}_X(D) \to \mathcal{O}_X(E) \to \mathcal{O}_X(E)|_F \to 0.$$

By the same reasoning as before we have $H^0(X, \mathcal{O}_X(E)|_F) \cong H^0(F, \mathcal{O}_F)$ and $H^1(X, \mathcal{O}_X(E)|_F) = 0$. Again we take the long exact sequence and consider the dimensions over k. We find that

$$\deg_k F = \chi(\mathcal{O}_X(E)) - \chi(\mathcal{O}_X(D)) = \deg_k \mathcal{O}_X(E) - \deg_k \mathcal{O}_X(D) = \deg_k E - \deg_k \mathcal{O}_X(D),$$

and therefore $\deg_k \mathcal{O}_X(D) = \deg_k E - \deg_k F = \deg_k D$. □

Suppose we have a 2-generated invertible sheaf $\mathcal{L}$ on a curve X over a field. Then to $\mathcal{L}$ (and a choice of generators) we have associated a morphism $f\colon X \to \mathbb{P}^1$. Our next goal is to show that the degree of $\mathcal{L}$ coincides with the degree of f, at least in the context where both make sense. We first prove the following statements.

Proposition 2.13. *Let X be a curve over a field k and $f\colon X \to \mathbb{P}^1_k$ a finite flat morphism. Let D be the point $(1:0) \in \mathbb{P}^1_k$ considered as a reduced subscheme of $\mathbb{P}^1_k$.*

1. *D is an effective Cartier divisor on $\mathbb{P}^1_k$, and $\mathcal{O}_{\mathbb{P}^1_k}(D) \cong \mathcal{O}(1)$.*
2. *The fiber $X_{(1:0)}$ over $(1:0)$ is an effective Cartier divisor on X, and $\mathcal{O}_X(X_{(1:0)}) = f^*\mathcal{O}(1)$.*
3. *We have $\deg f = \deg_k f^*\mathcal{O}(1)$.*

Proof. Let $\mathcal{I} = \mathcal{I}(D)$ be the sheaf of ideals corresponding to D.

1. To show that $\mathcal{O}_{\mathbb{P}^1_k}(D)$ is isomorphic to $\mathcal{O}(1)$ it is enough to show that $\mathcal{I}$ is isomorpic to $\mathcal{O}(1)^{\otimes -1} = \mathcal{O}(-1)$. Let x_0 and x_1 be the coordinates on $\mathbb{P}^1_k = \operatorname{Proj} k[x_0, x_1]$. Let $U_0 = D(x_0)$ and $U_1 = D(x_1)$. Keeping track of all gradings, we have

$$U_0 = \operatorname{Spec} k[\frac{x_1}{x_0}] \qquad U_1 = \operatorname{Spec} k[\frac{x_0}{x_1}]$$

$$\mathcal{O}(-1)|_{U_0} = \big(\frac{1}{x_0} \cdot k[\frac{x_1}{x_0}]\big)^\sim \qquad \mathcal{O}(-1)|_{U_1} = \big(\frac{1}{x_1} \cdot k[\frac{x_0}{x_1}]\big)^\sim$$

$$\mathcal{I}|_{U_0} = \big(\frac{x_1}{x_0} \cdot k[\frac{x_1}{x_0}]\big)^\sim \qquad \mathcal{I}|_{U_1} = \big(1 \cdot k[\frac{x_0}{x_1}]\big)^\sim$$

From these computations we see that multiplying by x_1 defines an isomorphism $\mathcal{O}(-1) \xrightarrow{\sim} \mathcal{I}$, which induces an isomorphism $\mathcal{O}_{\mathbb{P}^1_k}(D) \xrightarrow{\sim} \mathcal{O}(1)$. Moreover, since $\mathcal{O}(-1)$ is invertible, $\mathcal{I}$ is invertible, so D is indeed an effective Cartier divisor.

2. The sheaf of ideals corresponding to $X_{(1:0)} = f^{-1}(D)$ is the sheaf $f^{-1}(\mathcal{I}) \cdot \mathcal{O}_X$. By flatness of f, we have $f^{-1}(\mathcal{I}) \cdot \mathcal{O}_X = f^*\mathcal{I}$. Since $\mathcal{I}$ is invertible, it follows that the ideal sheaf $f^{-1}(\mathcal{I}) \cdot \mathcal{O}_X$ is invertible, so $X_{(1:0)}$ is an effective Cartier divisor.

   Consider the natural map

   $$\varphi\colon f^*\mathcal{O}_{\mathbb{P}^1_k}(D) = f^*\mathcal{H}om_{\mathcal{O}_{\mathbb{P}^1_k}}(\mathcal{I}, \mathcal{O}_{\mathbb{P}^1_k}) \to \mathcal{H}om_{\mathcal{O}_X}(f^*\mathcal{I}, f^*\mathcal{O}_{\mathbb{P}^1_k}) = \mathcal{H}om_{\mathcal{O}_X}(f^{-1}\mathcal{I}, \mathcal{O}_X).$$

   By considering the stalks, one sees that this map is an isomorphism, since all involved sheaves are locally free of rank 1. Hence, φ is an isomorphism. Thus, we get

   $$f^*\mathcal{O}(1) \cong f^*\mathcal{O}_{\mathbb{P}^1_k}(D) \cong \mathcal{H}om_{\mathcal{O}_X}(f^{-1}\mathcal{I}, \mathcal{O}_X) = \mathcal{O}_X(X_{(1:0)}).$$

3. Combining the above with Proposition 2.3 and Theorem 2.12 we obtain

   $$\deg_k f^*\mathcal{O}(1) = \deg_k \mathcal{O}_X(X_{(1:0)}) = \deg_k X_{(1:0)} = \deg f. \qquad \square$$

Theorem 2.14. *Let X be an integral curve over a field k and $\mathcal{L}$ a 2-generated invertible sheaf on X. Let $s_0, s_1 \in \mathcal{L}(X)$ be generators, and $f\colon X \to \mathbb{P}^1_k$ the corresponding morphism (see Corollary 1.32). Then $\deg f = \deg_k \mathcal{L}$, and if $\mathcal{L} \ncong \mathcal{O}_X$ then f is finite and flat.*

Proof. If $\mathcal{L} \cong \mathcal{O}_X$, then from the construction of f we see that f is constant, and therefore we have $\deg f = 0 = \deg \mathcal{L}$. Assume that $\mathcal{L} \ncong \mathcal{O}_X$. We note that f is not constant, since otherwise $\mathcal{L} = f^*\mathcal{O}(1)$ would be isomorphic to $\mathcal{O}_X$. Since X and $\mathbb{P}^1_k$ are integral projective curves, any morphism between them is either constant or finite, so f must then be finite. Flatness then follows since $\mathbb{P}^1$ is a Dedekind scheme, so flatness is equivalent to torsion-freeness. Now by Proposition 2.13 it follows that $\deg_k \mathcal{L} = \deg_k f^*\mathcal{O}(1) = \deg f$. □

Chapter 3

Gonality

In this chapter, we define the notions of the gonality and divisor gonality for curves over a field. The goal is to study the behaviour of these quantities under reduction.

3.1 Gonality and divisor gonality

Definition 3.1. Let X be a curve over a field k. The *gonality* $\operatorname{gon} X$ of X over k is the lowest degree of a 2-generated invertible sheaf $\mathcal{L}$ on X such that $\mathcal{L} \not\cong \mathcal{O}_X$. Any such invertible sheaf attaining this minimal degree is called *gonal*.

Using the correspondence between 2-generated invertible sheaves and morphisms to $\mathbb{P}^1$, we can translate this definition to a statement about morphisms to $\mathbb{P}^1$.

Proposition 3.2. *Let X be an integral curve over a field k. Then the gonality of X over k coincides with the lowest degree of a finite morphism $f\colon X \to \mathbb{P}^1_k$.*

Proof. Let $\mathcal{L}$ be a gonal invertible sheaf, s_0 and s_1 generators, and $f\colon X \to \mathbb{P}^1_k$ the corresponding morphism. Since $\mathcal{L} \not\cong \mathcal{O}_X$, Theorem 2.14 implies that f is finite and has degree $\deg \mathcal{L} = \operatorname{gon} X$. Conversely, if $f\colon X \to \mathbb{P}^1_k$ is finite, it is flat since X and $\mathbb{P}^1_k$ are integral and projective over k. The $\mathcal{O}_X$-module $\mathcal{L} = f^*\mathcal{O}(1)$ is a 2-generated invertible sheaf. Since $\deg \mathcal{L} = \deg f > 0$, we have $\mathcal{L} \not\cong \mathcal{O}_X$. Therefore we see that $\deg f = \deg \mathcal{L} \geq \operatorname{gon}_k(X)$. □

Remark 3.3. The notion of gonality is not constant across the literature. For instance, [Eis05] defines the gonality of X as the lowest degree of a nonconstant morphism $X \to \mathbb{P}^1$, in [DS17] the gonality is the lowest degree of a finite morphism $X \to \mathbb{P}^1_k$ and in [Poo07] the gonality is the lowest degree of a dominant rational map $X \dashrightarrow \mathbb{P}^1_k$. [Cap14] calls a smooth curve X/k d-gonal if it has a linear series of degree d and rank 1 (compare Corollary 3.13), and more general curves are defined to be d-gonal if they are the specialization of a family of smooth d-gonal curves. It should be noted, however, that all of these different definitions coincide with ours when X is smooth over k, and at least the first three of these four references deal almost exclusively with gonalities of smooth curves.

Definition 3.4. Let X be a curve over a field k, and D an effective Cartier divisor on X. We will call global sections of $\mathcal{O}_X(D)$ in the image of the canonical map $H^0(X, \mathcal{O}_X) \to H^0(X, \mathcal{O}_X(D))$ *constant*. We will say that D *admits non-constant sections* if there are global sections of $\mathcal{O}_X(D)$ that are not constant.

Lemma 3.5. *Let X be a curve over a field k. An effective Cartier divisor D on X admits non-constant sections if and only if* $\dim_k H^0(X, \mathcal{O}_X) < \dim_k H^0(X, \mathcal{O}_X(D))$.

Proof. Notice that both dimensions are finite since X is projective over k. Since the canonical map $\mathcal{O}_X \to \mathcal{O}_X(D)$ is injective, $H^0(X, \mathcal{O}_X) \to H^0(X, \mathcal{O}_X(D))$ is also injective, and the result follows. □

Notice that the above lemma implies that if D and E are effective Cartier divisors on X such that $\mathcal{O}_X(D) \cong \mathcal{O}_X(E)$, then D admits non-constant sections if and only if E does.

It turns out that the notion of gonality does not behave very well under reduction. Therefore we introduce a related notion, that of the divisor gonality, which behaves better.

Definition 3.6. The *divisor gonality* $\operatorname{dgon}_k X$ of X over k is the lowest degree of an effective Cartier divisor D on X that admits non-constant sections. Any such effective Cartier divisor attaining this minimal degree is called *gonal*.

We want to show that the divisor gonality of X is a lower bound for the gonality of X. Unfortunately, this is not always the case if the field k we are working over is too small. The problem is that if k is very small, then a 2-generated invertible sheaf may fail to be effective (see Example 3.10 for an example of what can go wrong). Recall that we denote the set of associated points of X by $\operatorname{Ass}(X)$.

Proposition 3.7. *Let X be a curve over a field k and $\mathcal{L}$ a 2-generated invertible sheaf on X. Assume that $\#k \geq \# \operatorname{Ass}(X)$ (this is automatically satisfied if k is infinite). Then there is an effective Cartier divisor D on X such that $\mathcal{L} \cong \mathcal{O}_X(D)$. Moreover, there is a global section $t \in H^0(X, \mathcal{O}_X(D))$ such that 1_D and t generate $\mathcal{O}_X(D)$.*

Proof. Let s_0, s_1 be generators for $\mathcal{L}$. First we show that there are $\alpha_0, \alpha_1 \in k$ such that $s = \alpha_0 s_0 + \alpha_1 s_1$ is a regular section. For any $\eta \in \operatorname{Ass}(X)$, define

$$V_\eta = \{(a,b) \in k^2 : (as_0 + bs_1)_\eta \in \mathfrak{m}_\eta \mathcal{L}_\eta\}.$$

Since $\eta \in D(s_0) \cup D(s_1)$, we have $(1,0) \notin V_\eta$ or $(0,1) \notin V_\eta$. Since V_η is clearly a linear subspace of k^2, it follows that $\dim V_\eta \leq 1$. Since X is Noetherian, $\operatorname{Ass}(X)$ is finite. By the assumption on k, we see that

$$\bigcup_{\eta \in \operatorname{Ass}(X)} V_\eta \neq k^2.$$

Let $(\alpha_0, \alpha_1) \in k^2 \setminus \bigcup_{\eta \in \operatorname{Ass}(X)} V_\eta$, and set $s = \alpha_0 s_0 + \alpha_1 s_1$. Then s does not vanish at η for all $\eta \in \operatorname{Ass}(X)$. By Lemma 1.20 we see that s is regular.

Notice that α_0 or α_1 are not both zero. Without loss of generality, we may assume that $\alpha_0 \neq 0$. Then s and s_1 generate $\mathcal{L}$, since $s_0 = (s - \alpha_1 s_1)/\alpha_0$. Set $D = \mathcal{Z}(s)$. By Lemma 1.18, D is an effective Cartier divisor on X. By Theorem 1.21 there is an isomorphism $\mathcal{L} \cong \mathcal{O}_X(D)$ that maps s to 1_D. Let t be the image of s_1 under this isomorphism, then 1_D and t generate $\mathcal{O}_X(D)$. □

Lemma 3.8. *Let X be a curve over a field k. Let D be an effective Cartier divisor on X and $s \in H^0(X, \mathcal{O}_X(D))$ a global section of $\mathcal{O}_X(D)$ such that $\mathcal{O}_X(D)$ is generated by 1_D and s. Then D admits non-constant sections if and only $D \neq \emptyset$.*

Proof. If $D = \emptyset$ then $\mathcal{O}_X(D) = \mathcal{O}_X$, so D clearly does not admit non-constant sections. For the other direction, suppose that D does not admit non-constant sections. In particular, s is constant. Therefore the canonical map $\mathcal{O}_X \to \mathcal{O}_X(D)$ is surjective (since the generators 1_D and s are in the image). Since it is injective (1_D is a regular section of $\mathcal{O}_X(D)$), this implies that $\mathcal{O}_X(D) \cong \mathcal{O}_X$, and therefore (by Theorem 2.12) that $\deg D = \deg \mathcal{O}_X = 0$, and so $D = \emptyset$. □

Theorem 3.9. *Let X be a curve over a field k. Assume that $\#k \geq \# \operatorname{Ass}(X)$. Then*

$$\operatorname{gon} X \geq \operatorname{dgon} X.$$

Proof. Let $\mathcal{L} \ncong \mathcal{O}_X$ be a 2-generated invertible sheaf on X of degree $\operatorname{gon} X$. Then by Proposition 3.7 there is an effective Cartier divisor D on X with $\mathcal{L} \cong \mathcal{O}_X(D)$, and $\mathcal{O}_X(D)$ is generated by 1_D and a global section $s \in \mathcal{O}_X(D)(X)$. Since $\mathcal{L} \ncong \mathcal{O}_X$, we have $D \neq \emptyset$, so by Lemma 3.8 D admits non-constant sections. Hence, by definition of the divisor gonality and Theorem 2.12, we have

$$\operatorname{dgon}(X) \leq \deg D = \deg \mathcal{O}_X(D) = \deg \mathcal{L} = \operatorname{gon}(X). \qquad \square$$

Example 3.10. It should be noted that the assumption on the size of k in 3.9 cannot be omitted. As an example, let k be a finite field, and let X be the projective line $\mathbb{P}^1_k$, but with an added embedded point at each rational point of $\mathbb{P}^1_k$. An explicit embedding of X in $\mathbb{P}^2_k$ is for example given by the equations

$$yz \prod_{\alpha \in k} (x - \alpha z) = y^2 = 0.$$

This is a projective curve over k. By construction, every rational point of X is an embedded point. Since a Cartier divisor can not be supported at an embedded point by Corollary 1.22.4, any non-zero effective Cartier divisor on X will have degree at least 2. In particular, $\operatorname{dgon} X \geq 2$.

We claim that $\operatorname{gon} X = 1$. There is a morphism $f\colon X \to \mathbb{P}^1_k$ that sends y to 0. This morphism is an isomorphism away from the embedded points of X. Let $\mathcal{L} = f^{-1}\mathcal{O}(1)$. It is a 2-generated invertible sheaf by Lemma 1.29. We calculate the degree of $\mathcal{L}$. If we change base from k to an extension field L of k, then the degree of $\mathcal{L}$ does not change, because the cohomology groups in the new situation have same dimension over L as the old cohomology groups had over k. So to calculate the degree of $\mathcal{L}$, we may replace k by its algebraic closure.

Let $P \in \mathbb{P}^1_k$ be a point not in the image of any associated point of X (we can do that now, since k is infinite while $\operatorname{Ass} X$ is finite). Then P is an effective Cartier divisor of degree 1 (its residue field is k since k is algebraically closed). Then a calculation very similar to Proposition 2.13 shows that $\mathcal{O}(1) \cong \mathcal{O}_{\mathbb{P}^1_k}(P)$, so that $\mathcal{L} = f^*\mathcal{O}(1) \cong f^*\mathcal{O}_{\mathbb{P}^1_k}(P)$. Notice that the global section f^*1_P of $f^*\mathcal{O}_{\mathbb{P}^1_k}(P)$ only vanishes in the fiber X_P above P, and since there are no associated points of X in this fiber, Corollary 1.22.4 implies that f^*1_P is regular. By Lemma 1.24 we have $\mathcal{Z}(f^*1_P) = f^{-1}\mathcal{Z}(1_P) = X_P$, and so $f^*\mathcal{O}_{\mathbb{P}^1_k}(P) \cong \mathcal{O}_X(X_P)$. But since f is an isomorphism in a neighbourhood of P, we have $\deg X_P = \deg P = 1$. Putting this all together we have

$$\deg \mathcal{L} = \deg f^*\mathcal{O}_{\mathbb{P}^1_k}(P) = \deg \mathcal{O}_X(X_P) = \deg X_P = 1.$$

Hence $\mathcal{L}$ already had degree 1 before base changing to an algebraic closure. Hence $\operatorname{gon} X = 1$.

3.2 Removing common zeros

We have shown that under some assumptions on k, the divisor gonality of a curve X over k does not exceed the gonality of X. If we have an effective Cartier divisor $D \subseteq X$ admitting a non-constant section s, then one can ask how close 1_D and s are to generating $\mathcal{O}_X(D)$. In general, 1_D and s do not generate $\mathcal{O}_X(D)$, because s may vanish at some of the points of D. In this section, we will look at some situations where we can partially or completely remove such common zeros of s and 1_D. The main tool is the following theorem.

Theorem 3.11. *Let X be a curve over a field, let $D \subseteq X$ be an effective Cartier divisor and let $s \in H^0(X, \mathcal{O}_X(D))$ be a global section. Let E be an effective Cartier divisor on X such that $E \subseteq \mathcal{Z}(s)$ and $E \subseteq D$ as closed subschemes of X. Then the Cartier divisor $D - E$ is* *effective, and there is a unique $t \in H^0(X, \mathcal{O}_X(D-E))$ that maps to s under the canonical map $H^0(X, \mathcal{O}_X(D-E)) \to H^0(X, \mathcal{O}_X(D))$. Moreover, t is constant in $\mathcal{O}_X(D-E)$ if and only if s is constant in $\mathcal{O}_X(D)$.*

Proof. Since $E \subseteq D$, from Lemma 1.11 $D-E$ is effective. Consider the canonical exact sequence

$$0 \to \mathcal{I}(E) \to \mathcal{O}_X \to \mathcal{O}_E \to 0.$$

We tensor with $\mathcal{O}_X(D)$ to get an exact sequence

$$0 \to \mathcal{O}_X(D-E) \to \mathcal{O}_X(D) \to \mathcal{O}_X(D)|_E \to 0.$$

Now we take global sections, and we consider the canonical maps from $H^0(X, \mathcal{O}_X)$, to get the following commutative diagram with exact row.

$$\begin{tikzcd}
& H^0(X, \mathcal{O}_X) \arrow[d] \arrow[dr] & & \\
0 \arrow[r] & H^0(X, \mathcal{O}_X(D-E)) \arrow[r] & H^0(X, \mathcal{O}_X(D)) \arrow[r] & H^0(X, \mathcal{O}_X(D)|_E) \arrow[r] & 0
\end{tikzcd}$$

The global section $s \in H^0(X, \mathcal{O}_X(D))$ vanishes in E since $E \subseteq \mathcal{Z}(s)$, and so it comes from a unique element $t \in H^0(X, \mathcal{O}_X(D-E))$. Moreover, s is in the image of $H^0(X, \mathcal{O}_X)$ if and only if t is. □

Corollary 3.12. *Let X be a curve over a field, and let D be an effective Cartier divisor. Let $s \in H^0(X, \mathcal{O}_X(D))$ be a non-constant global section.*

1. *Let $x \in D$ be a point such that $\mathcal{O}_{X,x}$ is regular. If s vanishes in x, then D is not gonal (i.e. $\operatorname{dgon} X < \deg D$).*
2. *If for all $y \in D$, the local ring $\mathcal{O}_{X,y}$ is regular, then $\operatorname{gon} X \leq \deg D$.*

Proof. Let $x \in D$ be a point such that $\mathcal{O}_{X,x}$ is regular. First notice that x is a closed point of X, since D has codimension 1 in the 1-dimensional scheme X. Let P be the closed set $\{x\} \subseteq X$ with the reduced subscheme structure. Since $\mathcal{O}_{X,x}$ is Noetherian and regular of dimension 1, its maximal ideal $\mathfrak{m}_x$ is generated by a regular element. Since P is exactly the closed set of X corresponding to $\mathfrak{m}_x$, this shows that P is an effective Cartier divisor. Suppose towards a contradiction that s vanishes in P. Then $P \subseteq D \cap \mathcal{Z}(s)$, so Theorem 3.11 implies that $D-P$ is effective and admits non-constant sections. Therefore,

$$\operatorname{dgon} X \leq \deg(D-P) = \deg D - \deg P < \deg D$$

since $P \neq \emptyset$.

For the second statement, first suppose that s does not vanish on any point of D. Notice that 1_D vanishes only on the points of D. Therefore, for any point $x \in X$ at least one of s and 1_D does not vanish, and by Lemma 1.28 this is the same as saying that s and 1_D generate $\mathcal{O}_X(D)$. Since D admits a non-constant global section, we certainly have $\mathcal{O}_X(D) \ncong \mathcal{O}_X$. Therefore by Theorem 2.12

$$\operatorname{gon} X \leq \deg \mathcal{O}_X(D) = \deg D.$$

For the general case, let $E_1 = \mathcal{Z}(s) \cap D$. Then E_1 is a closed zero-dimensional subscheme of X, and X is regular at all points of E_1. Therefore, by a similar argument as in the first part of the proof, E_1 is an effective Cartier divisor on X. Applying Theorem 3.11 gives us a unique non-constant element $t_1 \in H^0(X, \mathcal{O}_X(D - E_1))$ mapping to s. Now we let $E_2 = \mathcal{Z}(t_1) \cap (D - E_1)$, and repeat the argument to get a non-constant element $t_2 \in H^0(X, \mathcal{O}_X(D - E_1 - E_2))$ mapping to t_1. Repeating this inductively, we get a sequence (E_k) of effective Cartier divisors of X such that for every n the Cartier divisor $D - \sum_{k=1}^{n} E_k$ is effective. Looking at the degrees, we see that this is only possible if there is an N such that $E_k = \emptyset$ for $k \geq N$. Let $D' = D - \sum_{k=1}^{N} E_k$. Then D' is effective, and the non-constant global section t_N of $\mathcal{O}_X(D')$ does not vanish on any point of D'. Hence we are in the previous situation, and we have

$$\operatorname{gon} X \leq \deg D' \leq \deg D \qquad \square$$

Corollary 3.13. *Let X be a curve over a field. If X is regular then* $\operatorname{gon} X = \operatorname{dgon} X$.

Proof. Suppose $D \subseteq X$ is an effective Cartier divisor of degree $\operatorname{dgon} X$ admitting non-constant sections. By Corollary 3.12.2 and the regularity of X, we have

$$\operatorname{gon} X \leq \deg D = \operatorname{dgon} X.$$

For the other inequality, write $X = \bigsqcup_{i \in I} X_i$ as a disjoint union of its connected components. From the definition of gonality and divisor gonality, it easily follows that $\operatorname{gon} X = \min\{\operatorname{gon} X_i : i \in I\}$ and $\operatorname{dgon} X = \min\{\operatorname{dgon} X_i : i \in I\}$. So we can assume that X is connected. But each X_i is connected and regular, and therefore integral. Therefore $\# \operatorname{Ass}(X_i) = 1$ for each i, and so Theorem 3.9 applies. This gives us $\operatorname{gon} X_i \geq \operatorname{dgon} X_i$ for each $i \in I$, and finally that $\operatorname{gon} X = \operatorname{dgon} X$. □

3.3 Reduction

In this section, let R be a discrete valuation ring, $S = \operatorname{Spec} R$, η the generic point of S and s the closed point of S. Write $K = \kappa(\eta)$ for the field of fractions of R and $k = \kappa(s)$ for the residue field of R.

Definition 3.14. A morphism $X \to S$ is called *cohomologically flat* if the canonical homomorphism $H^0(X, \mathcal{O}_X) \otimes_R k \to H^0(X_s, \mathcal{O}_{X_s})$ is an isomorphism.

The following is Corollary 9.1.24 in [Liu02].

Theorem 3.15. *Let X be a regular integral curve over S. Let $\Gamma_1, \ldots, \Gamma_r$ be the irreducible components of X_s, with multiplicities $d_1, \ldots, d_r$. Assume that* $\gcd(d_1, \ldots, d_r) = 1$ *and that $\kappa(s)$ is perfect. Then $X \to S$ is cohomologically flat.* □

The goal of this section is to prove the following theorem.

Theorem 3.16. *Let X be a regular curve over S. Assume that X is cohomologically flat over S. Then*

$$\operatorname{dgon} X_\eta \geq \operatorname{dgon} X_s.$$

The strategy is as follows. We start with an effective Cartier divisor D' in the generic fiber X_η of X of minimal degree such that it admits non-constant sections. Then we take the closure D of D' in X, and then the intersection D_s of D with the special fiber X_s. We then show that, under the assumptions on X, D_s is an effective Cartier divisor on X_s of the same degree as D', and that D_s admits non-constant sections.

We break up the proof in a few lemmas. We will use the following proposition, which is a special case of [Sta17, Lemma 30.15.9].

Proposition 3.17. *Let X be a regular Noetherian scheme, and $D \subseteq X$ a closed subscheme. If D has no embedded components and every irreducible component of D has codimension 1 in X, then D is an effective Cartier divisor.* □

Lemma 3.18. *Let X be a regular curve over S. Let $D' \subseteq X_\eta$ be an effective Cartier divisor of the generic fiber, and let D be the closure of D' in X. Then D is an effective Cartier divisor of X, and D is flat over S.*

Proof. We use Proposition 3.17 to show that D is an effective Cartier divisor. First we note that every generic point of D is an element of the generic fiber X_η, since every point in D is a specialisation of a point in $D' \subseteq X_\eta$. Let $\xi \in D$ be a generic point of D. Then $\xi \in D'$, and so it has codimension 1 in X_η. The map $X_\eta \to X$ is an open immersion, since X_η is exactly the open subscheme of X where any fixed uniformizer of R does not vanish. Therefore the canonical map of local rings $\mathcal{O}_{X,\xi} \to \mathcal{O}_{X_\eta,\xi}$ is an isomorphism. Since the codimension of a point is exactly the Krull dimension of the corresponding local ring (see [Sta17, Lemma 27.10.3]), it follows that the codimension of ξ in X is also 1.

To show that D has no embedded points, we note that the restriction map $\mathcal{O}_D \to \mathcal{O}_{D'}$ is injective, since D' is dense in D by definition. Moreover, we have $\operatorname{Ass}(D) = \operatorname{Ass}_{\mathcal{O}_X}(\mathcal{O}_D)$, the set of point of X associated to the $\mathcal{O}_X$-module $\mathcal{O}_D$, and similarly for D'. Hence, [Sta17, Lemma 30.2.4] gives us $\operatorname{Ass}(D) = \operatorname{Ass}_{\mathcal{O}_X}(\mathcal{O}_D) \subseteq \operatorname{Ass}_{\mathcal{O}_X}(\mathcal{O}_{D'}) = \operatorname{Ass}(D')$. Since D' has no embedded points, it follows that D does not either. So by the above proposition, D is an effective Cartier divisor.

To show that D is flat over S, we can work locally. We reduce to the case that $X = \operatorname{Spec} A$ for an R-algebra A. Let $A_K = A \otimes_R K$. Then D' corresponds to some ideal $J \subseteq A_K$, and D corresponds to $I = J \cap A$. Now notice that the map $A/I \to A_K/J$ is injective, by definition of I. Since A_K/J is a K-algebra, it follows that A/I is torsion-free over R. But then A/I is flat over R since R is a discrete valuation ring, which is what we wanted to show. □

Lemma 3.19. *Let X be a regular curve over S. Let $D \subseteq X$ be an effective Cartier divisor which is flat over S. Then D_s is an effective Cartier divisor of X_s.*

Proof. This is a local question, so we reduce to commutative algebra. Let $X = \operatorname{Spec} A$, where A is a flat R-algebra, and let $D = \operatorname{Spec} A/fA$ for some regular element $f \in A$. The assumption that D is flat over S translates to saying that A/I is torsion-free over R. Let $A_k = A \otimes_R k$. The reduction D_s corresponds to the ideal $I \otimes k$ of A_k. This is clearly generated by the element $f \otimes 1$ of A_k. Thus, it is enough to show that $f \otimes 1$ is regular in A_k.

For this, suppose that $f \otimes 1$ is a zero-divisor (or zero) in A_k. Let $t \in R$ be a uniformizer. The map $A \to A_k$ is surjective with kernel tA, so by the assumption on $f \otimes 1$ there is an $a \in A \setminus tA$ such that $af \in tA$. Let $b \in A$ be such that $af = tb$. Since A/fA is torsion-free over R and $tb \in fA$, it follows that $b \in fA$. Write $b = cf$ for an element $c \in A$. Then we have $af = tcf$. Since f is regular in A, this implies $a = tc \in tA$, contradicting our choice of a. □

We can now prove the theorem.

Proof of Theorem 3.16. Let D' be a gonal divisor of X_η. Let D be the closure of D' in X. Notice that $D_\eta = D'$. By Lemma 3.18, D is an effective Cartier divisor on X and flat over S. By Lemma 3.19, D_s is an effective Cartier divisor on X_s. Now we use Proposition 2.11 and Theorem 2.12 to obtain

$$\deg_k D_s = \deg_k \mathcal{O}_{X_s}(D_s) = \deg_K \mathcal{O}_{X_\eta}(D_\eta) = \deg_K D_\eta = \deg_K D' = \operatorname{dgon} X_\eta.$$

By the upper semi-continuity of cohomology (see [Liu02, Theorem 5.3.20(a)]), we have

$$\dim_k H^0(X_s, \mathcal{O}_{X_s}(D_s)) \geq \dim_K H^0(X_\eta, \mathcal{O}_{X_\eta}(D_\eta)).$$

Since X is cohomologically flat over S, we have

$$\dim_k H^0(X_s, \mathcal{O}_{X_s}) = \dim_K H^0(X_\eta, \mathcal{O}_{X_\eta}).$$

Since D_η admits non-constant sections, this together with Lemma 3.5 gives the the inequalities

$$\dim_k H^0(X_s, \mathcal{O}_{X_s}) = \dim_K H^0(X_\eta, \mathcal{O}_{X_\eta}) < \dim_K H^0(X_\eta, \mathcal{O}_{X_\eta}(D_\eta)) \leq \dim_k H^0(X_s, \mathcal{O}_{X_s}(D_s)),$$

which shows that D_s also admits non-constant sections. So finally we have

$$\operatorname{dgon} X_s \leq \deg D_s = \operatorname{dgon} X_\eta. \qquad \square$$

Corollary 3.20. *Let X be a regular curve over S. Suppose that k is perfect and that X_s is reduced (or more generally, that X is cohomologically flat over S). Then*

$$\operatorname{gon} X_\eta \geq \operatorname{dgon} X_s.$$

If X_s is regular, we even have

$$\operatorname{gon} X_\eta \geq \operatorname{gon} X_s$$

Proof. Let $X = \bigsqcup_{i \in I} X_i$ be the decomposition of X into connected components. Then each X_i is a regular integral curve over S. We have $\operatorname{gon} X_\eta = \min_{i \in I} \operatorname{gon}(X_i)_\eta$ and similarly $\operatorname{gon} X_s = \min_{i \in I} \operatorname{dgon}(X_i)_s$. So it is enough to show the corollary for each component. Therefore, we may assume that X is integral.

From Theorem 3.15 it follows that $X \to S$ is cohomologically flat. Therefore, Theorem 3.16 applies, and shows that $\operatorname{dgon} X_\eta \geq \operatorname{dgon} X_s$. Since K is the field of fractions of a discrete valuation ring, K is infinite (all subrings of a finite field are fields). So Theorem 3.9 applies, and gives us $\operatorname{gon} X_\eta \geq \operatorname{dgon} X_\eta$, and therefore

$$\operatorname{gon} X_\eta \geq \operatorname{dgon} X_\eta \geq \operatorname{dgon} X_s.$$

If X_s is also regular then from Corollary 3.13 we obtain that $\operatorname{gon} X_s \leq \operatorname{dgon} X_s$, and therefore $\operatorname{gon} X_\eta \geq \operatorname{gon} X_s$. □

3.4 Partial normalizations

In section 2 of this chapter, we saw that we could remove common zeros for the sections s and 1_D of $\mathcal{O}_X(D)$ on a curve X over k, provided that those zeros are regular points of X. In this chapter we will consider what can be done if this assumption is not satisfied. The idea is to normalize X partially at those points where s and 1_D have common zeros, and then apply the results from section 2.

In this section, we let X be a geometrically reduced curve over a field k. We write X^{sing} for the subset of singular points of X, i.e. those $x \in X$ such that the local ring $\mathcal{O}_{X,x}$ is not regular. Notice that the points of X^{sing} are all closed points, since the assumption that X is geometrically reduced implies that $\mathcal{O}_{X,\eta}$ is a field for every generic point η of X. Since X is of finite type over a field, X^{sing} is also closed (see [Sta17, Lemma 28.18.3.1]), so that X^{sing} is finite.

Definition 3.21. For any subset $T \subseteq X^{\text{sing}}$ we denote by $\pi_T \colon X_T \to X$ the *partial normalization* of X at the points of T, i.e. the curve fitting in a triangle

$$\begin{tikzcd}
X' \arrow[d] \arrow[dr] & \\
X_T \arrow[r, "\pi_T"'] & X
\end{tikzcd}$$

where $X' \to X$ is the normalization morphism of X, such that $X_T \to X$ is an isomorphism away from T, and $X' \to X_T$ is an isomorphism away from (the inverse image of) $X^{\text{sing}} \setminus T$.

Notice that for $T = X^{\text{sing}}$, X_T is the normalization of X, while for $T = \emptyset$ we have $X_T = X$.

Lemma 3.22. *Let $x \in X^{\text{sing}}$ be a singular point, and let $T \subseteq X^{\text{sing}}$ with $x \in T$. Then the fiber $(X_T)_x \subseteq X_T$ over x is an effective Cartier divisor of X_T. Moreover, the degree of $(X_T)_x$ does not depend on the choice of T (as long as $x \in T$).*

Proof. Let $D = (X_T)_x$ as a closed subscheme of X_T. Let $y \in D$ be a point. We claim that X_T is regular in y. Indeed, the map $X' \to X_T$ is an isomorphism away from the inverse image of $X^{\text{sing}} \setminus T$, so in particular it is an isomorphism away from y. Since X' is regular, it follows that X_T is regular in an open neighbourhood of y, and in particular X_T is regular in y.

Therefore $\mathcal{O}_{X_T,y}$ is a discrete valuation ring, so any non-zero ideal of $\mathcal{O}_{X_T,y}$ is generated by a regular element. In particular the ideal $\mathcal{I}(D)_y$ of $\mathcal{O}_{X_T,y}$ (which is non-zero, since D has codimension 1) is generated by a regular element of $\mathcal{O}_{X_T,y}$. Therefore D is an effective Cartier divisor on X_T.

To show that the degree of D does not depend on T, let $S = X^{\text{sing}}$. Then the map $X_S \to X_T$ is an isomorphism in an open neighbourhood of $D = (X_T)_x$, and so $\deg D = \deg (X_S)_x$, independent of our choice of T. □

Definition 3.23. For each $x \in X^{\text{sing}}$ we define the *multiplicity* of x in X to be the number

$$m(x) = \deg_k (X_T)_x$$

for any $T \subseteq X^{\text{sing}}$ with $x \in T$.

We have the following easy lower bound for $m(x)$.

Lemma 3.24. *Let $x \in X^{\text{sing}}$, and $T \subseteq X^{\text{sing}}$ with $x \in T$. Then*

$$m(x) \geq \sum_{\substack{y \in X_T \\ \pi_T(y) = x}} [\kappa(y) : k].$$

Proof. Let $D = (X_T)_x$. Then for any $y \in X_T$ we have $y \in D$ if and only if $\pi_T(y) = x$, since D is the fiber of X_T over x. Moreover, we have

$$\mathcal{O}_D = \bigoplus_{y \in D} \mathcal{O}_{D,y}.$$

Each of these local rings is a non-zero vector space over $\kappa(y)$, and has therefore at least dimension $[\kappa(y) : k]$ over k. Thus

$$\deg D = \sum_{\substack{y \in X_T \\ \pi_T(y)=x}} \dim_k \mathcal{O}_{D,y} \geq \sum_{\substack{y \in X_T \\ \pi_T(y)=x}} [\kappa(y) : k]. \qquad \square$$

Lemma 3.25. *Let D be an effective Cartier divisor on X and $T \subseteq X^{\text{sing}}$. Let $D_T = \pi_T^{-1} D$. Then D_T is an effective Cartier divisor on X_T, and there is a unique isomorphism of $\mathcal{O}_{X_T}$-modules $\pi_T^* \mathcal{O}_X(D) \to \mathcal{O}_{X_T}(D_T)$ mapping $\pi_T^* 1_D$ to 1_{D_T}.*

Proof. We want to apply Theorem 1.25, so we check the conditions. First we notice that π_T is a finite morphism, because is it quasi-finite and projective. In particular, π_T is affine. Moreover, X and X_T are reduced, so the only associated points of X_T and X are generic points of the irreducible components. It is clear that the map $X_T \to X$ sends generic points to generic points, since it is finite. Hence, we have $\pi_T(\operatorname{Ass} X_T) \subseteq \operatorname{Ass} X$ (in fact, equality holds). Hence the theorem applies, and the statement follows. □

Lemma 3.26. *Let D be an effective Cartier divisor on X and $T \subseteq X^{\text{sing}}$. Let $D_T = \pi_T^{-1} D$. Then $\deg_k D_T = \deg_k D$.*

Proof. It is enough to show the statement for $T = X^{\text{sing}}$, since then for any other subset $S \subseteq X^{\text{sing}}$, we have $\deg D_T = \deg D$ and $\deg D_T = \deg D_S$. If $T = X^{\text{sing}}$ then X_T is just the normalization of X. Then from [Liu02], Corollary 7.5.8 we have $\deg \mathcal{O}_X(D) = \deg \pi_T^* \mathcal{O}_X(D)$. By Lemma 3.25 we have $\pi_T^* \mathcal{O}_X(D) = \mathcal{O}_{X_T}(D_T)$. Thus, using Theorem 2.12 we have

$$\deg D = \deg \mathcal{O}_X(D) = \deg \mathcal{O}_{X_T}(D_T) = \deg D_T. \qquad \square$$

The following is the main result of this section.

Theorem 3.27. *We have*

$$\operatorname{dgon} X \geq \min_{T \subseteq X^{\text{sing}}} \begin{cases} \operatorname{gon} X_T + \sum_{x \in T} m(x) & \text{if } H^0(X, \mathcal{O}_X) \to H^0(X_T, \mathcal{O}_{X_T}) \text{ is an isomorphism.} \\ \sum_{x \in T} m(x) & \text{else.} \end{cases}$$

Proof. Let $D \subseteq X$ be a gonal effective Cartier divisor, and $s \in H^0(X, \mathcal{O}_X(D))$ a non-constant section. Let $Z = \mathcal{Z}(s) \cap D$ as a closed subscheme of X. By Corollary 3.12, s does not vanish at points of D where X is regular. Hence, every point of Z is a singular point of X. Let $T = |Z|$ be the set underlying the scheme Z. As before, we write $D_T = \pi_T^{-1}(D)$ and $Z_T = \pi_T^{-1}(Z)$. Let $s_T \in H^0(X_T, \mathcal{O}_{X_T}(D_T))$ be the global section corresponding to $\pi_T^* s$ under the canonical isomorphism $\pi_T^* \mathcal{O}_X(D) \to \mathcal{O}_{X_T}(D_T)$.

Notice that Z_T is a zero-dimensional subscheme of X_T, and that there is an open neighbourhood U of Z_T such that U is regular and 1-dimensional (specifically, one may take $U = X_T \setminus \pi_T^{-1}(X^{\text{sing}} \setminus T)$). Therefore, Z_T is an effective Cartier divisor of X_T. Since $Z \subseteq D$ (as closed subschemes of X), we also have $Z_T \subseteq D_T$. Since $Z \subseteq \mathcal{Z}(s)$, we have $Z_T \subseteq \pi_T^{-1}(\mathcal{Z}(s)) = \mathcal{Z}(s_T)$, where we use Lemma 1.24 for the last step. So we find that $Z_T \subseteq D_T \cap \mathcal{Z}(s_T)$.

This means that Theorem 3.11 applies. This tells us that $E := D_T - Z_T$ is effective, and that there is a unique $t \in H^0(X_T, \mathcal{O}_{X_T}(E))$ that maps to s_T in $H^0(X_T, \mathcal{O}_{X_T}(D_T))$, and that t is non-constant if and only if s_T is. Since $D_T - Z_T$ is effective, it follows that $\deg D_T \geq \deg Z_T$.

Suppose that $H^0(X, \mathcal{O}_X) \to H^0(X_T, \mathcal{O}_{X_T})$ is an isomorphism. We consider the commutative square

$$\begin{tikzcd}
H^0(X, \mathcal{O}_X) \arrow[r, "\sim"] \arrow[d] & H^0(X_T, \mathcal{O}_{X_T}) \arrow[d] \\
H^0(X, \mathcal{O}_X(D)) \arrow[r] & H^0(X_T, \mathcal{O}_{X_T}(D_T))
\end{tikzcd}$$

Notice that all arrows are injective and that the lower arrow maps s to s_T. Since s is not constant, it follows that s_T is also not constant. Hence, by Theorem 3.11, this shows that t is also not constant. Furthermore, we have

$$|\mathcal{Z}(t) \cap E| \subseteq |\mathcal{Z}(s_T) \cap D_T| \subseteq \pi_T^{-1}(T).$$

Therefore, all points $x \in E$ such that t vanishes in x are regular points of X_T. So by Corollary 3.12.2, we have in this case

$$\operatorname{gon} X_T \leq \deg E = \deg D_T - \deg Z_T.$$

So far, we have now proved that

$$\deg D_T \geq \begin{cases} \operatorname{gon} X_T + \deg Z_T & \text{if } H^0(X, \mathcal{O}_X) \to H^0(X_T, \mathcal{O}_{X_T}) \text{ is an isomorphism.} \\ \deg Z_T & \text{else.} \end{cases}$$

By Lemma 3.25, we have $\deg_k D_T = \deg D = \operatorname{dgon} X$. We want to obtain an estimate for $\deg Z_T$. For any $x \in T$, the fiber $(X_T)_x \subseteq Z_T$ over x is an effective Cartier divisor on X_T of degree $m(x)$ by Lemma 3.25. For $x, y \in Z$ with $x \neq y$ the sets $\pi_T^{-1}(x)$ and $\pi_T^{-1}(y)$ are disjoint. Hence, we have

$$\sum_{x \in T} (X_T)_x \subseteq Z_T$$

as effective Cartier divisors. Taking degrees, this shows that

$$\deg Z_T \geq \sum_{x \in T} m(x),$$

and that finishes the proof. □

We can combine the results of this section with the results of the previous section to get a statement about gonality and reduction that does not refer to divisor gonality.

Corollary 3.28. *Let $S = \{\eta, s\}$ be the spectrum of a local ring R with field of fractions $K = \kappa(\eta)$ and residue field $k = \kappa(s)$. Let X be a regular curve over S, and assume that k is perfect and that the special fiber X_s is reduced. Then*

$$\operatorname{gon} X_\eta \geq \min_{T \subseteq (X_s)^{\text{sing}}} \begin{cases} \operatorname{gon} X_T + \sum_{x \in T} m(x) & \textit{if } H^0(X, \mathcal{O}_X) \to H^0(X_T, \mathcal{O}_{X_T}) \textit{ is an isomorphism.} \\ \sum_{x \in T} m(x) & \textit{else.} \end{cases}$$

Proof. By Corollary 3.20 we have $\operatorname{gon} X_\eta \geq \operatorname{dgon} X_s$. Since X_s is reduced over the perfect field k, X_s is geometrically reduced over k. Therefore, Theorem 3.27 applies and gives the desired result. □

Chapter 4

Applications

In this chapter we give some applications of the theorems on reduction and partial normalization in the previous chapter. In the first section, we look at modular curves called $X(2,2n)_{\mathbb{Q}}$. These curves are mentioned in [DS17], where the authors state that their main result (which is a classification of all groups occurring infinitely often as the torsion group of an elliptic curve over number fields of fixed degree d for $d=5$ and $d=6$) could be extended to $d=7$ if the gonality of the curves $X(2,2n)_{\mathbb{Q}}$ for $n=11,12,13,14,15$ could be shown to be at least 8. Below we will obtain lower bound on the gonality of $X(2,2n)_{\mathbb{Q}}$ for odd n. In the second section, we look at the curves $X_0(p)_{\mathbb{Q}}/W_p$ for primes $p \geq 5$. We obtain an algorithm that computes a lower bound of the gonality over $\mathbb{Q}$ of these curves, using the reduction at $\mathbb{F}_p$. In both cases, we will obtain the lower bounds without using explicit equations for the curves involved, instead relying on the modular interpretation of these curve modulo some prime.

4.1 The gonality of $X(2,2n)$ over $\mathbb{Q}$ for n odd

In this section, we consider the gonality of the curves $X(2,2n)_{\mathbb{Q}}$ for odd n (which we will define in Definition 4.6 below). The goal is to give a good lower bound for $\operatorname{gon} X(2,2n)_{\mathbb{Q}}$. To do this we study the reduction $X(2,2n)_{\mathbb{F}_2}$, and apply Corollary 3.28 to get the desired lower bound.

We start with some background on elliptic curves.

Definition 4.1. Let $(E,\mathcal{O})$ be an elliptic curve over a scheme S. The 2-*torsion* of E is the subscheme $E[2]$ of E that is the kernel of the multiplication-by-2 group scheme morphism $[2]: E \to E$.

Definition 4.2. Let $(E,\mathcal{O})$ be an elliptic curve over a scheme S. A *Drinfeld basis for the* 2-*torsion* (or *full level 2 structure*) for E is a group homomorphism

$$\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](S)$$

such that

$$E[2] = \sum_{a \in (\mathbb{Z}/2\mathbb{Z})^2} [\varphi(a)]$$

as effective Cartier divisors on E. Here $[\varphi(a)]$ denotes the Cartier divisor defined by $\varphi(a)\colon S \to E$, see [KM85, Lemma 1.2.2].

Definition 4.3. For an elliptic curve E over an $\mathbb{F}_p$-scheme S, we denote by $F_E : E \to E^{(p)}$ the Frobenius morphism. It is an isogeny of degree p. The dual isogeny $V_E : E^{(p)} \to E$ is called the *Verschiebung*.

Lemma 4.4. *Let $(E, \mathcal{O})$ be an elliptic curve over a scheme S over $\mathbb{F}_2$. Then there is a unique S-point $Q_E \in E^{(2)}(S)$ such that* $\ker V_E = [\mathcal{O}] + [Q_E]$ *as effective Cartier divisors on $E^{(2)}$. For this point we have an equality $E^{(2)}[2] = 2[\mathcal{O}] + 2[Q_E]$ as effective Cartier divisors on $E^{(2)}$.*

Proof. There is a short exact sequence of group schemes

$$0 \to \ker(F_E) \to E[2] \to \ker(V_E) \to 0,$$

since $[2] = V_E \circ F_E$ and since F_E is surjective. Because V_E is an isogeny of degree 2, its kernel has degree 2 as Cartier divisor on $E^{(2)}$ (in the sense that for every $s \in S$, we have $\deg(\ker V_E)_s = 2$ as Cartier divisor on the curve E_s over $\kappa(s)$). Since we clearly have $\mathcal{O} \subseteq \ker V_E$, we see that $\ker V_E - \mathcal{O}$ is effective of degree 1, and therefore corresponds to a section $Q_E \in E^{(2)}(S)$. Then $\ker V_E = [\mathcal{O}] + [Q_E]$ by construction. Unicity of Q_E is clear. Finally we have $\ker F_E = 2[\mathcal{O}]$ and therefore

$$E^{(2)}[2] = \ker(F_E \circ V_E) = V_E^{-1}(2[\mathcal{O}]) = 2[\mathcal{O}] + 2[Q_E]. \qquad \square$$

If the point Q_E in the above proposition coincides with $\mathcal{O}$, we say that E is supersingular, otherwise we say that E is ordinary. Notice that E/S is supersingular if and only if $E_s/\kappa(s)$ is supersingular for every $s \in S$.

Proposition 4.5. *Let $(E, \mathcal{O})$ be an elliptic curve over an $\mathbb{F}_2$-scheme S, and let $Q_E \in E^{(2)}(S)$ be as above. Then there are three Drinfeld bases for the 2-torsion on $E^{(2)}$, given by*

1. $(\mathbb{Z}/2\mathbb{Z})^2 \to E^{(2)}[2]$ *given by* $(a, b) \mapsto a\mathcal{O} + bQ_E$.
2. $(\mathbb{Z}/2\mathbb{Z})^2 \to E^{(2)}[2]$ *given by* $(a, b) \mapsto aQ_E + b\mathcal{O}$.
3. $(\mathbb{Z}/2\mathbb{Z})^2 \to E^{(2)}[2]$ *given by* $(a, b) \mapsto aQ_E + bQ_E$.

These are identical if E is supersingular, otherwise they are pairwise distinct.

Proof. This follows immediately from Lemma 4.4. □

Definition 4.6. Let $n \geq 5$ be odd. The modular curve $Y(2, 2n)_{\mathbb{Z}[1/n]}$ over $\mathbb{Z}[1/n]$ is defined by the following universal property. For every $\mathbb{Z}[1/n]$-scheme S, we consider triples (E, Q, φ), where E is an elliptic curve over S, $Q \in E(S)$ is a point of exact order n, and $\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](S)$ is a Drinfeld basis for the 2-torsion of E. We consider two such triples (E, Q, φ) and (E', Q', φ') equivalent if there is an S-isomorphism $f : E \xrightarrow{\sim} E$ such that $f(Q) = Q'$ and $f \circ \varphi = \varphi'$. Then there is bijection, natural in S, between $Y(2, 2n)_{\mathbb{Z}[1/n]}(S)$ and the set of such triples up to equivalence.

The modular curve $X(2, 2n)_{\mathbb{Z}[1/n]}$ is defined to be the compactification of $Y(2, 2n)_{\mathbb{Z}[1/n]}$ (see [KM85, Section 8.6.3] for the details of this construction).

Remark 4.7. Let E/S be an elliptic curve, and assume for simplicity that $2n$ is invertible in S. Then choosing a Drinfeld basis for the 2-torsion of E is the same as picking two independent points $P_1, P_2 \in E[2](S)$. If $Q \in E[n](S)$ is a point of exact order n, then $Q + P_2$ is a point of order $2n$ (since n is odd), and independent of P_1. On the other hand, if we start with a point P_1 of exact order 2 and a point R of exact order $2n$ that is independent of P_1, then $2R$ has exact order n and P_1, nR forms a Drinfeld basis for E. So we see that the moduli problem of $X(2, 2n)$ can also be formulated as asking for a point of exact order 2 and an independent point of order $2n$ (at least over $\mathbb{Z}[1/2n]$, but with some care the argument extends to $\mathbb{Z}[1/n]$), which explains the name of $X(2, 2n)$.

Proposition 4.8. *Let $n \geq 5$ be odd. The modular curve $X(2, 2n)_{\mathbb{Z}[1/n]}$ is a regular curve over $\mathbb{Z}[1/n]$ (in the sense of Definition 2.1).*

Proof. That $Y(2,2n)_{\mathbb{Z}[1/n]}$ is regular and flat of relative dimension 1 over $\mathbb{Z}[1/n]$ follows essentially from [KM85, Theorem 5.1.1], since our moduli problem is the product of the moduli problems $[\Gamma(2)]$ and $[\Gamma_1(n)]$, and the second is rigid (since $n \geq 5$) and finite etale over $(\mathrm{Ell}/\mathbb{Z}[1/n])$. Then $X(2,2n)_{\mathbb{Z}[1/n]}$ is by construction projective over $\mathbb{Z}[1/n]$, and since it is regular at the cusps, it is also regular and flat over $\mathbb{Z}[1/n]$. □

We want to study $X(2,2n)_{\mathbb{F}_2}$. In order to do so, we start by describing the geometric picture. Let $\overline{\mathbb{F}}_2$ be an algebraic closure of $\mathbb{F}_2$. Recall that $X_1(n)$ is the compactified modular curve that parametrizes elliptic curves together with points of exact order n.

Proposition 4.9 (Description of $X(2,2n)_{\overline{\mathbb{F}}_2}$)**.** *Let $n \geq 5$ be odd. The curve $X(2,2n)_{\overline{\mathbb{F}}_2}$ over $\overline{\mathbb{F}}_2$ consists of three copies of $X_1(n)^{(2)}_{\overline{\mathbb{F}}_2}$ glued in the supersingular points. More precisely:*

1. *There are canonical morphisms $\epsilon_i : X_1(n)^{(2)}_{\overline{\mathbb{F}}_2} \to X(2,2n)_{\overline{\mathbb{F}}_2}$ with $i = 1,2,3$, and an action of S_3 on $X(2,2n)_{\overline{\mathbb{F}}_2}$ such that $\epsilon_{\sigma(i)} = \sigma \circ \epsilon_i$ for all $i \in \{1,2,3\}$ and all $\sigma \in S_3$.*
2. *The irreducible components of $X(2,2n)_{\overline{\mathbb{F}}_2}$ are exactly the images of the ϵ_i.*
3. *These components cross transversely in the closed points of $X(2,2n)_{\overline{\mathbb{F}}_2}$ corresponding to supersingular elliptic curves. The tangent space of $X(2,2n)_{\overline{\mathbb{F}}_2}$ has dimension 2 in these supersingular points, and away from these points $X(2,2n)_{\overline{\mathbb{F}}_2}$ is regular.*
4. *$X(2,2n)_{\overline{\mathbb{F}}_2}$ is reduced.*

Proof. Most of this can be found in [KM85], in section 13.7 and other places of the book, but for completeness we will give a sketch of a proof.

The fiber $Y(2,2n)_{\overline{\mathbb{F}}_2}$ has the same moduli interpretation as $Y(2,2n)_{\mathbb{Z}[1/n]}$, but with $\mathbb{Z}[1/n]$ replaced by $\overline{\mathbb{F}}_2$. By [KM85, Proposition 8.6.8(3)], $X(2,2n)_{\overline{\mathbb{F}}_2}$ is exactly the compactification of $Y(2,2n)_{\overline{\mathbb{F}}_2}$. In particular, $X(2,2n)_{\overline{\mathbb{F}}_2}$ is regular at the cusps.

Let $E_1(n)$ be the universal elliptic curve over $Y_1(n)$ and let $P_1(n) \in E_1(n)(Y_1(n))$ be the universal point of order n. Proposition 4.5 gives us three canonical Drinfeld bases $\varphi_1, \varphi_2, \varphi_3 : (\mathbb{Z}/2\mathbb{Z})^2 \to E_1(n)^{(2)}_{\overline{\mathbb{F}}_2}[2]$. Then for $i = 1,2,3$ the triples $(E_1(n)^{(2)}_{\overline{\mathbb{F}}_2}, P_1(n)^{(2)}_{\overline{\mathbb{F}}_2}, \varphi_i)$ are as in Definition 4.6 and therefore correspond to morphisms $Y_1(n)^{(2)}_{\overline{\mathbb{F}}_2} \to Y(2,2n)_{\overline{\mathbb{F}}_2}$. By regularity, these extend to morphisms $\epsilon_i : X_1(n)^{(2)}_{\overline{\mathbb{F}}_2} \to X(2,2n)_{\overline{\mathbb{F}}_2}$. The elliptic curve $E_1(n)_{\overline{\mathbb{F}}_2}$ is not supersingular, and therefore the Drinfeld bases φ_i are pairwise distinct. This shows that the morphisms ϵ_i are also pairwise distinct.

We claim that the ϵ_i are jointly surjective. Indeed, let $x \in Y(2,2n)_{\overline{\mathbb{F}}_2}$ be given. Then to the morphism $\kappa(x) \to Y(2,2n)_{\overline{\mathbb{F}}_2}$ corresponds a triple (E, P, φ) with E an elliptic curve over $\kappa(x)$, $P \in E(\kappa(x))$ a point of exact order n, and φ a Drinfeld basis for the 2-torsion. Then the pair (E, P) corresponds to a $\kappa(x)$-point in $Y_1(n)_{\overline{\mathbb{F}}_2}(\kappa(x))$, and therefore $(E^{(2)}, P^{(2)})$ corresponds to a $\kappa(x)$-point $y \in Y_1(n)^{(2)}_{\overline{\mathbb{F}}_2}(\kappa(x))$. The Drinfeld basis φ for the 2-torsion of E induces a Drinfeld basis for the 2-torsion of $E^{(2)}$, which is then one of the Drinfeld bases in Proposition 4.5. Hence, x is the image of y under one of the three maps ϵ_i. So indeed the ϵ_i are jointly surjective.

There is a natural action of $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ on $X(2,2n)_{\overline{\mathbb{F}}_2}$ (in fact on all of $X(2,2n)$) which acts on the choice of the Drinfeld basis for the 2-torsion. Notice that this action does not affect the point of order n that we have chosen. In particular, starting from a point in $X_1(n)_{\overline{\mathbb{F}}_2}$ and applying first a ϵ_i and then an element of $\mathrm{GL}_2(\mathbb{F}_2)$ is the same as applying a possibly different ϵ_j to the same point. Hence, after choosing the correct isomorphism $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ we have $\sigma \circ \epsilon_i = \epsilon_{\sigma(i)}$ for each $i = 1, 2, 3$ and each $\sigma \in S_3$.

Suppose that we have $\epsilon_i(x) = \epsilon_j(x)$ for some $x \in X_1(n)_{\overline{\mathbb{F}}_2}$ and indices $i \neq j$. It is clear that x cannot correspond to an ordinary elliptic curve, because for an ordinary elliptic curve $E/\kappa(x)$ there are three distinct choices for the Drinfeld basis on $E^{(2)}$. Therefore x is a cusp of $X_1(n)_{\overline{\mathbb{F}}_2}$ or it corresponds to a supersingular elliptic curve. But we have already seen that $X(2, 2n)_{\overline{\mathbb{F}}_2}$ is regular at the cusps, so x is also not a cusp. Hence, x corresponds to a supersingular point. On the other hand, for any point $x \in X_1(n)_{\overline{\mathbb{F}}_2}$ corresponding to a supersingular elliptic curve we have $\epsilon_i(x) = \epsilon_j(x)$.

By Proposition 4.8 $X(2, 2n)_{\mathbb{Z}[1/n]}$ is regular of dimension 2. Since $X(2, 2n)_{\mathbb{F}_2}$ is a closed subscheme of this, all points of $X(2, 2n)_{\mathbb{F}_2}$ have tangent dimension at most 2. Therefore, also all points of $X(2, 2n)_{\overline{\mathbb{F}}_2}$ have tangent dimension at most 2. Away from the supersingular points, the maps ϵ_i are local isomorphisms to their images, and so $X(2, 2n)_{\overline{\mathbb{F}}_2}$ is regular away from the supersingular points. At the supersingular points, $X(2, 2n)_{\overline{\mathbb{F}}_2}$ is clearly not regular, since the three components meet there. Therefore, the dimension of the tangent space in those points is 2.

We now see that $X(2, 2n)_{\overline{\mathbb{F}}_2}$ is reduced everywhere except possibly at the supersingular points. To show that $X(2, 2n)_{\overline{\mathbb{F}}_2}$ is reduced at these points as well and that the components cross transversely is done by explicitly calculating the complete local ring at these points, see [KM85, Theorem 13.8.4]. □

We can calculate the number of supersingular points as follows.

Proposition 4.10. *Let $n \geq 5$ be odd. Let r be the number of supersingular points of $X(2, 2n)_{\overline{\mathbb{F}}_2}$. Then*

$$r = \frac{n^2}{24} \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$$

Proof. By the description above we see that r is also the number of supersingular points on $X_1(n)_{\overline{\mathbb{F}}_2}$. There is a unique supersingular elliptic curve over $\overline{\mathbb{F}}_2$, which has 24 automorphisms over $\overline{\mathbb{F}}_2$. Since n is coprime with the characteristic and $\overline{\mathbb{F}}_2$ is algebraically closed, we have

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

The automorphism group of E acts freely on $E[n]$ since $n \geq 5$ (see [KM85, Theorem 2.7.3]). Therefore r equals the number of elements of order n in $(\mathbb{Z}/n\mathbb{Z})^2$, divided by 24.

Let $f(m)$ denote the number of order m elements of $(\mathbb{Z}/m\mathbb{Z})^2$ for all m. Then $f(ab) = f(a)f(b)$ for a, b coprime by the Chinese Remainder Theorem. If $m = p^k$, then $f(p^k) = p^{2k} - p^{2k-2} = p^{2k}(1 - 1/p^2)$. Therefore, we see that

$$f(n) = \prod_{p|n} p^{2\,\mathrm{ord}_n(p)}(1 - \frac{1}{p^2}) = n^2 \prod_{p|n}(1 - \frac{1}{p^2}). \qquad \square$$

Applying the reduction theorem to $X(2, 2n)_{\mathbb{Q}}$ enables us to relate its gonality to the gonality over $\mathbb{F}_2$. This leads to the following statement.

Proposition 4.11. *Let $n \geq 5$ be odd, and write $X_0 = X(2, 2n)_{\mathbb{F}_2}$ and $X = X(2, 2n)_{\overline{\mathbb{F}}_2}$. Let $\pi : X \to X_0$ be the canonical morphism. Let r denote the number of supersingular points on X. We have*

$$\operatorname{gon} X(2, 2n)_{\mathbb{Q}} \geq \min\big(3r, \min_{T_0 \subsetneq X_0^{\mathrm{sing}}} (\operatorname{gon}(X_0)_{T_0} + 3|\pi^{-1}(T_0)|\,)\big),$$

where $(X_0)_{T_0}$ denotes the partial normalization over X_0 at T_0.

Proof. We apply Corollary 3.20 to $X(2,2n)_{\mathbb{Z}_{(2)}}$. This is a regular curve over $\mathbb{Z}_{(2)}$ by Proposition 4.8. By Proposition 4.9, $X(2,2n)_{\overline{\mathbb{F}}_2}$ is reduced, so $X(2,2n)_{\mathbb{F}_2}$ is reduced as well. Finally, $\mathbb{F}_2$ is a perfect field. So we may apply Corollary 3.20, and find that

$$\operatorname{gon} X(2,2n)_{\mathbb{Q}} \geq \operatorname{dgon} X(2,2n)_{\mathbb{F}_2}.$$

We want to apply Theorem 3.27 to get a lower bound for $\operatorname{dgon} X_0$. We can do this because X_0 is reduced over $\mathbb{F}_2$, and therefore geometrically reduced. From the description of X in Proposition 4.9 it follows that the partial normalization $(X_0)_{T_0}$ is connected if and only T_0 is not all of X_0^{sing}. Therefore, the map $H^0(X_0, \mathcal{O}_{X_0}) \to H^0((X_0)_{T_0}, \mathcal{O}_{(X_0)_{T_0}})$ is an isomorphism if and only if T_0 is a strict subset of X_0^{sing}. We notice that over every $x \in X^{\text{sing}}$ there are three points in the normalization of X. Therefore, we have $m(x) \geq 3$ for each x. Thus the statement now follows from Theorem 3.27. □

Our goal is to obtain explicit lower bounds for the gonality of $X(2,2n)$ over $\mathbb{Q}$. To this end, we must study the gonality of the curves occurring as the partial normalizations of $X(2,2n)_{\overline{\mathbb{F}}_2}$. To make the exposition more clear, we state the result in the following general way.

Theorem 4.12. *Let $X_0/\mathbb{F}_2$ be a curve, $C_0/\mathbb{F}_2$ a regular integral curve. Let $\epsilon_{0,i} : C_0 \to X_0$ be morphisms for $i = 1,2,3$. Let $X = X_0 \times_{\mathbb{F}_2} \overline{\mathbb{F}}_2$, $C = C_0 \times_{\mathbb{F}_2} \overline{\mathbb{F}}_2$, and $\epsilon_i : C \to X$ be the base change of $\epsilon_{0,i}$ to $\overline{\mathbb{F}}_2$ for $i = 1,2,3$. Let $r \geq 0$ be an integer. Assume that the following holds true.*

1. *For each $i \in \{1,2,3\}$ the morphism $\epsilon_i : C \to X$ is injective, and the induced morphism $C \sqcup C \sqcup C \to X$ is the normalization of X.*
2. *There is an action of S_3 on X such that $\sigma \circ \epsilon_i = \epsilon_{\sigma(i)}$ for all $\sigma \in S_3$ and all $i \in \{1,2,3\}$.*
3. *There are r points $c_1, \ldots, c_r \in C(\overline{\mathbb{F}}_2)$ such that $\epsilon_1(c_k) = \epsilon_2(c_k) = \epsilon_3(c_k)$ for each $k \in \{1, \ldots, r\}$.*
4. *The components of X meet transversely in the r points $x_k := \epsilon_1(c_k)$, $k = 1 \ldots r$, and the tangent space in these points has dimension 2.*
5. *X is reduced.*

Then

$$\operatorname{gon} X_0 \geq \min(\frac{3}{2}r, 1 + r + 2\operatorname{gon} C_0 - \operatorname{genus} C_0, 4\operatorname{gon} C_0).$$

Proof. For brevity we will write $\mathbb{P}^1$ and $\mathbb{A}^1$ for $\mathbb{P}^1_{\overline{\mathbb{F}}_2}$ and $\mathbb{A}^1_{\overline{\mathbb{F}}_2}$. Let $\mathcal{L}_0$ be a non-trivial 2-generated invertible sheaf on X_0 of degree d, and assume that $d < 3r/2$. We will show that $d \geq 1 + r + 2\operatorname{gon} C_0 - \operatorname{genus} C_0$ or $d \geq 4\operatorname{gon} C_0$.

Let $\mathcal{L}$ be the base change of $\mathcal{L}_0$ to X (i.e. $\mathcal{L}$ is the pull-back of $\mathcal{L}_0$ along the canonical morphism $X \to X_0$). Let $s_0, t_0 \in \mathcal{L}_0(X_0)$ be generators for $\mathcal{L}_0$, and s and t the pull-backs of s_0 and t_0 to $\mathcal{L}$. Then to $\mathcal{L}$ and the generators s and t corresponds a morphism $f : X \to \mathbb{P}^1$. Notice that this morphism is exactly the base change of the morphism $X_0 \to \mathbb{P}^1_{\mathbb{F}_2}$ defined by the generators s_0 and t_0 of $\mathcal{L}_0$.

Define $\mathcal{L}_i = \epsilon_i^* \mathcal{L}_i$, $s_i = \epsilon_i^* s$ and $t_i = \epsilon_i^* t$ for $i = 1,2,3$. Then $\mathcal{L}_i$ is an invertible sheaf on C generated by s_i and t_i. Let f_i be the morphism $C \to \mathbb{P}^1$ defined by s_i and t_i. Then one sees from the construction of these maps that $f_i = f \circ \epsilon_i$, and that f_i is the base change of the morphism $C_0 \to \mathbb{P}^1_{\overline{\mathbb{F}}_2}$ defined by the pull-backs of s_0 and t_0. In particular, if f_i is not constant, then $\deg f_i \geq \operatorname{gon} C_0$ by Proposition 3.2.

By [Liu02, Proposition 7.5.7], we have $\deg \mathcal{L} = \deg \mathcal{L}_1 + \deg \mathcal{L}_2 + \deg \mathcal{L}_3$. Since $\deg f_i = \deg \mathcal{L}_i$ for each i by Theorem 2.14, this shows that

$$\deg f_1 + \deg f_2 + \deg f_3 = d. \tag{4.1}$$

Since X has only finitely many singular points, we may assume after applying an automorphism of $\mathbb{P}^1$ that the singular points of X do not map to the point $\infty = (1 : 0)$ of $\mathbb{P}^1$.

Since $\epsilon_i(c_k) = x_k$ for each i, we have $f_i(c_k) = f(\epsilon_i(x_k)) = f(\epsilon_j(x_k)) = f_j(c_k)$ for all indices $1 \leq i, j \leq 3$, $1 \leq k \leq r$. Since $f(x_k) \neq \infty$ for each k, this shows that

$$f_1(c_k) = f_2(c_k) = f_3(c_k) \neq \infty \tag{4.2}$$

for each k.

We identify $\mathbb{P}^1 \setminus \{(1 : 0)\} \cong \mathbb{A}^1$. Let

$$U = f_1^{-1}(\mathbb{A}^1) \cap f_2^{-1}(\mathbb{A}^1) \cap f_3^{-1}(\mathbb{A}^1)$$

be the open subset of C on which f_1, f_2 and f_3 do not have poles. By the previous paragraph, we have $c_k \in U$ for each k. We may consider the f_i as elements of $\Gamma(U, \mathcal{O}_C)$. In particular, their germ $f_{i,c_k} \in \mathcal{O}_{C,c_k}$ is well-defined for each k.

Claim 4.13. Fix $k \in \{1, \ldots, r\}$, and let $a_k = f(x_k)$ (considered as an element of $\overline{\mathbb{F}}_2$). We have

$$(f_{1,c_k} - a_k) + (f_{2,c_k} - a_k) + (f_{3,c_k} - a_k) \in \mathfrak{m}_{c_k}^2.$$

Proof of the claim. Consider the map

$$\Phi : \mathfrak{m}_{x_k}/\mathfrak{m}_{x_k}^2 \longrightarrow \left(\mathfrak{m}_{c_k}/\mathfrak{m}_{c_k}^2\right)^3, \qquad g \mapsto ((g \circ \epsilon_1)_{c_k}, (g \circ \epsilon_2)_{c_k}, (g \circ \epsilon_3)_{c_k}).$$

Clearly Φ is an $\overline{\mathbb{F}}_2$-linear map. The map Φ is injective since the images of the ϵ_i cross transversely in x_k. The domain of Φ has dimension 2 over $\overline{\mathbb{F}}_2$ by assumption, while the codomain has dimension 3 since C is regular.

We see that the image of Φ is a 2-dimensional subspace of a 3-dimensional vector space. Therefore, there are constants $a, b, c \in \overline{\mathbb{F}}_2$, not all zero, such that

$$a(g \circ \epsilon_1)_{c_k} + b(g \circ \epsilon_2)_{c_k} + c(g \circ \epsilon_3)_{c_k} \equiv 0 \mod \mathfrak{m}_{c_k}^2$$

holds for all $g \in \mathfrak{m}_x$. Now consider the action of S_3 on X. By assumption 2 it commutes with the morphisms ϵ_i, which shows that Φ is S_3-equivariant (where we equip $(\mathfrak{m}_{c_k}/\mathfrak{m}_{c_k}^2)^3$ with the natural S_3-action). In particular it follows that the image of Φ is S_3-invariant. This is only possible if $a = b = c$. Since not all of a, b and c are zero, we may take $a = b = c = 1$. Since $f - a_k \in \mathfrak{m}_{x_k}$, it follows that

$$(f_{1,c_k} - a_k) + (f_{2,c_k} - a_k) + (f_{3,c_k} - a_k) \equiv 0 \mod \mathfrak{m}_{c_k}^2 \qquad \square$$

Claim 4.14. None of the maps f_1, f_2 and f_3 are constant.

Proof of the claim. Since f is not constant, it is clear that not all three of the f_i can be constant. Assume that f_3 is constant. Without loss of generality f_3 takes on the value 0. If f_1 and f_2 are both non-constant, then they have both at least r zeroes (since they are zero in each c_k). Then they both have degree at least r, which is not possible because $\deg f_1 + \deg f_2 + \deg f_3 < 3r/2$. On the other hand, if f_2 is also constant, then f_1 has double roots in each c_k by Claim 4.13. Then we have $\deg f_1 \geq 2r$, which also contradicts $\deg f_1 + \deg f_2 + \deg f_3 < 3r/2$. □

After reassigning labels, we may assume that $\deg f_1 \geq \deg f_2 \geq \deg f_3$. Since none of the f_i are constant, they all have degree at least $\operatorname{gon} C_0$.

Claim 4.15. If $f_1 : C \to \mathbb{P}^1$ is not separable, then $d \geq 4 \operatorname{gon} C_0$.

Proof of the claim. We can write f_1 as the composition of a non-constant separable morphism $C \to \mathbb{P}^1$ and a purely inseparable morphism $\mathbb{P}^1 \to \mathbb{P}^1$. The latter has degree at least 2, the former has degree at least $\operatorname{gon} C_0$. Therefore $\deg f_1 \geq 2 \operatorname{gon} C_0$. Since $\deg f_2$ and $\deg f_3$ are also at least $\operatorname{gon} C_0$, the statement follows. □

In the rest of the proof we can assume that f_1 is separable.

Claim 4.16. We have $\deg f_2 + \deg f_3 \leq r - 1$.

Proof of the claim. Suppose that $\deg f_2 + \deg f_3 \geq r$. Then $\deg f_2 \geq r/2$ since $\deg f_2 \geq \deg f_3$. But since $\deg f_1 \geq \deg f_2$ it then follows that

$$\deg f_1 + \deg f_2 + \deg f_3 \geq r/2 + r = 3r/2 > d,$$

contradiction. □

Claim 4.17. We have $f_2 = f_3$.

Proof of the claim. Consider the function $g = f_2 - f_3$ as element of the function field of C. It induces a morphism $C \to \mathbb{P}^1$, since C is regular, and by slight abuse of notation we also denote this morphism by g. Counting the poles of g, we see that $\deg g \leq \deg f_2 + \deg f_3$ (because g cannot have more poles than f_2 and f_3 together, counting multiplicities). Therefore we have $\deg g \leq r - 1$. On the other hand, we have $g(x_k) = f_2(x_k) - f_3(x_k) = 0$ for each x_k, where we have used that f_2 and f_3 do not have poles in the x_k. Thus g is a function of degree at most $r - 1$ with r roots, and therefore $g = 0$. □

Claim 4.18. f_1 ramifies in each point c_k.

Proof of the claim. Fix k, and let $a_k = f_1(x_k)$ as before. By Claim 4.13, we have

$$(f_{1,c_k} - a_k) + (f_{2,c_k} - a_k) + (f_{3,c_k} - a_k) \in \mathfrak{m}_{c_k}^2.$$

By Claim 4.17 we have $f_2 = f_3$. Since we are working in characteristic 2, this gives

$$f_{1,c_k} - a_k \in \mathfrak{m}_{c_k}^2,$$

which exactly tells us that f_1 ramifies in c_k. □

We finish the proof by applying the Hurwitz formula (see [Har77, Corollary IV.2.4]). We already know that f_1 is finite by Claim 4.14, and we have assumed that f_1 is separable, so the Hurwitz formula applies.

Let R be the ramification divisor of f_1. Notice that at each point e_k, f_1 either has ramification degree 2, in which case the ramification is wild, or f_1 has ramification degree more than 2. In both cases, the contribution of e_k to the degree of R is at least 2. Hence, we have $\deg R \geq 2r$

(see [Har77], Proposition IV.2.2 and the text around it). Now we fill in the Hurwitz formula for f_1, this gives us

$$2 \cdot \mathrm{genus}(C) - 2 = \deg f_1 \cdot (0-2) + \deg R.$$

Rewriting and using that $\mathrm{genus}\, C = \mathrm{genus}\, C_0$ gives

$$\deg f_1 = \frac{1}{2} \deg R + 1 - \mathrm{genus}\, C_0 \geq r + 1 - \mathrm{genus}\, C_0.$$

Together with the fact that f_2 and f_3 have degree at least $\mathrm{gon}\, C_0$, this gives us

$$d = \deg f_1 + \deg f_2 + \deg f_3 \geq r + 1 + 2\,\mathrm{gon}\, C_0 - \mathrm{genus}\, C_0. \qquad \square$$

Corollary 4.19. *Let $n \geq 5$ be odd. Let r be the number of supersingular points of $X_1(n)_{\overline{\mathbb{F}}_2}$. Then*

$$\mathrm{gon}\,(X(2,2n)_{\mathbb{Q}}) \geq \min\left(\frac{3r}{2}, r + 1 + 2\,\mathrm{gon}\, X_1(n)_{\mathbb{F}_2} - \mathrm{genus}\, X_1(n)_{\mathbb{F}_2}, 4\,\mathrm{gon}\, X_1(n)_{\mathbb{F}_2}\right)$$

Proof. Let $X_0 = X(2,2n)_{\mathbb{F}_2}$ and $X = X(2,2n)_{\overline{\mathbb{F}}_2}$. Let $\pi : X \to X_0$ be the canonical map. In view of Proposition 4.11 we need to show that the above expression is a lower bound for $3r$ and for the quantity $\mathrm{gon}\,(X_0)_{T_0} + 3 \cdot |\pi^{-1}(T_0)|$ for each strict subset $T_0 \subsetneq X_0^{\mathrm{sing}}$.

From Theorem 4.12 it follows that the above minimum is a lower bound for $\mathrm{gon}\, X_0$. If $T_0 \subsetneq X_0^{\mathrm{sing}}$ and $T_0 \neq \emptyset$, then the lower bound on $\mathrm{gon}\, X_T$ in Theorem 4.12 is at worst $\frac{3}{2}|\pi^{-1}(T)| + 1$ less than this minimum, so that the quantity $\mathrm{gon}\, X_T + 3|T|$ is never lower than the above minimum. Also, we have $3r \geq 3r/2$. The statement now follows from Proposition 4.11. $\square$

We can make the formula a bit more explicit.

Corollary 4.20. *Let $n \geq 5$ be odd. Then*

$$\mathrm{gon}\, X(2,2n)_{\mathbb{Q}} \geq \min\left(\frac{n^2}{16}\prod_{p|n}\left(1 - \frac{1}{p^2}\right), 2\,\mathrm{gon}\, X_1(n)_{\mathbb{F}_2} + \frac{1}{4}\sum_{d|n}\varphi(d)\varphi(\frac{n}{d}), 4\,\mathrm{gon}\, X_1(n)_{\mathbb{F}_2}\right).$$

Here φ denotes the Euler phi function $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. The value for r is given above in Proposition 4.10, and equals

$$r = \frac{n^2}{24}\prod_{p|n}\left(1 - \frac{1}{p^2}\right).$$

The genus of $X_1(n)$ is calculated in [KK96] to be

$$\mathrm{genus}(X_1(n)) = 1 + \frac{n^2}{24}\prod_{p|n}\left(1 - \frac{1}{p^2}\right) - \frac{1}{4}\sum_{d|n}\varphi(d)\varphi(\frac{n}{d}). \qquad \square$$

We can find the value of the gonality of $X_1(n)$ over $\mathbb{F}_2$ for odd n with $5 \leq n \leq 39$ in [DvH14]. The authors compute the gonality of $X_1(n)$ over $\mathbb{Q}$, but state in remark 1 that the gonality of $X_1(n)_{\mathbb{Q}}$ for $n \leq 39$ coincides with the gonality of $X_1(n)_{\mathbb{F}_p}$ for p the smallest prime not dividing n. In particular, for $5 \leq n \leq 39$ odd this gives us the value of the gonality of $X_1(n)$ over $\mathbb{F}_2$. This leads to the following table, which shows the gonality of $X_1(n)$ over $\mathbb{F}_2$ (obtained from [DvH14]), and the lower bound for the gonality of $X(2,2n)$ over $\mathbb{Q}$ that Corollary 4.20 gives us.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
$\operatorname{gon} X_1(n)_{\mathbb{F}_2} =$	1	1	1	2	2	2	4	5	4	7	5	6	11	12	10	12	18	14
$\operatorname{gon} X(2,2n)_{\mathbb{Q}} \geq$	2	3	4	8	8	8	16	19	16	25	20	24	36	39	40	48	54	52

These lower bounds have implications for the existence of elliptic curves.

Corollary 4.21. *Let $\Phi^\infty(d)$ denote the set of all pairs (m, mn) such that $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/mn\mathbb{Z})$ occurs infinitely often (up to $\overline{\mathbb{Q}}$-isomorphism) as the torsion subgroup of an elliptic curve over a number field of degree d. Then*

1. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 11, 13, 15$ and $d < 8$.*
2. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 25$ and $d < 10$.*
3. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 27$ and $d < 12$.*
4. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 23$ and $d < 13$.*
5. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 17, 21$ and $d < 16$.*
6. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 29$ and $d < 18$.*
7. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 19$ and $d < 19$.*
8. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 31, 33$ and $d < 20$.*
9. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 35$ and $d < 24$.*
10. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 39$ and $d < 26$.*
11. *$(2, 2n) \notin \Phi^\infty(d)$ for $n = 37$ and $d < 27$.*

Proof. [DS17] proves that if $(2, 2n) \in \Phi^\infty(d)$ then $\operatorname{gon} X_1(2,2n)_{\mathbb{Q}} \leq 2d$, and if moreover the Jacobian of $X_1(2,2n)_{\mathbb{Q}}$ has rank 0, then we even have $\operatorname{gon} X_1(2,2n)_{\mathbb{Q}} \leq d$. Theorem 4.1 of [DS17] states that this latter criterion is fulfilled for all $n \leq 21$. Therefore, our result follows from the above table of lower bounds for $\operatorname{gon} X_1(2,2n)_{\mathbb{Q}}$. □

4.2 The gonality of $X_0(p)/W_p$ over $\mathbb{Q}$

Let $p \geq 5$ be prime. We investigate the gonality of $X_0(p)/W_p$ over $\mathbb{Q}$, by reducing it over $\mathbb{F}_p$.

Definition 4.22. The modular curve $Y_0(p)$ is defined by the following universal property. Let S be a scheme. We consider the contravariant functor $\mathcal{F}$ from the category of schemes to the category of sets that assigns to any scheme S the set of equivalence classes of triples (E, E', π) where E and E' are elliptic curves over S and $\pi\colon E \to E'$ is an isogeny of degree p. Two such triples (E_1, E_1', π_1) and (E_2, E_2', π_2) are equivalent if there are isomorphisms $\varphi\colon E_1 \xrightarrow{\sim} E_2$, $\varphi'\colon E_1' \to E_2'$ such that $\varphi' \circ \pi_1 = \pi_2 \circ \varphi$. Then there is a morphism from the functor $\mathcal{F}$ to the functor $\operatorname{Hom}_{\mathrm{Schemes}}(-, Y_0(p))$, universal for morphisms from $\mathcal{F}$ to representable functors.

We let $X_0(p)$ be the compactification of $Y_0(p)$ (see [KM85, Section 8.6.3] for the details of this construction).

The morphism $\mathcal{F} \to \mathrm{Hom}(-, Y_0(p))$ above is not an isomorphism. However, we have the following.

Lemma 4.23. *Let k be an algebraically closed field. Then the morphism $\mathcal{F}(k) \to Y_0(p)(k)$ induced by the functor morphism $\mathcal{F} \to \mathrm{Hom}(-, Y_0(p))$ is an isomorphism.*

Proof. [KM85, Lemma 8.1.3.1] □

Remark 4.24. The equivalence class of a triple (E, E', π) like above is uniquely determined by the kernel of π. Conversely, if $G \subseteq E[p]$ is a finite flat subgroup scheme which is a Cartier divisor of degree p, then the morphism $\pi : E \to E/G$ is an isogeny of degree p. Hence $Y_0(p)$ also corresponds to the moduli problem of degree p effective Cartier divisors on E, finite flat over S, that are subgroup schemes of E.

For an elliptic curve E over an $\mathbb{F}_p$-scheme S the Frobenius morphism $F_E : E \to E^{(p)}$ is an isogeny of degree p. Its dual $V_E : E^{(p)} \to E$ is called the *Verschiebung* morphism of $E^{(p)}$, and is also an isogeny of degree p. The following states that up to equivalence these are the only isogenies of degree p that occur.

Lemma 4.25. *Let E_1, E_2 be ordinary elliptic curves over a connected $\mathbb{F}_p$-scheme S, and $\pi : E_1 \to E_2$ an isogeny of degree p. Then one of the following possibilities occurs:*

1. *there is an isomorphism $\varphi : E_1^{(p)} \xrightarrow{\sim} E_2$ such that $\pi = \varphi \circ F_{E_1}$, or*
2. *there is an isomorphism $\varphi : E_1 \xrightarrow{\sim} E_2^{(p)}$ such that $\pi = V_{E_2} \circ \varphi$.*

Proof. This is a special case of [KM85, Theorem 13.3.3]. □

By considering the degree p subgroups of E, one sees that the Frobenius and Verschiebung morphisms are equivalent degree p isogenies if and only if E is supersingular.

This allows us to understand the geometric structure of $X_0(p)_{\mathbb{F}_p}$.

Proposition 4.26. *The geometric fiber $X_0(p)_{\overline{\mathbb{F}}_p}$ consists of two projective lines, glued in the certain supersingular points. More precisely:*

1. *There are canonical morphisms $\epsilon_i : \mathbb{P}^1_{\overline{\mathbb{F}}_p} \to X_0(p)_{\overline{\mathbb{F}}_p}$ for $i = 1, 2$.*
2. *The irreducible components of $X_0(p)_{\overline{\mathbb{F}}_p}$ are exactly the images of the ϵ_i.*
3. *These components cross in the points corresponding to supersingular elliptic curves over p. For every supersingular j-invariant in $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$ we have $\epsilon_1(j) = \epsilon_2(j^p)$. The completed local rings at these points are of the form $\overline{\mathbb{F}}_p[[x, y]]/(xy)$ and away from these points $X_0(p)_{\overline{\mathbb{F}}_p}$ is regular.*
4. *$X_0(p)_{\overline{\mathbb{F}}_p}$ is reduced.*

Proof. The argument is similar to the proof of Proposition 4.9, so we only sketch the broad lines. The maps ϵ_i for $i = 1, 2$ come from interpreting $\mathbb{P}^1$ as the compactified coarse moduli space of elliptic curves. Then the $\epsilon_i : \mathbb{P}^1_{\overline{\mathbb{F}}_p} \to X_0(p)_{\overline{\mathbb{F}}_p}$ come from considering, for any elliptic curve, either the Frobenius isogeny or the Verschiebung isogeny, which are up to equivalence the only choices for a degree p isogeny by Lemma 4.25. There is an action of $S_2 = \{\pm 1\}$ on $X_0(p)$ that interchanges a triple $(E, E^{(p)}, F_E)$ with $(E^{(p)}, E, V_E)$ and vice versa. Since the j-invariant of $E^{(p)}$ is exactly the p-th power of the j-invariant of E, it follows that $\epsilon_1(j) = \epsilon_2(j^p)$ for all supersingular j-invariants. All other considerations are as in the proof of Proposition 4.9, and can be found in more detail in [KM85, Section 13.4] and in [DR73, Théorème 6.9(ii)]. □

As it happens, the curve $X_0(p)$ is not always regular, and therefore we cannot apply the reduction theorems from the previous chapter. However, we will see that its quotient $X_0(p)/W_p$ is regular and flat over $\mathbb{Z}$.

Definition 4.27. We let W_p denote the Atkin-Lehner involution on $X_0(p)$ corresponding to interchanging triples (E, E', π) and (E', E, π^t), where π^t denotes the dual isogeny of π. More formally, interchanging these triples induces an automorphism α of the functor $\mathcal{F}$ in Definition 4.22. The composition $\mathcal{F} \to \mathcal{F} \to Y_0(p)$ induces a unique morphism $Y_0(p) \to Y_0(p)$ by the universal property of $Y_0(p)$, which in turn extends to a unique morphism $W_p : X_0(p) \to X_0(p)$. Since α is its own inverse, the same must be true for W_p.

Proposition 4.28. *The curve $X_0(p)/W_p$ is a regular curve over $\mathbb{Z}$.*

Proof. [DR73, Théorème 6.9] tells us that $X_0(p)$ is smooth over $\mathbb{Z}$ away from the supersingular points mod p. In these supersingular points, the completed local ring is isomorphic to $\mathbb{Z}_p[[u,v]]/(uv - p^e)$, where $e = 3$ for the elliptic curve with $j = 0$ (if it is supersingular mod p) and $e = 2$ for the elliptic curve with $j = 1728$ (if it is supersingular mod p), and $e = 1$ in all other supersingular points. Notice that the supersingular points with $e = 1$ are already regular, so we only need to worry about the two other points. Let x be such a supersingular point. Then the corresponding j-invariant is rational (namely 0 or 1728) and therefore fixed under the Frobenius morphism. Therefore, x is fixed under the action of W_p. The action of W_p in these points swaps the two branches at x, as can be seen from the description of the branches in Proposition 4.26 above. After possibly rescaling u or v we can therefore assume W_p acts on $\mathbb{Z}_p[[u,v]]/(uv - p^e)$ by interchanging u and v. The completed local ring of the image of x in the quotient is just the subring of fixed points of $\mathbb{Z}_p[[u,v]]/(uv - p^e)$ under this action. The map $\mathbb{Z}_p[[t]] \to \mathbb{Z}_p[[u,v]]/(uv - p^e)$ sending t to $u + v$ induces an isomorphism between $\mathbb{Z}_p[[t]]$ and the fixed subring of $\mathbb{Z}_p[[u,v]]/(uv - p^e)$. Hence, the completed local ring of the image of x in $X_0(p)/W_p$ is regular. □

Proposition 4.29. *The curve $(X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$ is obtained from $\mathbb{P}^1$ by gluing each supersingular j-invariant in $\mathbb{P}^1$ to its conjugate j^p. More precisely, there is a canonical morphism $\nu : \mathbb{P}^1_{\overline{\mathbb{F}}_p} \to (X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$ such that*

1. *$\nu(j) = \nu(j^p)$ for each $j \in \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ corresponding to a supersingular elliptic curve over $\overline{\mathbb{F}}_p$,*
2. *ν is an isomorphism away from the points of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$ corresponding to supersingular elliptic curves,*
3. *ν is surjective.*

The singularities of $(X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$ are nodal, and $(X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$ is reduced.

Proof. The action of W_p interchanges $(E, E^{(p)}, F_E)$ with $(E^{(p)}, E, V_{E^{(p)}})$ and vice versa. From the description of $X_0(p)_{\overline{\mathbb{F}}_p}$ in Proposition 4.26, we can view $X_0(p)_{\overline{\mathbb{F}}_p}$ as the gluing of two copies of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$, one corresponding to the Frobenius isogeny and the other to the Verschiebung isogeny. We see that W_p maps any j in the copy corresponding to the Frobenius isogeny to j^p in the other copy, and vice versa. Therefore, the composition

$$\nu : \mathbb{P}^1_{\overline{\mathbb{F}}_p} \xrightarrow{\epsilon_1} X_0(p)_{\overline{\mathbb{F}}_p} \longrightarrow (X_0(p)/W_p)_{\overline{\mathbb{F}}_p},$$

where the first arrow ϵ_i corresponds to the map $E \mapsto (E, E^{(p)}, F_E)$, is surjective, and an isomorphism on the open set corresponding to all ordinary elliptic curves. If j is a supersingular j-invariant, then $X_0(p)_{\overline{\mathbb{F}}_p}$ has a nodal singularity at the image of j. If j is $\mathbb{F}_p$-rational, then W_p

sends j to itself but interchanges the components, and we see that the quotient is regular in that point. If j is not $\mathbb{F}_p$-rational, then j is in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$, and the nodal crossing at j gets glued to the nodal crossing at j^p. Hence, the singularities of $X_0(p)_{\overline{\mathbb{F}}_p}/W_p$ occur exactly at the supersingular j-invariants that lie in $\mathbb{P}^1(\mathbb{F}_{p^2}) \setminus \mathbb{P}^1(\mathbb{F}_p)$, and they are nodal. □

Theorem 4.30. *Let $X = (X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$. We have*

$$\operatorname{gon}(X_0(p)/W_p)_{\mathbb{Q}} \geq \min_{T \subseteq X^{\text{sing}}} \big(\operatorname{gon} X_T + 2|T|\big).$$

Proof. The curve $(X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$ is integral, hence its quotient $(X_0(p)/W_p)_{\mathbb{F}_p}$ is integral as well. Therefore all of its partial normalizations are also integral. From Corollary 3.28 it follows that

$$\operatorname{gon}(X_0(p)/W_p)_{\mathbb{Q}} \geq \min_T \big(\operatorname{gon}((X_0(p)/W_p)_{\mathbb{F}_p})_T + \sum_{x \in T} m(x)\big),$$

where T runs over all subsets of $((X_0(p)/W_p)_{\overline{\mathbb{F}}_p})^{\text{sing}}$. Changing base to $\overline{\mathbb{F}}_p$ does not increase these terms, and therefore does not increase the minimum. Therefore, we have

$$\operatorname{gon}(X_0(p)/W_p)_{\mathbb{Q}} \geq \min_T \big(\operatorname{gon}((X_0(p)/W_p)_{\overline{\mathbb{F}}_p})_T + \sum_{x \in T} m(x)\big),$$

where this time T runs over the subsets of $((X_0(p)/W_p)_{\overline{\mathbb{F}}_p})^{\text{sing}}$. To end the proof, we notice that $m(x) \geq 2$ for each singular point of $((X_0(p)/W_p)_{\overline{\mathbb{F}}_p})^{\text{sing}}$ simply because there are two points above such x in the normalization $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$. □

The above theorem allows us to obtain a lower bound for the gonality of $X_0(p)/W_p$ over $\mathbb{Q}$, as soon as we have a way of calculating the gonality of each partial normalization of $(X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$. Fortunately, this last curve, and all of its partial normalizations, have a simple structure: they are obtained from $\mathbb{P}^1$ by identifying pairs of points of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$ corresponding to supersingular elliptic curves. Thus it suffices to study the gonality of such curves. To fix ideas, we make the following definition.

Definition 4.31. Let k be a field. Let $r \geq 0$ be a number, and let $x_i \in \mathbb{P}^1(k)$ and $y_i \in \mathbb{P}^1(k)$ for $i = 1, \ldots, r$ be points. We will assume that all x_i and y_i are distinct. Let X be the quotient of $\mathbb{P}^1_k$ obtained by identifying x_i with y_i for each $i \in \{1, \ldots, r\}$, in such a way that the completed local rings of X in the identified points are of the form $k[[u, v]]/(uv)$. Then we call X *the nodal curve defined by the set of pairs* $\{(x_i, y_i)\}$.

Our starting point for studying the gonality of such curves is the following observation.

Proposition 4.32. *Let k be a field, $r \geq 0$, and $x_i, y_i \in \mathbb{P}^1_k(k)$ for $i = 1, \ldots, r$ be $2r$ distinct points. Let X be the nodal curve defined by the pairs (x_i, y_i). Then the gonality of X is the lowest number $d > 0$ such that there exist a morphism $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$ with $\deg f = d$ such that $f(x_i) = f(y_i)$ for each $i \in \{1, \ldots, r\}$.*

Proof. Indeed, by the quotient property, a morphism $X \to \mathbb{P}^1_k$ is the same as a morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$ that takes the same values on each pair x_i, y_i. The result now follows from Proposition 3.2 since X is integral. □

Corollary 4.33. *Let k be a field, $r \geq 0$, and $x_i, y_i \in \mathbb{P}^1_k(k)$ for $i = 1, \ldots, r$ be $2r$ distinct points. Let X be the nodal curve defined by the pairs (x_i, y_i). Then*

$$\operatorname{gon} X \leq \max(2r, 1)$$

Proof. If $r = 0$ then $X = \mathbb{P}^1_k$, and the result is obvious. Otherwise, in Proposition 4.32, we can take a non-zero rational function that is zero in each x_i, y_i, and such that $\deg f = 2r$. $\square$

We want to turn Proposition 4.32 into a statement that is more computable.

Theorem 4.34. *Let k be an algebraically closed field, $r \geq 0$, and $x_i, y_i \in \mathbb{P}^1_k(k)$ for $i = 1, \dots, r$ be $2r$ distinct points. Let X be the nodal curve defined by the pairs (x_i, y_i). Embed $\mathbb{A}^1_k \subseteq \mathbb{P}^1_k$ in such a way that each x_i and y_i is in the image of $\mathbb{A}^1_k$, so that we can view the x_i and y_i as elements of k. Then the gonality of X over k is the lowest number $d > 0$ such that there exist elements $a_1, \dots, a_d, b_1, \dots, b_d, c \in k$ such that the polynomials*

$$g(x) = x^d + a_1 x^{d-1} + \ldots + a_d, \qquad \textit{and} \qquad h(x) = b_1 x^{d-1} + \ldots + b_d$$

satisfy the relations

$$g(x_i) \cdot h(y_i) = g(y_i) \cdot h(x_i) \textit{ for each } i \in \{1, \dots, r\} \qquad \textit{and} \qquad \mathrm{Res}(g, h) \cdot c = 1.$$

Proof. Clearly, if such polynomials g and h exist, then $f(x) = g(x)/h(x)$ is a morphism $\mathbb{P}^1 \to \mathbb{P}^1$ of degree exactly d (since $\mathrm{Res}(g, h) \neq 0$, so g and h are coprime), and it satisfies $f(x_i) = f(y_i)$ for each i. So by Proposition 4.32, we then have $\operatorname{gon} X \leq d$.

For the other direction, let $d = \operatorname{gon} X$. Let f be a degree d morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$ such that $f(x_i) = f(y_i)$ for each i, which exists by Proposition 4.32. After possibly replacing f with $1/(f - c)$ for some $c \in k$ (which does not change the degree of f), we can assume that $f(\infty) = \infty$ (where we write ∞ for the unique point of $\mathbb{P}^1_k \setminus \mathbb{A}^1_k$). Then we can write $f = g/h$ for coprime polynomials g and h of degree at most d, and the assumption that $f(\infty) = \infty$ guarantees that h has degree smaller than g. In particular we have $\deg h \leq d - 1$, and so $\deg g = d$ since $\deg f = d$. After multiplying g and h with the same unit, we can take g monic. Then we take the a_i and b_i to be the coefficients of g and h, and $c = 1/\mathrm{Res}(g, h)$ (which is well-defined, since g and h are coprime). $\square$

The above defines an algebraic system in $2r + 1$ variables with $r + 1$ equations. We can therefore check if it has solutions by computing a Gröbner basis for the ideal generated by the $r + 1$ equations. If the Gröbner basis for this ideal contains 1, then there are no solutions, otherwise there are solutions. This gives the following algorithm to compute the right hand side of Theorem 4.30. Let ss_p denote the monic polynomial over $\mathbb{F}_p$ whose zeros in $\overline{\mathbb{F}}_p$ are exactly the supersingular j-invariants.

```
Calculate the right hand side of Theorem 4.30.
F := [factors of $ss_p$ over $\mathbb{F}_p$ of degree 2]
S := {$(x_k, y_k)$ : $x_k$ and $y_k$ are the roots of F[k] over $\overline{\mathbb{F}}_p$ for $k$=1...r}

minimum := $2 \cdot$size(S)
for each subset U of S do:
    d := 1
    while d is less than minimum - $2 \cdot$size(S-U) do:
        R := $\overline{\mathbb{F}}_p[a_1, \dots, a_d, b_1, \dots, b_d, c]$
        $g$ := $x^d + a_1 x^{d-1} + \cdots + a_d$
        $h$ := $b_1 x^{d-1} + \cdots + b_d$
        I := ideal of R generated by the element $c \cdot \mathrm{Res}(g, h) - 1$ and
            the elements $g(x) \cdot h(y) - g(y) \cdot h(x)$ for each pair $(x, y)$ in U.
        if 1 not in I:
            minimum := d + 2·size(S-U)
        d := d + 1
return minimum
```

Here the initialisation of the variable `minimum` to `2·size(S)` is because of Corollary 4.33.

We have implemented this algorithm, and we have run it on all primes between 5 and 500. The running time of the algorithm depends heavily on the maximal degree d that occurs while running it, and this in turn depends on the number of supersingular pairs of j-invariants that are not $\mathbb{F}_p$-rational. Therefore, not all computations finish within reasonable time. However, by restricting the range of degrees d allowed in the computation, one can still find a lower bound for the expression in Theorem 4.30 and therefore for $X_0(p)/W_p$ over $\mathbb{Q}$.

The tables below give for each prime p the number of pairs of supersingular j-invariants in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ (i.e. the number of singular points of $(X_0(p)/W_p)_{\overline{\mathbb{F}}_p}$), and the lower bound for the gonality of $(X_0(p)/W_p)_{\mathbb{Q}}$ given by Theorem 4.30. For values marked with a $\geq$-symbol the computation was aborted before it finished, so these lower bounds may be strictly weaker than Theorem 4.30.

p	5	7	11	13	17	19	23	29	31	37	41	43
#Double points	0	0	0	0	0	0	0	0	0	1	0	1
Lower bound	1	1	1	1	1	1	1	1	1	2	1	2

p	47	53	59	61	67	71	73	79	83	89	97	101
#Double points	0	1	0	1	2	0	2	1	1	1	3	1
Lower bound	1	2	1	2	2	1	2	2	2	2	3	2

p	103	107	109	113	127	131	137	139	149	151	157	163
#Double points	2	2	3	3	3	1	4	3	3	3	5	6
Lower bound	2	2	3	3	3	2	3	3	3	3	4	4

p	167	173	179	181	191	193	197	199	211	223	227	229
#Double points	2	4	3	5	2	7	6	4	6	6	5	7
Lower bound	2	3	3	3	2	4	4	3	4	4	3	4

p	233	239	241	251	257	263	269	271	277	281	283	293
#Double points	7	3	7	4	7	5	6	6	10	7	9	8
Lower bound	5	3	4	3	4	4	4	4	6	4	5	5

p	307	311	313	317	331	337	347	349	353	359	367	373
#Double points	10	4	11	11	11	12	10	11	11	6	11	13
Lower bound	5	3	6	6	6	6	5	6	6	4	≥ 7	≥ 7

p	379	383	389	397	401	409	419	421	431	433	439	443
#Double points	13	8	11	15	12	13	9	15	8	15	11	14
Lower bound	6	5	6	≥ 7	6	≥ 7	≥ 6	≥ 7	5	≥ 7	≥ 7	≥ 7

p	449	457	461	463	467	479	487	491	499
#Double points	14	17	12	16	13	8	17	12	18
Lower bound	≥ 7	≥ 7	≥ 7	≥ 7	≥ 7	5	≥ 7	6	≥ 7

Bibliography

[Cap14] Lucia Caporaso. Gonality of algebraic curves and graphs. In *Algebraic and Complex Geometry*, volume 71 of *Springer Proc. Math. Stat.*, pages 77–108. Springer, Cham, 2014.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[DS17] Maarten Derickx and Andrew V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proc. Amer. Math. Soc*, 2017.

[DvH14] Maarten Derickx and Mark van Hoeij. Gonality of the modular curve $X_1(N)$. *J. Algebra*, 417:52–71, 2014.

[Eis05] David Eisenbud. *The Geometry of Syzygies*, volume 229 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2005.

[Har77] Robin Hartshorne. *Algebraic Geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[KK96] Chang Heon Kim and Ja Kyung Koo. On the genus of some modular curves of level N. *Bull. Austral. Math. Soc.*, 54(2):291–297, 1996.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*, volume 108 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1985.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[Poo07] Bjorn Poonen. Gonality of modular curves in characteristic p. *Math. Res. Lett.*, 14(4):691–701, 2007.

[Sta17] The Stacks Project Authors. *Stacks Project.* *http://stacks.math.columbia.edu, 2017.*