M. Derickx

Torsion points on elliptic curves and gonalities of modular curves

Master thesis, September 24, 2012

Primary supervisor: prof. dr. B. Edixhoven

Mathematisch Instituut, Universiteit Leiden

Contents

Abstract

This thesis consists of two related parts. In the first part the $\mathbb{Q}$-gonality of $\mathcal{X}_1(N)$ is computed for all odd $N \leq 29$ and a very good lower bound is given for $N = 31$ (see corollary 2.17). In the second part of this thesis it shown that if there is a torsion point of prime order p on an elliptic curve over a number field with degree 5 over $\mathbb{Q}$, then $p \leq 19$ or $p \in \{29, 31, 41\}$. Also all primes $p \leq 19$ occur as the order of a torsion point of some elliptic curve over a number field of degree at most 5. Table 3.2 also contains the results obtained using the same techniques for number field of degrees 6 and 7.

Preface

As already mentioned in the abstract this thesis consists of two parts. These parts can be read independently of each other. Part I is about computing gonalities of modular curves and contains a large part where some tools are developed to compute gonalities of general curves over finite fields. This part requires significantly less prerequisites then the second part and most of it should be readable without knowing what a modular curve is.

Part II which is the main part of this thesis and focuses on the question which primes can occur as the order of a point on an elliptic curve over a number field of degree at most d for $d = 5, 6, 7$. This part requires a lot more theory. And it would be unfeasible to discuss it all in detail. Instead I refer to [Diamond and Im, 1995] which I have personally found very useful in learning the prerequisites on modular forms and modular curves needed for writing this thesis. For a quick introduction without proofs one can also consult the preliminaries section of [Bosman, 2008]. The more experienced reader might also enjoy [Katz and Mazur, 1985], but I would certainly not recommend that to someone new to the subject.

I would like to thank William Stein for the inspiring talk he gave on this subject that ultimately led me to choose this as a subject for my masters thesis and allowing me to use his code for $d = 4$ as a starting point for the code I ended up writing for $d = 5, 6, 7$. I also would like to thank Mark van Hoeij, Sheldon Kamienny, Barry Mazur, Michael Stoll, Marco Streng and Andrew V. Sutherland for the interesting discussions related to the subject of this thesis. And last but not least I want to thank Bas Edixhoven for everything he taught me and the great amount of time and dedication he has for his students.

1 Definitions and notation

Let N be an integer and $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ be a subgroup then we define the congruence subgroups $\Gamma_0(N), \Gamma_1(N)$ and Γ_H as follows:

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \mod N \right\}$$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod N \right\}$$

$$\Gamma_H := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \mod N, b \mod N \in H, c = 0 \mod N \right\}$$

1.1 Modular Curves

For an arbitrary scheme S we define an elliptic curve over S to be a proper smooth group scheme E/S such that all its geometric fibers are connected curves of genus 1. Now let N be an integer and suppose that S is an $\mathbb{Z}[1/N]$-scheme then we say that a section $P \in E(S)$ has **exact order** N if $NP = 0$ and $P_k \in E_k(k)$ has order N for all geometric points k of S. Now let $\mathcal{F}_1(N)$ denote the functor $\mathcal{F}_1(N)\colon \mathrm{Sch}/_{\mathbb{Z}[1/N]} \to \mathrm{Sets}$ which sends a $\mathbb{Z}[1/N]$-scheme S to the set of all isomorphism classes of pairs (E, P) where E/S is an elliptic curve and $P \in E(S)$ has **exact order** N. We have the following important result of Igusa [see Diamond and Im, 1995, thm. 8.2.1]

Theorem 1.1. *If $N \geq 4$ then there is a scheme $\mathcal{Y}_1(N)$ which represents the functor $\mathcal{F}_1(N)$. Moreover $\mathcal{Y}_1(N)$ is smooth of relative dimension 1 over $\mathbb{Z}[1/N]$ and has geometrically connected fibres.*

By $E_1(N)_{univ}$ we will denote the elliptic curve over $\mathcal{Y}_1(N)$ corresponding to $\mathrm{Id}\colon \mathcal{Y}_1(N) \to \mathcal{Y}_1(N)$. There is also a similar functor which we will also use in this thesis. Namely the functor $\mathcal{F}_\mu(N)\colon \mathrm{Sch}/_{\mathbb{Z}[1/N]} \to \mathrm{Sets}$ which sends a $\mathbb{Z}[1/N]$-scheme S to the set of all isomorphism classes of pairs (E, i) where E/S is an elliptic curve and $i\colon \mu_{n,S} \to E$ is closed immersion (and a morphism of group schemes of course). There also exists a scheme $\mathcal{Y}_\mu(N)$ that represents the functor $\mathcal{F}_\mu(N)$. However the elliptic curve over $\mathcal{Y}_\mu(N)$ corresponding to the morphism W_N is not isomorphic to the elliptic curve $E_\mu(N)_{univ}$ corresponding to $\mathrm{Id}\colon \mathcal{Y}_\mu(N) \to \mathcal{Y}_\mu(N)$. However they are isogenous because the curve coresponding to W_N is isomorphic to $E_\mu(N)_{univ}/\mu_N\mathcal{Y}_\mu(N)$. Now $\mathcal{Y}_\mu(N)$ and $\mathcal{Y}_1(N)$ are not proper over $\mathbb{Z}[1/N]$, but they are open subschemes of proper $\mathbb{Z}[1/N]$-schemes $\mathcal{X}_\mu(N)$ and $\mathcal{X}_1(N)$. If $N \geq 5$ these schemes $\mathcal{X}_\mu(N)$ and $\mathcal{X}_1(N)$ also have a moduli interpretation in terms of so-called generalized elliptic curves [see Diamond and Im, 1995, Chap. 9].

Let d be an integer coprime to N then there are the automorphisms $\langle d\rangle\colon \mathcal{X}_1(N) \to \mathcal{X}_1(N)$ and $\langle d\rangle\colon \mathcal{X}_\mu(N) \to \mathcal{X}_\mu(N)$. The first one sends the pair (E, P) to (E, dP) and in the second case it sends (E, i) to $(E, [d] \circ i)$ where $[d]\colon E \to E$ denotes multiplication by d. These automorphisms $\langle d\rangle$ are called the diamond operators. Now the diamond operators give group actions of $(\mathbb{Z}/N\mathbb{Z})^*$ on both $\mathcal{X}_1(N)$ and $\mathcal{X}_\mu(N)$. This action actually factors trough $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ since multiplication with -1 gives an isomorphism between the pairs (E, P) and $(E, -P)$ and (E, i) to $(E, [-1] \circ i)$. This allows us to make the following definition.

Definition 1.2. Suppose $H \subset (\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ is a subgroup then we define $\mathcal{X}_H := \mathcal{X}_\mu(N)/H$ and we define $X_0(N) := X_{(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}}$.

In this thesis we will use $J_1(N), J_\mu(N), J_H$ and $J_0(N)$ as shorthand notation for the Jacobians of the curves $\mathcal{X}_1(N), \mathcal{X}_\mu(N), \mathcal{X}_H$ and $\mathcal{X}_0(N)$.

1.2 Katz modular forms

In this section we take $N \geq 5$ so that $\mathcal{X}_1(N)$ and $\mathcal{X}_\mu(N)$ have a moduli interpretation. The pullback of $\Omega^1_{E_\mu(N)_{univ}/\mathcal{X}_\mu(N)}$ along the morphism $0\colon \mathcal{X}_\mu(N) \to E_\mu(N)_{univ}$ will be denoted by $\omega_\mu(N)$. It is an invertible sheaf on $\mathcal{X}_\mu(N)$. For all $\mathbb{Z}[1/N]$-algebras A and any integer k we can consider the invertible sheaf $\omega_\mu(N)_A^{\otimes k}$ on $\mathcal{X}_\mu(N)_A$. A global section of this sheaf is called a Katz modular form of weight k with coefficients in A and we will use the notation

$$M_k(\Gamma_1(N), A) := H^0(\mathcal{X}_\mu(N)_A, \omega_\mu(N)_A^{\otimes k})$$

for the space of Katz modular forms. Viewing $\mathcal{X}_\mu(N)(\mathbb{C})$ as $\mathbb{H}^*/\Gamma_1(N)$ we can identify $M_k(\Gamma_1(N), \mathbb{C})$ with the usual modular forms. Let *cusps* be the divisor of all cusps on $\mathcal{X}_\mu(N)$ (with multiplicity 1) then we define the space of all cuspforms of weight k to be

$$S_k(\Gamma_1(N), A) := H^0(\mathcal{X}_\mu(N)_A, \omega_\mu(N)_A^{\otimes k}(-cusps)).$$

Cuspforms of weight 2

The Kodaira-Spencer isomorphism

$$\omega_\mu(N)^{\otimes 2}(-cusps) \to \Omega^1_{\mathcal{X}_\mu(N)}$$

allows us to identify

$$S_2(\Gamma_1(N), A) := H^0(\mathcal{X}_\mu(N)_A, \omega_\mu(N)_A^{\otimes k}(-cusps)) \cong H^0(\mathcal{X}_\mu(N)_A, \Omega^1_{\mathcal{X}_\mu(N)_A/A}).$$

This allows us to define S_2 also for other congruence subgroups. Namely suppose that $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ and A is a $\mathbb{Z}[1/N]$ algebra then we define

$$S_2(\Gamma_H, A) := H^0(\mathcal{X}_{H,A}, \Omega^1_{\mathcal{X}_{H,A}/A}).$$

It is not necessarily true that $S_2(\Gamma_H, A) \cong S_2(\Gamma_1(N), A)^H$. Now $S_2(\Gamma_1(N), A)^H$ is the definition of the space of Katz Modular forms that can be found in the literature. So we will not call the just defined space S_2 the space of Katz Modular forms. It is however the correct notion needed later on in this thesis because with this definition of S_2 we have

$$S_2(\Gamma_H, A) := H^0(\mathcal{X}_{H,A}, \Omega^1) \cong H^0(J_{H,A}, \Omega^1) \cong \cot_0 J_{H,A}. \tag{1.2.1}$$

By viewing $\mathcal{X}_H(\mathbb{C})$ as $\mathbb{H}^*/\Gamma_H$ we again can identify $S_2(\Gamma_H, \mathbb{C})$ with the usual modular forms. By $T_1, T_2, \ldots$ we denote the usual Hecke operators. These act on $S_2(\Gamma_H, \mathbb{C})$ and we let $\mathbb{T}_{\Gamma_H} \subset \operatorname{End} S_2(\Gamma_H, \mathbb{C})$ denote the $\mathbb{Z}$-algebra generated by $T_1, T_2, \ldots$ and $\mathbb{T}_{\Gamma_0(N)}$ and $\mathbb{T}_{\Gamma_1(N)}$ are defined similarly. If H is clear from the context I will also sometimes just write $\mathbb{T}$. Over the complex numbers there is the isomorphism

$$J_H(\mathbb{C}) \cong H^0(X_H(\mathbb{C}), \Omega^1)^\vee / H_1(X_H(\mathbb{C}), \mathbb{Z}).$$

Precomposition gives an action of $\mathbb{T}$ on $S_2(\Gamma_H, C)^\vee := H^0(X_H(\mathbb{C}), \Omega^1)^\vee$ and this action induces an action of $\mathbb{T}$ on $J_H(\mathbb{C})$, this action is actually defined over $\mathbb{Z}[1/N]$ [see Diamond and Im, 1995, p.p. 85-86]. So by base change $\mathbb{T}$ also acts on $J_{H,A}$ and hence $\cot_0 J_{H,A}$. Using the isomorphism 1.2.1 we can extend the action of $\mathbb{T}_{\Gamma_H}$ on $S_2(\Gamma_H, \mathbb{C})$ to all $S_2(\Gamma_H, A)$ in a way that is compatible with base change.

q-expansions

Now the Tate curve E_q over $A[[q]]$ with the standard $\mu_{N,A}$ immersion will give us an element in $P \in \mathcal{X}_\mu(N)(A[[q]])$ and hence an $P_H \in \mathcal{X}_H(A[[q]])$ for all subgroups $H \subseteq (\mathbb{Z}/N\mathbb{Z})^* / \{\pm 1\}$. For this P_H we have $P_{H,A} = \infty_A$ and q is called the standard formal parameter at ∞_A. Now pulling back along P_H gives us a homomorphism:

$$S_2(\Gamma_H, A) := H^0(\mathcal{X}_{H,A}, \Omega^1_{\mathcal{X}_{H,A}/A}) \to H^0(\operatorname{Spec} A[[q]], \Omega^1_{E_q/A[[q]]}).$$

The right hand side is a free $A[[q]]$ module with basis dt/t where dt/t is the standard differential on E_q. By writing every element with respect to this basis we get a homomorphism

$$S_2(\Gamma_H, A) \to A[[q]].$$

The image of a modular form $f \in S_2(\Gamma_H, A)$ under this map is called the q-expansion of f. Over $\mathbb{C}$ this is the same as usual q-expansion.

1.3 Multisets

Multisets are a variation on sets which can contain the same element multiple times. The precise definition I will use is the following:

Definition 1.3. A multiset is a pair (S, f) where S is a set and $f\colon S \to \mathbb{Z}_{\geq 1}$. The function f is called the multiplicity function. A multiset (S, f) is called finite if S is finite and for finite multisets the cardinality is defined as $\#S := \sum_{s \in S} f(s)$.

I will also use set like notation to define multisets, I will use $\{$ and $\}$ for sets while using $\{\!\{$ and $\}\!\}$ for multisets. For example $\{\!\{1, 1, 2\}\!\}$ denotes the multiset which contains the element 1 twice and the element 2 once, i.e. it is the pair (S, f) with $S = \{1, 2\}$ and f is given by $f(1) = 2$ and $f(2) = 1$. The operators $\subseteq, \cap, \cup$ and $\uplus$ on multisets are defined as follows:

Definition 1.4. Let (S_1, f_1) and (S_2, f_2) be two mulitisets then

- $(S_1, f_1) \subseteq (S_2, f_2)$ if $S_1 \subseteq S_2$ and $\forall s \in S_1 : f_1(s) \leq f_2(s)$.
- $(S_1, f_1) \cap (S_2, f_2) := (S_1 \cap S_2, s \mapsto \min(f_1(s), f_2(s))$
- $(S_1, f_1) \cup (S_2, f_2) := (S_1 \cup S_2, s \mapsto \max(f_1(s), f_2(s)))$ where $f_1(s) = 0$ if $s \notin S_1$ and $f_2(s) = 0$ if $s \notin S_2$.
- $(S_1, f_1) \uplus (S_2, f_2) := (S_1 \cup S_2, s \mapsto f_1(s) + f_2(s))$ where $f_1(s) = 0$ if $s \notin S_1$ and $f_2(s) = 0$ if $s \notin S_2$.

Note that the operators $\subseteq, \cap, \cup$ coincide with the usual set operations when viewing a set S as the multiset $(S, s \mapsto 1)$.

Part I
Gonalities

2 The gonality of $\mathcal{X}_1(N)$

A map of degree d from $\mathcal{X}_1(N)_{\mathbb{Q}}$ to $\mathbb{P}^1_{\mathbb{Q}}$ allows us to construct infinitely many points on the modular curve $\mathcal{X}_1(N)_{\mathbb{Q}}$ of degree at most d and hence also infinitely many elliptic curves E over a number field of degree at most d which have a rational N torsion point. Frey also proved a converse result as a short corollary of a theorem of Faltings.

Theorem 2.1 ([Frey, 1994])**.** *Let K be a number field and C/K be a projective absolutely irreducible smooth curve with $C(K) \neq \emptyset$ and suppose d is an integer such that C has infinitely many points of degree at most d over K. Then there is dominant morphism $C \to \mathbb{P}^1_K$ of degree $\leq 2d$.*

Now we make the following definition:

Definition 2.2. Let C be a projective absolutely irreducible smooth curve over a field K and let $K \subset L$ be a field extension. Then the lowest possible degree [1] of dominant map from C_L to $\mathbb{P}^1_L$ is called the L-gonality of C. The L gonality is denoted by $\mathrm{gon}_L(C)$.

The above discussion shows that the gonality of $\mathcal{X}_1(N)_{\mathbb{Q}}$ is a useful quantity to know if one wants to study the points on $\mathcal{X}_1(N)$ over number fields.

Another motivation for wanting to know the gonality is the following theorem due to Michael Stoll in [Derickx, Kamienny, Stein, and Stoll, in preparation]:

Theorem 2.3. *Let $C/\mathbb{Q}$ be a projective smooth and geometrically connected curve with Jacobian J, let $d \geq 1$ be an integer, and let ℓ be a prime of good reduction for C. Let $P_0 \in C(\mathbb{Q})$ be chosen as base-point for the morphism $\iota\colon C \to J$. This also induces morphisms $C^d \to J$ and $C^{(d)} \to J$ from the dth power and from the dth symmetric power of C. If the following assumptions hold*

1. *The $\mathbb{Q}$ gonality of C is at least $d+1$*
2. *$J(\mathbb{Q})$ is finite.*
3. *$\ell > 2$ or $J(\mathbb{Q})[2]$ injects into $J(\mathbb{F}_\ell)$ (for example, $\#J(\mathbb{Q})_{tors}$ is odd).*

[1] See 2.8 for several equivalent definitions of the degree of a morphism to $\mathbb{P}^1_L$

4. *The reduction map $C(\mathbb{Q}) \to C(\mathbb{F}_\ell)$ is surjective.*

5. *The intersection of the image of $C^{(d)}(\mathbb{F}_\ell)$ in $J(\mathbb{F}_\ell)$ with the image of $J(\mathbb{Q})$ under reduction mod ℓ is contained in the image of $C^d(\mathbb{F}_\ell)$.*

Then the only points of degree $\leq d$ on C are the rational points on C.

In the same article it is shown among other things that there are ℓ such 2-5 are satisfied for $d = 5$ and $C = \mathcal{X}_1(29)_\mathbb{Q}, \mathcal{X}_1(31)_\mathbb{Q}$ or $\mathcal{X}_1(41)_\mathbb{Q}$. It is already known that the gonality of $\mathcal{X}_1(41)_\mathbb{Q}$ is 8 or higher by the following lower bound:

Theorem 2.4 ([Abramovich, 1996][2])**.** *Let N be a prime then*

$$\mathrm{gon}_\mathbb{C}(\mathcal{X}_1(N)) \geq \frac{7}{1600}(N^2 - 1).$$

If Selberg's eigenvalue conjecture is true then $\frac{7}{1600}$ can be replaced by $\frac{1}{192}$.

But this bound, even with the assumption of Selberg's eigenvalue conjecture, is not good enough to show that the gonality is at least 6 or higher for $\mathcal{X}_1(29)_\mathbb{Q}$ and $\mathcal{X}_1(31)_\mathbb{Q}$. We will show that $\mathrm{gon}_\mathbb{Q}(\mathcal{X}_1(29)) \geq 11$ and $\mathrm{gon}_\mathbb{Q}(\mathcal{X}_1(31)) \geq 12$ so that Michael Stoll's theorem can also be applied to show that the only points on $\mathcal{X}_1(29)$ and $\mathcal{X}_1(31)$ of degree ≤ 5 over $\mathbb{Q}$ are the cusps. Together with with theorem 3.1 this will give $S(5) = \{2, 3, 5, 7, 11, 13, 17, 19\}$.

The main idea is to use the following theorem which will be proven in section 2.2.

Theorem 2.5. *Let $S = \operatorname{Spec} R$ be the spectrum of a discrete valuation ring with generic point η and closed point s. Let X be a projective S-scheme, smooth of relative dimension one, with geometrically irreducible fibres. Then*

$$\mathrm{gon}_{k(\eta)}(X_\eta) \geq \mathrm{gon}_{k(s)}(X_s).$$

This theorem allows us to reduce computations of a lower bound for the $\mathbb{Q}$-gonality of $\mathcal{X}_1(N)$ to computations of the gonality over finite fields. And over a finite field $\mathbb{F}$ computing the gonality is reduced to finding the smallest degree of an effective divisor such D that $\dim H^0(\mathcal{X}_1(N)_\mathbb{F}, \mathcal{O}_{\mathcal{X}_1(N)_\mathbb{F}}(D)) \geq 2$. This is a finite problem so at least it is theoretically computable.

Doing this computation by brute force is however too slow to be practical for $\mathcal{X}_1(29)_{\mathbb{F}_2}$ and $\mathcal{X}_1(31)_{\mathbb{F}_2}$. In section 2.3 we describe how to exploit

[2]Abramovich actually proves a lower bound for all modular curves. The statement that is given here is what one gets if we restrict to the case we are interested in here.

the automorphisms of $\mathcal{X}_1(N)_{\mathbb{F}}$ and $\mathbb{P}^1_{\mathbb{F}}$ to make the gonality computations possible.

Note that the asymptotic behaviour of the gonality $\mathcal{X}_1(N)$ is already quite well known. Because $X_1(N)$ has a $\mathbb{Q}$ rational point we see in particular that if $g(\mathcal{X}_1(N)) \geq 2$ then $\mathrm{gon}_{\mathbb{Q}}(\mathcal{X}_1(N)) \leq g(\mathcal{X}_1(N))$ [see Poonen, 2007, Appendix A]. In the case that N is a prime > 11 we in particular see that:

$$\mathrm{gon}(\mathcal{X}_1(N)) \leq \frac{(N-5)(N-7)}{24}.$$

As a corollary we get the following theorem which is a slight improvement of [Clark et al., thm. 7](accepted for publication).

Theorem 2.6. *Let $N > 3$ be a prime number and K a number field. Then:*

a) The set of points of $\mathcal{X}_1(N)$ of degree less than $\lceil \frac{7}{3200}(N^2-1) \rceil$ over K is finite. Assuming Selberg's eigenvalue conjecture the bound can be improved to $\lceil \frac{1}{384}(N^2-1) \rceil$.

b) The set of points of $\mathcal{X}_1(N)$ of degree at most $\frac{(N-5)(N-7)}{24}$ over K is infinite.

Note that the theorem in [Clark et al.] is not stated relative to a number field. We added it here because the proof given there is also valid for the relative statement. The bound in b) given there is $\frac{N^2-12N+11}{12}$. The reason for this is that they use a weaker upper bound for the gonality which is also true for curves that don't have a rational point.

Proof. Part a) follows directly from Frey his theorem together with the lower bound for the $\mathbb{C}$-gonality given by Abramovich. While part b) is directly clear from the upper bound of the gonality in terms of the genus. □

2.1 Ingredients for the proof of theorem 2.5

This section discusses the theory of [Liu, 2002] used to prove theorem 2.5. We will give several equivalent definitions of the degree of a morphism to the $\mathbb{P}^1$, so that we can use the one most suitable one while proving the theorem.

Dominant morphisms to the projective line

Let X be a normal curve over a field k then there are at least two ways to describe a dominant morphism to $\mathbb{P}^1_k$. The first one is by using the equivalence between "the category of projective normal curves over k with

dominant morphisms" and "the category of function fields of transcendence degree 1 over k with k-algebra morphisms". To make this more explicit let $\psi\colon K(\mathbb{P}^1_k) = k(t) \to K(X)$ be a morphism then ψ induces a morphism $\pi\colon X \to \mathbb{P}^1_k = \operatorname{Proj} k[x_0, x_1]$ as follows. Let $f := \psi(t)$, then this will be a transcendental element in $K(X)$. Now let $U = X \setminus \operatorname{Supp}(f)_\infty$ the open subset on which f has no poles and $V = X \setminus \operatorname{Supp}(f)_0$ be the set where it has no zeros. Now let $\pi_0\colon U \to D_+(x_0)$ be the morphism corresponding to the ring morphism $k[x_1/x_0] \to \mathcal{O}_X(U)$ given by $x_1/x_0 \mapsto f$ and similar $\pi_1\colon U \to D_+(x_1)$ is the morphism corresponding to $k[x_0/x_1] \to \mathcal{O}_X(V)$ given by $x_0/x_1 \mapsto 1/f$. These morphisms agree on $U \cap V$ by construction and hence we get a morphism $\pi\colon X \to \mathbb{P}^1_k$. Since f is transcendental π will be dominant. To get ψ back from π simply let ξ, η be the generic points of X and $\mathbb{P}^1_k$ respectively then since π is dominant we see that $\pi(\xi) = \eta$ hence π induces a morphism $k(t) = \mathcal{O}_{\mathbb{P}^1_k,\eta} \to \mathcal{O}_{X,\xi} = K(X)$ which is equal to ψ.

The second way to describe a morphism from $X \to \mathbb{P}^1_k$ is more general and will actually work for X any scheme and $\mathbb{P}^1_k$ replaced by any projective space over any ring.

Proposition 2.7. *[Liu, 2002, prop. 5.1.31] Let $\mathbb{P}^d_A := \operatorname{Proj} A[T_0, \ldots, T_d]$ be a projective space over a ring A and let X be an A scheme.*

(a) Let $\pi\colon X \to \mathbb{P}^d_A$ be a morphism then $\pi^*(\mathcal{O}_{\mathbb{P}^d_A}(1))$ is an invertible sheaf on X which is generated by the $d+1$ global sections $\pi^*(T_0), \ldots, \pi^*(T_d)$.

(b) Conversely, for any invertible sheaf $\mathcal{L}$ on X generated by $d+1$ global sections $s_0, \ldots, s_d$ there exists a unique morphism $\pi\colon X \to \mathbb{P}^d_A$ such that $\mathcal{L} \cong \pi^*(\mathcal{O}_{\mathbb{P}^d_A}(1))$ and $\pi^*(T_i) = s_i$.

Proof. I refer to [Liu, 2002] for a complete proof. I will here only show how π is constructed in the proof of part (b) since that is actually an important part for understanding the proposition. Let $X_{s_i} := \{x \in X \mid \mathcal{L}_x = s_{i,x}\mathcal{O}_{X,x}\}$ be the open part of X where s_i generates $\mathcal{L}$. Then the X_{s_i} cover X and we can construct π by giving $\pi_i = \pi|_{X_{s_i}}\colon X_{s_i} \to D_+(T_i)$. These π_i are given on global sections as follows:

$$\mathcal{O}_{\mathbb{P}^d_A}(D_+(T_i)) \to \mathcal{O}_X(X_{s_i}), T_j/T_i \mapsto s_j/s_i \in \mathcal{O}_X(X_{s_i})$$

□

Degrees and gonality

Now we restrict to the case where X is a projective smooth and geometrically connected curve over a field k. Let $\psi\colon K(\mathbb{P}^1_k) = k(t) \to K(X)$ a map of

k-algebra's and $f := \psi(t)$. Let D be the Cartier divisor such that the corresponding Weil divisor $[D] = (f)_\infty$ is the pole divisor f and let $\mathcal{L} = O_X(D)$ be the invertible sheaf generated by $s_0 := 1, s_1 := f$ then it is clear that the two constructions in the previous subsection give the same morphism π. In this setting we can define the degree of π in several different but equivalent ways.

Definition / Proposition 2.8. *Let X over k be a projective smooth geometrically connected curve and $\pi\colon X \to \mathbb{P}^1_k$ be a dominant morphism then the following integers are equal:*

(1) $[K(X) : k(t)]$

(2) $\deg (f)_\infty$

(3) $\deg D$

(4) $\deg \mathcal{O}_X(D) = \deg \mathcal{L} := \chi_k(L) - \chi_k(\mathcal{O}_X)$

Where $k(t), f$ and D are as above. The degree of π is defined to be any of the above integers and is denoted by $\deg \pi$.

Proof. I will give references to [Liu, 2002] for 3 equalities which will make everything equal. The equality of (1) and (2) is corollary 7.3.9. The equality of (2) and (3) is remark 7.3.2 and the equality of (3) and (4) is part a of lemma 7.3.30. □

Recall that we defined the gonality of a curve to be the minimum of the degrees of all dominant morphisms to the projective line. The definition of gonality is the simplest in terms of proposition 2.8 part (1) because then we have[3]

$$\operatorname{gon}(X) = \min_{f \in K(X)} [K(X) : k(f)].$$

Proposition 2.9. *Let $S = \operatorname{Spec} R$ be the spectrum of a discrete valuation ring with generic point η and closed point s. Let X be a projective and flat S-scheme whose fibers are curves and let $\mathcal{L}$ be an invertible sheaf on X then* $\deg \mathcal{L}_{k(s)} = \deg \mathcal{L}_{k(\eta)}$.

Proof. Since X is flat over S we also have that all locally free sheaves on X are flat over S. In particular $\mathcal{O}_X$ and $\mathcal{L}$ are flat over S and we can use the

[3]Note that occurrence of non transcendental f in this minimum does not influence the outcome since non transcendental f they will never give rise to a minimum.

invariance of the Euler-Poincaré characteristic [see Liu, 2002, prop. 5.3.28] to get

$$\deg \mathcal{L}_{k(s)} = \chi(\mathcal{L}_{k(s)}) - \chi(\mathcal{O}_{X,k(s)}) = \chi(\mathcal{L}_{k(\eta)}) - \chi(\mathcal{O}_{X,k(\eta)}) = \deg \mathcal{L}_{k(s)}$$

□

Proposition 2.10. *Let X be a projective curve over a field k and let $0 \to \mathcal{F} \to \mathcal{G}$ be an an exact sequence of invertible sheaves. Then* $\deg \mathcal{F} \leq \deg \mathcal{G}$

Proof. The statement $\deg \mathcal{F} \leq \deg \mathcal{G}$ is equivalent to showing $\chi_k(\mathcal{F}) \leq \chi_k(\mathcal{G})$. Now remark that we have the exact sequence $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{F}/\mathcal{G} \to 0$ hence $\chi_k(\mathcal{G}) = \chi_k(\mathcal{F}) + \chi_k(\mathcal{G}/\mathcal{F})$. So it suffices to show that $\chi_k(\mathcal{G}/\mathcal{F}) \geq 0$, but this is indeed the case as $\mathcal{G}/\mathcal{F}$ is a skyscraper sheaf and hence $H^1(X, \mathcal{G}/\mathcal{F}) = 0$ showing that $\chi_k(\mathcal{G}/\mathcal{F}) = \dim_k H^0(X, \mathcal{G}/\mathcal{F}) \geq 0$ □

2.2 Proof of theorem 2.5 (Gonality under specialisation)

The idea of the proof is to construct for every dominant morphism $\pi\colon X_\eta \to \mathbb{P}^1_{k(\eta)}$ a dominant morphism $X_s \to \mathbb{P}^1_{k(s)}$ of smaller or equal degree.

As X is smooth over a regular ring, it is itself regular. Since X is projective over a discrete valuation ring it is also Noetherian and it is integral because it is irreducible and reduced. This means we may identify Weil divisors with Cartier divisors and invertible sheaves, i.e. $\operatorname{Cl} X = \operatorname{CaCl} X = \operatorname{Pic} X$. Now X_s is a closed irreducible subscheme of X of codimension 1 whose complement is X_η hence by II.6.5(c) of [Hartshorne, 1977] we have the exact sequence

$$\mathbb{Z} \to \operatorname{Cl} X \to \operatorname{Cl} X_\eta \to 0.$$

In other words $\operatorname{Cl} X \to \operatorname{Cl} X_\eta$ is surjective and hence the corresponding map $\operatorname{Pic} X \to \operatorname{Pic} X_\eta$ is also surjective.

Now let $\pi\colon X_\eta \to \mathbb{P}^1_{k(\eta)} = \operatorname{Proj} k(\eta)[T_0, T_1]$ be a dominant morphism then by surjectivity of $\operatorname{Pic} X \to \operatorname{Pic} X_\eta$ there is an invertible sheaf $\mathcal{F}$ on X such that $\mathcal{F}_\eta = \pi^*(\mathcal{O}_{\mathbb{P}^1_{k(\eta)}}(1))$. By [Liu, 2002, 5.1.20 (a)] we have

$$\dim_{k(s)} H^0(X_s, \mathcal{F}_s) \geq \dim_{k(\eta)} H^0(X_\eta, \mathcal{F}_\eta)$$

so since $\mathcal{F}_\eta$ has the two $k(\eta)$ linearly independent global sections $\pi^*(T_0)$ and $\pi^*(T_1)$, we see that $\mathcal{F}_s$ also has pair of $k(s)$ linearly independent global sections, let s_0, s_1 be such a pair. Define $\mathcal{L} \subset \mathcal{F}_s$ to be the sheaf generated by s_0, s_1. Now X_s is smooth of relative dimension 1 over the field $k(s)$, so

the local rings are either a field or a d.v.r. implying that locally either s_0 or s_1 generates $\mathcal{L}$ so $\mathcal{L}$ is invertible. Now let $\pi' \colon X_s \to \mathbb{P}^1_{k(s)}$ be the morphism given by $\mathcal{L}, s_0, s_1$. Since s_0 and s_1 are linearly independent the morphism π' is not constant and hence dominant. So the theorem now follows from the inequality

$$\deg \pi' = \deg \mathcal{L} \leq \deg \mathcal{F}_s = \deg \mathcal{F}_\eta = \deg \pi$$

□

2.3 How to compute the $\mathbb{F}_q$-gonality of $\mathcal{X}_1(N)$ in practice

In this section we give the $\mathbb{F}_2$ gonalities of $\mathcal{X}_1(N)$ for several odd N. We do this so that theorem 2.5 will give us lower bounds for the $\mathbb{Q}$ gonality of $\mathcal{X}_1(N)$. These bounds turn out to be surprisingly good in practice. After that I will explain how I computed these gonalities.

Proposition 2.11. *The $\mathbb{F}_2$ gonalities of $\mathcal{X}_1(N)$ for the odd N with $N \leq 31$ are as follows:*

N	$\text{gon}_{\mathbb{F}_2}$	N	$\text{gon}_{\mathbb{F}_2}$	N	$\text{gon}_{\mathbb{F}_2}$	N	$\text{gon}_{\mathbb{F}_2}$
1	1	9	1	17	4	25	5
3	1	11	2	19	5	27	6
5	1	13	2	21	4	29	11
7	1	15	2	23	7	31	12

Table 2.1: some $\mathbb{F}_2$ gonalities

Proof. For $N < 17$ this follows directly from the tables in [Sutherland, 2012]. It is clear that the curves of gonality at most 1 according to the tables in Sutherland cannot have lower gonality. The same holds for the curves of gonality at most 2 since those have nonzero genus.

For the other N the gonalities where computed using Magma. The computations themselves can be found in Appendix A. □

In the rest of this section I will explain why the calculations are correct and what tricks I used to make them fast enough to make them finish before my graduation deadline.

Theorem 2.12. *Let $\mathbb{F}$ be a finite field and let $C/\mathbb{F}$ be smooth projective geometrically irreducible curve. Then the $\mathbb{F}$-gonality of C is computable.*

Proof. Let d be a positive integer and define

$$S_d := \{D \in \operatorname{div} C \mid D \geq 0, \deg D = d\}. \tag{2.3.1}$$

Now $\operatorname{gon}_F C > d$ if and only if for all $D \in S_d$ we have $\dim H^0(C, D) = 1$. The sets S_d are finite. So we can compute the gonality as follows:

Step 1 set $d = 1$

Step 2 While for all $D \in S_d : \dim H^0(C, D) = 1$ increase d by 1.

Step 3 Output d.

□

The above already gives a very slow (but deterministic) way of computing the $\mathbb{F}$ gonality. However even over $\mathbb{F}_2$ this brute force way is too slow to be useful in practice.

Now the main idea to make the computation faster is by exploiting the automorphisms of C and $\mathbb{P}^1_{\mathbb{F}}$. These automorphisms act on the dominant morphism $C \to \mathbb{P}^1_{\mathbb{F}}$ and this action does not change the degree of the morphism.

Definition 2.13. Let C be a smooth projecitve geometrically irreducible curve over a finite field $\mathbb{F}$ and d an integer. We say that a that a set of divisors $S \subset \operatorname{div} C$ dominates all functions of degree $\leq d$ if for all dominant $f \colon C \to \mathbb{P}^1_{\mathbb{F}_p}$ of degree $\leq d$ there are $g \in \operatorname{Aut}(C)$, $h \in \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}_p})$ and $D \in S$ such that $\operatorname{div} h \circ f \circ g \geq -D$.

The idea behind this definition is that as soon that there exists an $f \colon C \to \mathbb{P}^1_{\mathbb{F}_p}$ of degree $\leq d$ that there will then be a $D \in S$ such that $H^0(C, D)$ contains a function of degree $\leq d$, namely the function $h \circ f \circ g$. So we have the following proposition.

Proposition 2.14. *Suppose that $C, \mathbb{F}$ and d are as above and $S \subset \operatorname{div} C$ dominates all functions of degree $\leq d$ then*

$$\operatorname{gon}_{\mathbb{F}} C \geq \min(d+1, \inf_{\substack{D \in S, \\ f \in H^0(C,D), \\ \deg f \neq 0}} \deg f).$$

Now in the calculations for the lower bounds in Appendix A the strategy is to find an as small as possible set S of which we can show that it dominates all functions of degree $\leq d$ while also trying to keep the dimension of the corresponding Riemann-Roch spaces small enough so that it is still feasible

to calculate the degree of all functions in the occurring Riemann-Roch spaces. Upper bounds are just obtained by finding functions of low degree.

The following proposition already gives one way to find a smaller set that still dominates all functions of degree $\leq d$.

Proposition 2.15. *Let C be a curve over a finite field $\mathbb{F}_q$ and d an integer. Define $n := \lceil \#C(\mathbb{F}_q)/(q+1) \rceil$ and*

$$D = \sum_{p \in C(\mathbb{F}_q)} p \in \operatorname{div}(C)$$

then

$$S_{d-n} + D := \{s' + D \mid s' \in S_{d-n}\}$$

dominates all functions of degree $\leq d$.

Proof. For all $f \colon C \to \mathbb{P}^1_{\mathbb{F}_q}$ we have $f(C(\mathbb{F}_q)) \subseteq \mathbb{P}^1(\mathbb{F}_q)$ so there is always a $g \in \operatorname{Aut} \mathbb{P}^1_{\mathbb{F}_q}$ such that $g \circ f$ has a pole at at least n distinct points in $C(\mathbb{F}_q)$. So suppose that f has degree at most d then there is an element $s \in S_{d-n}$ such that $\operatorname{div} g \circ f \geq -s - D$. □

Note that the above trick increases the degree of the divisors we have to check by $\#C(\mathbb{F}_q) - n$. But the upper bounds for the gonality of $\mathcal{X}_1(N)_{\mathbb{F}_2}$ we get from the tables in [Sutherland, 2012] are often significantly lower then the genus of $\mathcal{X}_1(N)_{\mathbb{F}_2}$. For example the genus of $X_1(29)$ is 22 while its gonality is at most 11. So we still expect the dimension of these Riemann-Roch spaces to be small for divisors of degree slightly larger then the gonality.

The second trick used to make the computations faster is the following.

Proposition 2.16. *Let C be a curve over a finite field, d be an integer and suppose that S dominates all functions of degree $\leq d$. Let $S' \subset \operatorname{div} C$ be such that for all $s \in S$ there are $s' \in S'$ and $g \in \operatorname{Aut} C$ such that $g(s') \geq s$. Then S' also dominates all functions of degree $\leq d$.*

Proof. This is by definition of S dominating all functions of degree $\leq d$. □

This proposition will in particular be useful when $C = \mathcal{X}_1(N)_{\mathbb{F}_q}$ since the diamond operators will ensure that $\mathcal{X}_1(N)_{\mathbb{F}_q}$ always has nontrivial automorphisms if $N > 6$.

2.4 Some $\mathbb{Q}$ gonalities of $\mathcal{X}_1(N)$ for small odd N

Now we use the computed $\mathbb{F}_2$ gonalities to determine the $\mathbb{Q}$ gonalities.

Corollary 2.17. *For the odd N with $N \leq 29$ the $\mathbb{Q}$-gonality of $\mathcal{X}_1(N)$ is the same as the $\mathbb{F}_2$ gonality listed in table 2.1 and the $\mathbb{Q}$ gonality of $\mathcal{X}_1(31)$ is 12 or 13.*

Note that the $\mathbb{Q}$ gonality was already known for $N \leq 22$ [see Sutherland, 2012]. And at the moment in fact all gonalities (not just the odd ones) have been computed for $N \leq 40$ in a joint work of Mark van Hoeij and me that still has to be published.

Proof. For $N \neq 25, 27$ this follows directly from the gonality calculations over $\mathbb{F}_2$ together with 2.5 and the tables in [Sutherland, 2012]. For $N = 25, 27$ it suffices to give maps to $\mathbb{P}^1_{\mathbb{Q}}$ of degree 5 and 6 respectively since 5 and 6 are the lower bounds for the $\mathbb{Q}$-gonality that follow from the gonality calculations over $\mathbb{F}_2$.

For $N = 25$ we can construct a map of degree 5 by noticing that the quotient map to $\mathcal{X}_1(25)_{\mathbb{Q}}/\langle 16\rangle$ has degree 5 since 16 has order 5 in $(\mathbb{Z}/25\mathbb{Z})^*/\{\pm 1\}$. Also $\mathcal{X}_1(25)_{\mathbb{Q}}/\langle 16\rangle$ has genus 0 and a rational point (some of the cusps are rational) hence it is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$.

```
sage: G=GammaH(25,[16])
sage: G.genus()
0
```

For $N = 27$ we can construct a map of degree 6 by noticing that quotient the map to $\mathcal{X}_1(27)_{\mathbb{Q}}/\langle 10\rangle$ has degree 3 since 10 has order 3 in $(\mathbb{Z}/27\mathbb{Z})^*/\{\pm 1\}$. Also $\mathcal{X}_1(27)_{\mathbb{Q}}/\langle 10\rangle$ has genus 1 and has a rational point, hence it is an elliptic curve and its gonality is 2. So composition gives us a map of degree 6 from $\mathcal{X}_1(27)_{\mathbb{Q}}$ to $\mathbb{P}^1_{\mathbb{Q}}$.

```
sage: G=GammaH(27,[10])
sage: G.genus()
1
```

□

Part II
Torsion Points

3 Introduction

This Part of my thesis will be about studying the existence of torsion points of prime order over number fields of small degree. Suppose d is an integer and define the set $B(d)$ to be the set of integers N such that there exist an elliptic curve E over a number field K with $[K : \mathbb{Q}] \leq d$ and a point $P \in E(K)$ of order N. There is also a related set $S(d)$ which has the same definition except with the additional condition that N is prime. These sets have already been studied by a lot of different people. The first result on this was by Mazur who among other things completely determined $B(1)$ in [Mazur, 1977], in fact he determined all group structures that occur as $E(\mathbb{Q})_{tors}$. Later it was shown that $B(d)$ is finite for several small d giving rise to the so called uniform boundedness conjecture which states that $B(d)$ is finite for all d. A first step in proving this conjecture was provided in [Kamienny and Mazur, 1995], there it was shown that for all d we have $S(d)$ is finite if and only $B(d)$ is finite. Later Merel managed to show that indeed $S(d)$ is always finite in [Merel, 1996] and hence the uniform boundedness conjecture is also true. The main goal of this part of my thesis is to study the set $S(d)$ for several small values of d.

3.1 What is known about $S(d)$

Let Primes(N) be the set of primes less then or equal to N then the following is already known about $S(d)$:

$S(d) \subseteq \text{Primes}((3^{d/2}+1)^2)$	([Oesterlé, not published])
$S(1) = \text{Primes}(7)$	([Mazur, 1977])
$S(2) = \text{Primes}(13)$	([Kamienny, 1992b])
$S(3) = \text{Primes}(13)$	([Parent, 2000, 2003])
$S(4) = \text{Primes}(17)$	([Derickx, Kamienny, Stein, and Stoll])

Table 3.1: Some known bounds on $S(d)$.

Note that at this moment the article [Derickx et al.] is still in preparation. And although I will be a co-author of that article the result above should really be attributed to Kamienny, Stein and Stoll since they already announced a proof of $S(4) = \text{Primes}(17)$ way before I knew anything about the subject. A large part for calculating $S(4)$ consists of using a computer to check for a lot of primes p whether the hypotheses of theorem 1.10 of [Parent, 2000] are satisfied showing that for these primes we have $p \notin S(d)$. Simply running the same computer calculations for $S(5)$ would take too long, this is why they did not do it for other d. The main goal of section 5 will be to make it computationally more efficient to check the hypotheses of theorem 1.10 of [Parent, 2000] so that these techniques can also be used for $S(5), S(6)$ and $S(7)$.

There are two improvements I will make that will shorten the computation time needed dramatically. The biggest improvement comes from translating the work in [Parent, 2000] to the setting of $\mathcal{X}_0(p)$ so that we can use hecke operators in $\mathbb{T}_{\Gamma_0(p))}$ instead of $\mathbb{T}_{\Gamma_1(p))}$. Altough it has not been done before in the exact way I will do it here it is not very original since this is basically a combination of the tactics used in [*Parent*, 1999] where Parent uses $\mathcal{X}_0(p)$ and [*Parent*, 2000] where he developed techniques to get around the difficulties ocurring when reducing modulo 2 [4]. The second way of speeding things up is more original and is explained in section 5.5.

Note that one of the conditions for showing $p \notin S(d)$ using theorem 1.10 of [Parent, 2000] is that $p > (l^{d/2} + 1)^2$ (here l can be any prime). By being more carefull in the analysis of what happens when $l = 2$ I will however be able to show $p \notin S(d)$ for some primes $p \leq (l^{d/2} + 1)^2$ using the same techniques as in [Parent, 2000].

Sadly enough [Parent, 2000] contains a small error (see the footnote at 5.8 in this thesis). This mistake affects the calculations done for $S(3)$ but also for $S(4)$. It will be only a little effort to make the computer also check whether the hypotheses of theorem 1.10 of [Parent, 2000] are still satisfied for $S(3)$ and $S(4)$. So I will redo these computations to verify that the same results about $S(d)$ can still be obtained. To be more precise I will prove the following theorem.

Theorem 3.1. *If* $\max(S(7)) \leq \lfloor (3^{7/2} + 1)^2 \rfloor = 2281$ [5] *then the following inclusions of sets hold:*

[4] see the text after 5.5 for a short discussion of the difficulties when reducing modulo 2

[5] This condition will be satisfied if Oesterlé his bound holds. The article of Oesterlé which should contain a prove of this bound is cited as "article à paraître" in [Parent, 1999], indicating that the article would be published not to far in the future. But since it is now 13 years later it doesn't look like that this will happen. So I included this condition for

$S(3) \subseteq \text{Primes}(17)$
$S(4) \subseteq \text{Primes}(19) \cup \{29\}$
$S(5) \subseteq \text{Primes}(19) \cup \{29, 31, 41\}$
$S(6) \subseteq \text{Primes}(41) \cup \{73\}$
$S(7) \subseteq \text{Primes}(43) \cup \{59, 61, 67, 71, 73, 113, 127\}$

Table 3.2: Some new bounds on $S(d)$.

Note that these results for $S(3)$ and $S(4)$ are slightly weaker then what is mentioned in table 3.1. But this is no problem since in the original proofs for $S(3) = \text{Primes}(13)$ and $S(4) = \text{Primes}(17)$ there where also some special cases for which different techniques where needed. These special cases will also be taken care of in [Derickx et al.]. These techniques can also be used to improve the results for $S(5)$. In fact it is now known that $S(5) = \text{Primes}(19)$ since Michael Stoll managed to show $29, 31, 41 \notin S(5)$. A proof of this will be given in [Derickx et al.]. The proof that $29, 31, 41 \notin S(5)$ uses the gonality calculations for $p = 29$ and 31 done in Part I of this thesis.

3.2 Approach

The main idea is to rule out possibilities depending on the type of reduction an elliptic curve over a number field can have. The reduction type of an elliptic curve E over a number field K can depend on the model you chose over $\mathcal{O}_K$. So to make the reduction type independent of this choice, we take the reduction type of a model of E over $\mathcal{O}_K$ which is equal to its Weierstrass minimal model at all primes $q \in \mathcal{O}_K$ lying over a fixed prime $l \in \mathbb{Z}$. The different possibilities are listed in the following proposition.

Proposition 3.2. *Let K be a number field and l be a prime number. Let E/K be an elliptic curve and $P \in E(K)$ a point of prime order. Then either there is a prime $q \subset \mathcal{O}_K$ lying over l satisfying one of the following conditions:*

(i) E has good reduction at q

(ii) E has additive reduction at q

the theorem to make explicit how this current gap in the literature affects this theorem.

(iii) E has non-split multiplicative reduction

(iv) E has split multiplicative reduction at q and P does not reduce to the singular point.

or

(v) E has split multiplicative reduction at all primes lying over l and P reduces to the singular point at all these primes.

To be able to formulate the separate results for cases $(i-v)$ independently we will make the following definition.

Definition 3.3. Let $x \in \{i, ii, iii, iv, v\}$ be one of the cases in proposition 3.2 and l be a prime. Then for an integer d we denote by $S_l^{(x)}(d)$ the set of primes p such that there exists an elliptic curve E over a number field K of degree at most d with a point P of order p satisfying case x of proposition 3.2

It follows directly from the proposition that for all primes l we have $S(d) = S_l^{(i)}(d) \cup S_l^{(ii)}(d) \cup S_l^{(iii)}(d) \cup S_l^{(iv)}(d) \cup S_l^{(v)}(d)$. So theorem 3.1 follows from using this equality together with the restrictions on $S_2^{(i)}(d), \ldots, S_2^{(v)}(d)$ listed in tables 4.2, 4.3 and 5.1 and equation 4.2.1.

Now let $l \nmid p$ be distinct primes, K be a number field of degree d and $P \in E(K)[p]$. Then the order of the point P stays the same after reduction at a prime $q \supset (l)$, so if we can bound the order of the torsion points on the reduction of the curve we can also bound it for the curve itself. If we take the case (i) for example the residue class degree of q (i.e. $[\mathcal{O}_K/q : \mathbb{F}_l]$) is bounded above by the degree of K. Now let $d := [K : \mathbb{Q}]$ be the degree of K then one can use the Hasse bound to see that $\max S_l^{(i)}(d) \leq (l^{d/2} + 1)^2)$. In particular we see that l has to be small in order to get a small upper bound. For this reason primes bigger then 5 are rarely used in the literature, and we will use $l = 2$. Now in the case of bad reduction, points reducing to a singular point give difficulty in this approach since the group structure on the reduction is only defined for the non-singular points. Luckily there is already theory for dealing with these difficulties namely the theory of Neron models of elliptic curves. It turns out that in cases $(i) - (iv)$ it is easy to give an upper bound on the torsion order depending on l and d. To give a bound for the torsion order in the (v) case is much more work. How to do this is explained in section 5. For this we use an approach similar to the one in [Parent, 1999].

4 Point orders in different types of reduction

4.1 case (i): Good Reduction

Shortly after definition 3.3 we already mentioned how one can use the Hasse bound to bound $\max S_l^{(i)}(d)$. The result we obtained there can actually be slightly improved since not all integers in the Hasse interval have an elliptic curve corresponding to them. Being as precise as possible we will not only bound $\max S_l^{(i)}(d)$ but also try to show that $p \notin S_l^{(i)}(d)$ for as many primes p smaller then this bound as possible. Similar to the argument given after definition 3.3 we will show $p \notin S_l^{(i)}(d)$ by showing that there is no elliptic curve E over a finite field $\mathbb{F}_q$ with $[\mathbb{F}_q : \mathbb{F}_l] \leq d$ such that $p \mid \#E(\mathbb{F}_q)$. For this we need to know which values $\#E(\mathbb{F}_q)$ can take for a certain prime power q. The occurring values are precisely classified by [Waterhouse, 1969, thm. 4.1]. This theorem is stated below.

Theorem 4.1. *Let $\mathbb{F}_q$ be a finite field with $q = l^a$ then the set*

$$\{\#E(\mathbb{F}_q) \mid E/\mathbb{F}_q \text{ is an elliptic curve}\}$$

consists of the integers n with $|n-q-1| \leq 2\sqrt{q}$ satisfying any of the following conditions.

1. $\gcd(n-1, l) = 1$
2. *If a is even :* $n = q + 1 \pm 2\sqrt{q}$
3. *If a is even and $l \not\equiv 1 \mod 3$:* $n = q + 1 \pm \sqrt{q}$
4. *If a is odd and $l = 2$ or 3 :* $n = q + 1 \pm l^{\frac{a+1}{2}}$
5. *If either a is odd or (a is even and $l \not\equiv 1 \mod 4$) :* $n = q + 1$

In the rest of this section we will work with $l = 2$. This means that the condition 1 comes down to saying that n is even. So in this case we have for $P \in E(\mathbb{F}_q)$ of prime order p with $p > 2$ that $p \leq n/2 \leq (2^{a/2} + 1)^2/2$. The set of special cases $(2-5)$ is very small hence the lowering of the bound $(2^{a/2} + 1)^2$ by a factor 2 in case 1 will allow us to show $p \notin S_l^{(i)}(d)$ for quite some primes in the range between $(2^{a/2}+1)^2/2$ and $(2^{a/2}+1)^2$. Table 4.1 lists which primes occur as a divisor of $\#E(\mathbb{F}_{2^a})$ for a some elliptic curve $E/\mathbb{F}_{2^a}$.

a	primes dividing $\#E(\mathbb{F}_{2^a})$ for some $E/\mathbb{F}_{2^a}$
1	Primes(5)
2	Primes(7)
3	Primes(7) $\cup \{13\}$
4	Primes(17)
5	Primes(19) $\cup \{41\}$
6	Primes(19) $\cup \{29, 31, 37, 73\}$
7	Primes(37) $\cup \{43, 59, 61, 67, 71, 73, 113\}$

Table 4.1:

Remark. Table 4.1 is not an increasing list with respect to inclusion. For example 41 occurs for $a = 5$ but not for $a = 6$ or $a = 7$. So although 41 doesn't occur for $a = 6$ we cannot rule out the existence of a number field K of degree 6 with a prime $q \subseteq \mathcal{O}_K$ lying over 2 with at which the elliptic curve has good reduction because $2\mathcal{O}_K$ might split as $q \cdot r$ where $q, r \subset O_K$ are primes residue class degree 1 and 5 respectively.

From table 4.1 one can obtains the restrictions on $S_2^{(i)}(d)$ listed in table 4.2.

$$S_2^{(i)}(3) \subseteq \text{Primes}(7) \cup \{13\}$$
$$S_2^{(i)}(4) \subseteq \text{Primes}(17)$$
$$S_2^{(i)}(5) \subseteq \text{Primes}(19) \cup \{41\}$$
$$S_2^{(i)}(6) \subseteq \text{Primes}(19) \cup \{29, 31, 37, 41, 73\}$$
$$S_2^{(i)}(7) \subseteq \text{Primes}(43) \cup \{59, 61, 67, 71, 73, 113\}$$

Table 4.2: Some bounds on $S_2^{(i)}(d)$.

4.2 case $(ii) - (iv)$: Additive and Some Multiplicative Reduction

The following proposition shows how big the order of the point P can be with respect to the prime of reduction l in cases $(ii) - (iv)$ of 3.2.

Proposition 4.2. *Let E be an elliptic curve over a number field K and $l \in \mathbb{Z}$ prime $q \subset \mathcal{O}_K$ is a prime lying over l with residue field k of degree f over $\mathbb{F}_l$ and $P \in E(K)$ a point of prime order p. If the elliptic curve has*

(ii) additive reduction then $p = 2, 3$ or l,

(iii) non-split multiplicative reduction then $p = 2, l$ or $p \mid (l^f + 1)$,

(iv) split multiplicative reduction and P reduces to a non-singular point then $p = l$ or $p \mid (l^f - 1)$

Proof. Let K_q be the completion of K with respect to q and $R \subset K_q$ its ring of integers. Let $\mathcal{E}$ denote the Neron model over R of $E_{\mathcal{K}_q}$ and $\tilde{\mathcal{E}} := \mathcal{E} \times_{\operatorname{Spec} R} \operatorname{Spec} k$ its special fiber and $\tilde{\mathcal{E}}^0$ be the identity component of the special fiber. Now in all three cases $p = l$ is a case of which we do not need to show that it is impossible, so we can assume $p \neq l$ and hence that $E(K)[p]$ will inject into $\tilde{\mathcal{E}}(k)$. Now the group scheme $\tilde{\mathcal{E}}$ sits in an exact sequence

$$0 \to \tilde{\mathcal{E}}^0 \to \tilde{\mathcal{E}} \to \Phi \to 0$$

Where Φ is the component group of $\tilde{\mathcal{E}}$. And since the $\operatorname{Hom}(k, \_)$ functor is left exact we get an exact sequence of groups

$$0 \to \tilde{\mathcal{E}}^0(k) \to \tilde{\mathcal{E}}(k) \to \Phi(k)$$

Hence $p \mid \#\tilde{\mathcal{E}}^0(k)$ or $p \mid \#\Phi(k)$ and we can apply this to the three different cases.

In the additive case $\tilde{\mathcal{E}}^0(k) \cong k$ and $\#\Phi(k) \leq 4$ so $p = 2, 3$.

In the non-split multiplicative case $\#\tilde{\mathcal{E}}^0(k) = \#k + 1$ and $\#\Phi(k) \leq 2$ so $p = 2$ or $p \mid (l^f + 1)$.

In the split multiplicative case we cannot say anything about $\#\Phi(k)$, but in case (iv) the point P reduces to a non singular point so we know that it specializes to a point in the identity component hence $p \mid \#\tilde{\mathcal{E}}^0(k) = \#k^* = l^f - 1$. □

It directly follows from this proposition that

$$S_2^{(ii)}(d) \subseteq \{2, 3\} \tag{4.2.1}$$

for all d. Bounds for $S_2^{(iii)}(d)$ and $S_2^{(iv)}(d)$ can also be obtained by determining the divisors of $p \mid 2^e + 1$ resp. $p \mid 2^e - 1$ for all $e \leq d$. The results are given in the following table:

$$
\begin{aligned}
&S_2^{(iii)}(3) \subseteq \text{Primes}(5)\\
&S_2^{(iii)}(4) \subseteq \text{Primes}(5) \cup \{17\}\\
&S_2^{(iii)}(5) \subseteq \text{Primes}(11) \cup \{17\}\\
&S_2^{(iii)}(6) \subseteq \text{Primes}(17)\\
&S_2^{(iii)}(7) \subseteq \text{Primes}(17) \cup \{43\}\\
&S_2^{(iv)}(3) \subseteq \{2,3,7\}\\
&S_2^{(iv)}(4) \subseteq \text{Primes}(7)\\
&S_2^{(iv)}(5) \subseteq \text{Primes}(7) \cup \{31\}\\
&S_2^{(iv)}(6) \subseteq \text{Primes}(7) \cup \{31\}\\
&S_2^{(iv)}(7) \subseteq \text{Primes}(7) \cup \{31,127\}
\end{aligned}
$$

Table 4.3: Some bounds on $S_2^{(iii)}(d)$ and $S_2^{(iv)}(d)$.

5 A new version of Kammienny's Criterion over $\mathbb{F}_2$

In the literature there are already several ways of dealing with the case we have not treated yet, namely case (v) of 3.2. Mazur gave two different approaches in [Mazur, 1977] and [Mazur, 1978] for elliptic curves over $\mathbb{Q}$. Kamienny generalized a part of Mazurs approach to number fields of a bounded degree in [Kamienny, 1992a], where he reduced everything to a question about certain Hecke operators being linearly independent, this linear independence question is now known as "Kamienny's criterion". Ways of dealing with case (v) as well as several variations of Kamienny's criterion can be found in [Merel, 1996], [Oesterlé, not published], [Parent, 1999] and [Parent, 2000]. In this section I will explain the common part of these approaches as well as well as giving a generalisation of the version of Kamienny's criterion that is found in [Parent, 2000].

The general strategy of dealing with case (v) of proposition 3.2 is as follows.

Step 1 Suppose for contradiction that there exists a pair (E,P) where E is an elliptic curve over a number field K of degree d and P is a point of prime order p and let l be a prime such that his data together satisfies (v).

Step 2 Use the pair (E, P) to construct a point $s \in \mathcal{X}_0(p)^{(d)}(\mathbb{Q})$ such that $s_{\mathbb{F}_l} = \infty^{(d)}_{\mathbb{F}_l}$.

Step 3 Construct a map $f\colon \mathcal{X}_0(p)^{(d)} \to A$ for some abelian variety A such that $f(s) = f(\infty^{(d)})$.

Step 4 Use a variation of Kamienny's criterion to check whether f is a formal immersion at $\infty^{(d)}_{\mathbb{F}_l}$. If f is indeed a formal immersion then this implies $s = \infty^{(d)}$ contradicting the assumption in Step 1. As a conclusion we get that such a pair (E, P) does not exist, i.e. that $p \notin S_l^{(v)}(d)$

The different versions of Kamienny's criterion come from taking different choices for the abelian variety A and different choices of the map f. Note that as in [Parent, 2000] one can also use the pair (E, P) to construct a point $s \in X_\mu(p)^{(d)}(\mathbb{Q})$ instead of $X_0(p)^{(d)}(\mathbb{Q})$ and modify steps 2, 3 and 4 accordingly. This approach requires a little more work, and a little more notation to formulate. This is why I formulated it in this overview only for $\mathcal{X}_0(p)$ since formulating it for $\mathcal{X}_\mu(p)$ would just be distracting. The road we will take in the rest of this section however is expressing everything in terms of $\mathcal{X}_H$ which is a quotient of $\mathcal{X}_\mu(p)$, where H can be any subgroup of $(\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$. Although this also gives the same complication in notation as for $\mathcal{X}_\mu(p)$ we really do need this since I will need to be able to also state Kamienny's criterion for $\mathcal{X}_\mu(p)$ as in [Parent, 2000] for section 5.5.

5.1 Step 2

Throughout this part d will be an integer, $l \neq p$ two distinct primes with $p > 4$, K a number field of degree d, E an elliptic curve over K and $\mathcal{E}$ its Néron model over $\mathcal{O}_K$ and $P \in E(K)$ a point of prime order p such that these data together satisfy condition (v) of 3.2. This means that at all primes in $\mathcal{O}_K$ lying over l the elliptic curve E has split multiplicative reduction and P does not reduce to the identity component of the Néron model. Furthermore we will denote $E' := E/\langle P\rangle$ and $\beta\colon \mu_p \to E'$ the closed immersion sending μ_p to kernel of the dual isogeny of $E \to E'$. Now let $q \subset \mathcal{O}_K$ be a prime lying over l with residue field k. Since the order of P is coprime to l its specialization $P_k \in \mathcal{E}_k$ will also have order p. The special fiber at k of $\mathcal{E}$ will be a Néron np-gon for a certain n hence the Deligne-Rapoport specialisation of the generalized elliptic curve corresponding to E will be a Néron p-gon. So the generalized elliptic curve over $\mathcal{O}_K[1/p]$ corresponding to (E', β) will specialize to a Néron 1-gon at q. Rephrasing this in terms of points on $\mathcal{X}_\mu(p)$

and $\mathcal{X}_0(p)$ this means that if $s \in \mathcal{X}_\mu(p)(\mathcal{O}_K)$ [6] is the point coming from the pair (E', β) then the image of s in $\mathcal{X}_0(p)(\mathcal{O}_K)$ will specialize to $\infty_{\mathbb{F}_l}$. This proves the following proposition.

Proposition 5.1. *Let $p > 4$ be prime and H be a subgroup of $(\mathbb{Z}/p\mathbb{Z})^* \{\pm 1\}$. If there exists an elliptic curve E over a number field K of degree d, a point $P \in E(K)$ of order p and a prime $l \neq p$ which together satisfy (v) of 3.2 then there is a non cuspidal $s_{H,l} \in \mathcal{X}_H(p)(\mathcal{O}_K)$ whose image in $\mathcal{X}_0(p)$ specializes to ∞_k for all residue fields k of $\mathcal{O}_K$ of characteristic l.*

The next step is to make the above statement independent of the number field K by using the symmetric product. Let $\tau_1, \ldots, \tau_d$ be all embeddings of K into $\mathbb{C}$ and $s_{H,l}$ be as in the previous proposition then

$$s_{H,l}^{(d)} := \tau_1(s_{H,l}) + \cdots + \tau_d(s_{H,l}) \in \mathcal{X}_H(p)^{(d)}(\mathbb{Q})$$

because it is invariant under the action of the absolute Galois group of $\mathbb{Q}$. The proposition and the fact that the cusps of $\mathcal{X}_H(p)$ lying above $\infty \in \mathcal{X}_0(p)(\mathbb{Z})$ are defined over $\mathbb{Z}$ make sure we can write $s_{H,l,\mathbb{F}_l}^{(d)} = n_0\sigma_{0,\mathbb{F}_l} + \ldots + n_i\sigma_{i,\mathbb{F}_l}$ with the $\sigma_0, \ldots, \sigma_i$ pairwise distinct cusps in $\mathcal{X}_H(p)(\mathbb{Z})$ lying above infinity and $n_0 \geq \ldots \geq n_i \geq 1$ a sequence integers that sum to d. This shows that we can make the following definition.

Definition 5.2. Let d be an integer, $n_0 \geq n_1 \geq \ldots \geq n_i \geq 1$ a sequence of integers that sum to d and $\sigma_0, \ldots, \sigma_i$ pairwise distinct cusps in $\mathcal{X}_H$ that lie above $\infty \in \mathcal{X}_0$, then we call $n_0\sigma_0 + \ldots + n_i\sigma_i$ an **ordered sum of $\mathcal{X}_H(p)$ cusps (of degree d)**. Also if l is a prime, $s_{H,l}$ as in 5.1 and

$$s_{H,l,\mathbb{F}_l}^{(d)} = n_0\sigma_{0,\mathbb{F}_l} + \ldots + n_i\sigma_{i,\mathbb{F}_l}$$

then we call $n_0\sigma_0 + \ldots + n_i\sigma_i \mathcal{X}_H(p)^{(d)}(\mathbb{Z})$ the **(ordered) sum of cusps associated to** $s_{H,l,\mathbb{F}_l}^{(d)}$.

Remark. If $\mathcal{X}_H(p) = X_0(p)$ there is only one ordered sum of cusps that lie above infinity of degree d, namely $d\infty$. Hence in this case we have $s_{H,l,\mathbb{F}_l} = d\infty_{\mathbb{F}_l}$.

[6] We can put O_K here instead of $O_K[1/p]$ here since $\mathcal{X}_\mu(p)$ and $\mathcal{X}_0(p)$ are projective over $\mathbb{Z}$

5.2 Step 3

5.2.1 The winding quotient

Integration gives us a map

$$H_1(\mathcal{X}_H(\mathbb{C}), cusps, \mathbb{Z}) \to \hom_{\mathbb{C}}(H^0(\mathcal{X}_H(\mathbb{C}), \Omega^1), \mathbb{C}) \cong H_1(\mathcal{X}_H(\mathbb{C}), \mathbb{R}).$$

By a theorem of Manin and Drinfeld the image of this map is contained in $H_1(\mathcal{X}_H(\mathbb{C}), \mathbb{Q})$. Let $\{0, \infty\} \in H_1(\mathcal{X}_H(\mathbb{C}), cusps; \mathbb{Z})$ be the element coming from a path from 0 to $i\infty$ in the complex upper half plane.

Definition 5.3. The element $e := \omega \mapsto \int_{\{0,\infty\}} \omega \in H_1(X_H(N), \mathbb{Q})$ is called the winding element and the corresponding ideal $\mathcal{A}_e := \mathrm{Ann}(e) \subseteq \mathbb{T}$ consisting of the elements annihilating e is called the winding ideal. The quotient $J_H^e := J_H/\mathcal{A}_e J_H$ is called the winding quotient.

The most important property of the winding quotient that we will use is the following.

Theorem 5.4. *The rank of $J_H^e(\mathbb{Q})$ is 0.*

In [Parent, 1999] this theorem is proved for $J_0^e(N)$ using a result from [Kolyvagin and Logachëv, 1989]. This result states that an abelian variety A over $\mathbb{Q}$ that is a quotient of $J_0(N)_{\mathbb{Q}}$ has Mordel-Weil rank 0 if its analytic rank is zero. The result of Kolyvagin and Logachev was generalized by Kato [see Kato, 2004, cor. 14.3] to abelian varieties that are a quotient of $J_1(N)_{\mathbb{Q}}$. The theorem follows from using Kato's generalization in Parents proof. I will give here a short sketch of this proof.

Proof. Since we can view $J_{H,\mathbb{Q}}^e$ as a quotient of $J_\mu^e(N)_{\mathbb{Q}}$ it suffices to prove the theorem only for $J_\mu^e(N)_{\mathbb{Q}}$. The isomorphism $W_N \colon X_\mu(N) \to \mathcal{X}_1(N)$ is defined over $\mathbb{Q}$ and interchanges the cusp 0 with ∞ so this isomorphism sends the winding ideal to the winding ideal hence we get an isomorphism $J_\mu^e(N)_{\mathbb{Q}} \cong J_1^e(N)_{\mathbb{Q}}$. So instead of working with the alternate model $X_\mu(N)$ and its Jacobian we can also work with $X_1(N)$.

The Hecke algebra $\mathbb{T}_{\mathbb{Q}}$ viewed as sub algebra of the endomorphism ring of $S_2(\Gamma_1(N))_{\mathbb{Q}}$ can be written as

$$\mathbb{T}_{\mathbb{Q}} := R_{f_1} \times R_{f_2} \ldots \times R_{f_k}$$

where the f_i range over all Galois orbits of newforms for Γ_1 of level M_i dividing N and R_{f_i} is the restriction of $\mathbb{T}_{\mathbb{Q}}$ to the subspace $\mathcal{E}_{f_i}$ of $S_2(\Gamma_1(N))_{\mathbb{Q}}$ consisting of all elements that can be written as linear combinations of the

Galois conjugates of $B_d(f_i)$ with $d \mid N/M_i$ [see Parent, 1999, thm. 3.5] . Now let M be an integer that divides N and d an integer dividing N/M then degeneracy map $B_d\colon \mathcal{X}_1(N) \to \mathcal{X}_1(M)$ give rise to $B_d^*\colon J_1(M)_{\mathbb{Q}} \to J_1(N)_{\mathbb{Q}}$ and we can define $J_1(N)_{\mathbb{Q}}^{new} := J_1(N)_{\mathbb{Q}}/\Sigma_{M|N,d|M/N} \operatorname{im} B_d^*$. And we can use the maps $B_{d,*}\colon J_1(N)_Q \to J_1(M)_{\mathbb{Q}}$ to define a map of abelian varieties

$$\Phi\colon J_\mu(N)_{\mathbb{Q}} \to \oplus_{M|N} \oplus_{d|N/M} J_\mu(M)_{\mathbb{Q}}^{new}.$$

Now the identification

$$S_2(\Gamma_1(N))_{\mathbb{C}} \cong H^0(\mathcal{X}_1(N)_{\mathbb{C}}, \Omega^1) \cong H^0(J_1(N)_{\mathbb{C}}, \Omega^1) \cong \cot_0(J_1(N)_{\mathbb{C}}$$

together with the isomorphism $\oplus_{M|N} \oplus_{d|N/M} S^2(\Gamma_1(M))_{\mathbb{C}}^{new} \to S^2(\Gamma_1(M))_{\mathbb{C}}^{new}$ show that $\Phi_{\mathbb{C}}$ is an isogeny, so Φ is one also. We also have an isogeny $J_1(M)^{new} \to \oplus J_f$ where f runs over the Galois orbits of newforms in $S_2(\Gamma_1(N)$ and J_f is the abelian variety attached to such a Galois orbit. Combining these isogenies with Φ we get an isogeny

$$J_1(N)_{\mathbb{Q}} \to \bigoplus_i \bigoplus_{d|N/M_i} J_{f_i,\mathbb{Q}}.$$

where the f_i range over all Galois orbits of newforms for Γ_1 of level M_i dividing N. Define R^{f_i} as $\oplus_{i\neq j} R_{f_j}$ then the product $\oplus_{d|N/M_i} J_{f_i,\mathbb{Q}}$ will be isogenous to $J_1(N)_{\mathbb{Q}}/R^{f_i} J_1(N)_{\mathbb{Q}}$.

Now Parent shows that if the integration pairing $\langle e, f_i\rangle \neq 0$ that then $A_{e,\mathbb{Q}} \cap R_{f_i} = 0$ and conversely that if $\langle e, f_i\rangle = 0$ $A_{e,\mathbb{Q}} \cap R_{f_i} = R_{f_i}$. Now since $L(f_i, 1) = 2\pi\langle e, f_i\rangle$ we can write

$$A_{e,\mathbb{Q}} = \bigoplus_{i:L(f_i,1)=0} R_{f_i}.$$

Combining this with the previous discussion we get an isogeny

$$J_1^e(N) \to \bigoplus_{i:L(f_i,1)\neq 0} J_1^e(N)/R^{f_i} J_1^e(N) \to \bigoplus_{i:L(f_i,1)\neq 0} \oplus_{d|N/M_i} J_{f_i,\mathbb{Q}}$$

where the latter product has rank 0 by Kato's theorem. □

5.2.2 Using the winding quotient to make maps as in step 3

We can use the above theorem to construct maps $f\colon X_H(p)^{(d)} \to A$ for some abelian variety A such that $f(s_{H,l}^{(d)}) = f(\sigma)$ where $s_{H,l}$ is as in proposition 5.1 and σ is the ordered sum of cusp associated to $s_{H,l,\mathbb{F}_l}^{(d)}$. The most straightforward way is the following:

Corollary 5.5. *Let $l \neq 2$ be a prime and let $f\colon X_H(p)^{(d)} \to J_0^e(p)$ be the canonical map normalized by $f(\sigma) = 0$ then $f(s_{H,l}^{(d)}) = f(\sigma) = 0$*

Proof. Because $J_H^e(N)(\mathbb{Q})$ has rank 0 we know that $f(s_{H,l})$ is torsion. Because $l \neq 2$ we know that the torsion of $J_H^e(N)(\mathbb{Q})$ injects into $J_H^e(N)(\mathbb{F}_l)$. So because $s_{H,l,\mathbb{F}_l}^{(d)} = \sigma_{\mathbb{F}_l}$ we have that $f(s_{H,l}^{(d)}) = f(\sigma)_{\mathbb{F}_l} = 0$ and hence $f(s_{H,l}^{(d)}) = 0$. □

An approach similar to this one is taken using $l = 3$ in [Oesterlé, not published] to obtain formulas depending on the degree d that bound the order of a torsion point of prime order over a number field of degree d and $l = 3, 5$ in [Parent, 1999] to bound the order of points of prime power order.

However since the upper bounds in cases (i) trough (iv) of proposition 3.2 are better for smaller l one would really like to use $l = 2$. There are two difficulties when $l = 2$. The first one is that it is not necessarily true that the $J_H^e(N)(\mathbb{Q})$ injects into $J_H^e(N)(\mathbb{F}_2)$. And the second one arises during Step 4, because the exact sequence that relates $\cot J_H^e(N)_{\mathbb{F}_l}$ to $\cot J_H(N)_{\mathbb{F}_l}$ is not necessarily exact anymore. In [Parent, 2000] there is already a way of dealing with these difficulties when using $X_\mu(N)$. I will generalize his approach so one can use $X_H(N)$. The main reason for this is computational one, since it is more efficient to compute with for example $X_0(N)$ compared to $X_1(N)$. So for Step 3 we instead use the following corollary.

Corollary 5.6. *Let l be a prime, $s_{H,l} \in \mathcal{X}_H(p)(K)$ be as in proposition 5.1, σ the ordered sum of cusps associated to $s_{H,l}^{(d)}$ and let $f\colon \mathcal{X}_H(p)^{(d)} \to J_H(p)$ be the canonical map normalized by $f(\sigma) = 0$. Take $t_1, t_2 \in \mathbb{T}$ such that $t_1\colon J_H(p) \to J_H(p)$ factors via $J_H^e(p)$ and $t_2 = 1$ if $l \neq 2$ and if $l = 2$ then t_2 is such that it kills all μ_2 embeddings in $J_H(p)_{\mathbb{Z}[1/p]}$. Then*

$$t_2 \circ t_1 \circ f(s_{H,l}) = t_2 \circ t_1 \circ f(\sigma) = 0$$

.

Proof. Because $J_H^e(N)(\mathbb{Q})$ has rank 0 we know that $t_1 \circ f(s_{H,l}^{(d)})$ is torsion. Since we have $s_{H,l,\mathbb{F}_l}^{(d)} = \sigma_{\mathbb{F}_l}$ we have $t_1 \circ f(s_{H,l,\mathbb{F}_l}^{(d)}) = t_1 \circ f(\sigma_{\mathbb{F}_l}) = 0$ hence if $l \neq 2$ the injectivity of $J_0^e(N)(\mathbb{Q}) \hookrightarrow J_0^e(N)(\mathbb{F}_l)$ allows us to conclude that $t_1 \circ f(s_{H,l}^{(d)}) = 0$ and we are done. If $l = 2$ then [Parent, 2000, prop. 1.7] tells us that either $t_1 \circ f(s_{H,l}^{(d)}) = 0$ in which case we are done or $t_1 \circ f(s_{H,l}^{(d)})$ is a μ_2 embedding, in which case $t_2 \circ t_1 \circ f(s_{H,l}^{(d)}) = 0$ and we are also done. □

The operator t_2 as in the above corollary can be obtained using the following proposition.

Proposition 5.7. *Let p and q be two distinct primes then $(T_q - \langle q\rangle - q)(Q) = 0$*[7] *for all $Q \in J_H(p)(\mathbb{Q})$ with Q torsion of order coprime to q.*

Proof. Let $Q \in J_{H,\mathbb{Z}_{[1/p]}}(p)(\mathbb{Q})$ be torsion of order coprime to q, then $(T_q - \langle q\rangle - q)(Q)$ is also a point of order coprime to q. Now let $Q_{\mathbb{F}_q} \in J_H(p)_{\mathbb{F}_q}(\mathbb{F}_q)$ be its specialisation and let Frob_q be the Frobenius on $J_H(p)_{\mathbb{F}_q}$ and Ver_q its dual (verschiebung). Then we have the Eichler-Shimura relation $T_{q,\mathbb{F}_q} = \langle q\rangle \mathrm{Frob}_q + \mathrm{Ver}_q$ [see Diamond and Im, 1995, p. 87] and $\mathrm{Ver}_q \circ \mathrm{Frob}_q = q$ in $\mathrm{End}_{\mathbb{F}_q}(J_H(p)_{\mathbb{F}_q})$. So

$$T_{q,\mathbb{F}_q}(Q_{\mathbb{F}_q}) = \mathrm{Frob}_q(Q_{\mathbb{F}_q}) + \langle q\rangle \mathrm{Ver}_q(Q_{\mathbb{F}_q}) = \langle q\rangle Q_{\mathbb{F}_q} + qQ_{\mathbb{F}_q}$$

giving $(T_{q,\mathbb{F}_q} - \langle q\rangle - q)(Q_{\mathbb{F}_q}) = 0$. Since specializing a point on a group scheme can only change its order by a power of the characteristic of the residue field we see that the order of $(T_q - \langle q\rangle - q)(Q)$ must be a power of q, and coprime to q at the same time hence $(T_q - \langle q\rangle - q)(P) = 0$ □

So what we need now is to find a way to find Hecke operators t_1 as in the previous corollary. Now suppose if $t_1 \in \mathbb{T}$ is such that $t_1 A_e = 0$ then t_1 is a Hecke operator such that $t_1 \colon J_H(p) \to J_H(p)$ factors via $J_H^e(p)$. So Lemma 1.9 of [Parent, 1999] already gives a way of finding such Hecke operators for $J_\mu(p)$ as soon as we have found an element t that generates the Hecke algebra $\mathbb{T}_\mathbb{Q}$. The Hecke algebra $\mathbb{T}_\mathbb{Q}$ is of prime level and weight 2 so it is a product of number fields. In particular we know that such a t exists. By just trying "random" elements we should probably find such a t reasonably fast. But testing whether t is a generator requires calculating its minimal polynomial, which is a computationally expensive task if t is represented by a huge matrix, so we don't want to try many different t. Therefore we generalize his Lemma slightly such that we don't need t to be a generator.

Proposition 5.8. *Let $t \in \mathbb{T}_{\Gamma_H}$ be an element and let $P(X) = \prod_{i=1}^n P_i(X)^{e_i}$ its factorized characteristic polynomial when viewing t as an element of* $\mathrm{End}\, S_2(\Gamma_1(N))_\mathbb{Q}$. *Define*

$$I := \{i \in \{1, \ldots, n\} \mid P/P_i^{e_i}(t)e = 0 \text{ or } e_i > 1\}$$

then $t_1(t) := \prod_{i\in I} P_i^{e_i}(t)$ is such that $t_1 A_e = 0$.

Proof. We have already seen that the Hecke algebra $\mathbb{T}_{\Gamma_H,\mathbb{Q}}$ viewed as sub algebra of the endomorphism ring of $S_2(\Gamma_H)_\mathbb{Q}$ can be written as

$$\mathbb{T}_{\Gamma_H,\mathbb{Q}} := R_{f_1} \times R_{f_2} \ldots \times R_{f_k}$$

[7] This is slightly different from [Parent, 2000, prop. 1.8], in that proposition it should also read $a_q := T_q - \langle q\rangle - q$. The mistake in that paper comes from Parent using the Eichler-Shimura relation for the $\mathcal{X}_1(N)$ model of $X_1(N)$ while in his article he is only working with the $\mathcal{X}_\mu(N)$ model. For more details on the Eichler-Shimura relations corresponding to the different models see page 87 of [Diamond and Im, 1995]

where the f_i range over all Galois orbits of newforms for Γ_H of level M_i dividing N and the R_{f_i} are the restriction of $\mathbb{T}_{\Gamma_H,\mathbb{Q}}$ to certain subspaces $\mathcal{E}_{f_i}$ of $S_2(\Gamma_{\Gamma_H,\mathbb{Q}})_{\mathbb{Q}}$. And we have also seen that $A_{e,\mathbb{Q}} = \oplus_{i:L(f_i,1)=0} R_{f_i}$. Now define $\mathcal{E}_e := \oplus_{i:L(f_i,1)=0}\mathcal{E}_{f_i}$ and $\mathcal{E}_e^{\perp} := \oplus_{i:L(f_i,1)\neq 0}\mathcal{E}_{f_i}$ then $S_2(\Gamma_H)_{\mathbb{Q}} = \mathcal{E}_e \oplus \mathcal{E}_e^{\perp}$ and $A_{e,\mathbb{Q}} := \left\{t' \in \mathbb{T}_{\mathbb{Q}} \mid t'|_{\mathcal{E}_e^{\perp}} = 0\right\}$ so in particular $t_1 A_{e,\mathbb{Q}} = 0$ if $t_1|_{\mathcal{E}_e} = 0$. So it suffices to show that $t_1|_{\mathcal{E}_{f_i}} = 0$ for all i such that $L(f_i, 1) = 0$. Now all $\mathcal{E}_i$ are contained in some generalized eigenspace corresponding to the factor $P_{j_i}^{e_{j_i}}$ for some j_i depending on i. Now for the i such that $e_{j_i} > 1$ we have $P_{j_i}^{e_{j_i}}(t)|\mathcal{E}_{f_i} = 0$ so $t_1|\mathcal{E}_{f_i} = 0$. For the other i we have $e_{j_i} = 1$ and in particular $\mathcal{E}_{f_i} = \ker P_{j_i}(t)$ so that we have $P/P_{j_i}(t) \in R_i$, now $L(f_i, 1) = 0$ implies $P/P_{j_i}(t)e = 0$ hence $j_i \in I$ and hence $t_1|_{\mathcal{E}_{f_i}} = t_1|_{\ker P_{j_i}(t)} = 0$ □

5.3 step 4

The goal of this section is to define what a formal immersion is and give a criterion that implies that the map $t_2 \circ t_1 \circ f \colon \mathcal{X}_H(p)^{(d)} \to J_H(p)$ as in corollary 5.6 is a formal immersion at $\sigma_{\mathbb{F}_l}$. To be precise we will prove the following variant of Kamienny's Criterion which is a slight generalization of the variant that can be found as [Parent, 2000, prop. 2.8].

Proposition 5.9 (Kamienny's Criterion)**.** *Let $\sigma = n_0\sigma_0 + \ldots + n_k\sigma_k$ be an ordered sum of cusps of $\mathcal{X}_H(p)$ of degree d such that the σ_i all lie above $\infty \in X_0(p)$. Let $\langle d_0\rangle, \ldots, \langle d_k\rangle \in (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}/H$ be the diamond operators such that $\sigma_0 = \langle d_i\rangle\sigma_i$. Let $f \colon X_H(p)^{(d)} \to J_H(p)$ be the canonical map normalized by $f(\sigma) = 0$ and let $t \in \mathbb{T}_{\Gamma_H}$ then $t \circ f$ is a formal immersion at $\sigma_{\mathbb{F}_l}$ if and only if the d Hecke operators*

$$\left(t\langle d_i\rangle T_j\right)_{\substack{i\in 0,\ldots,k \\ j\in 1,\ldots,n_i}}$$

are $\mathbb{F}_l$ linearly independent in $\mathbb{T}_{\Gamma_H} \otimes \mathbb{F}_l$.

Before we proof this proposition we first develop the theory necessary to prove it.

5.3.1 Formal Immersions

Definition / Proposition 5.10 (Formal Immersion)**.** *Let $\phi \colon X \to Y$ be a morphism of noetherian schemes and $x \in X$ be a point which maps to $y \in Y$. Then ϕ is a formal immersion at x if the two following equivalent conditions hold:*

- *the induced morphism of the complete local rings $\widehat{\phi^*} \colon \widehat{\mathcal{O}_{Y,y}} \to \widehat{\mathcal{O}_{X,x}}$ is surjective.*

- *The maps $\phi\colon k(y) \to k(x)$ and $\phi^*\colon \cot_y(Y) \to \cot_x(X)$ are both surjective.*

Proof. It is clear that the first condition implies the second. The other implication can be proved by using Nakayama's lemma to lift a basis of $\cot_y(Y)$ to a set of generators $f_1, \ldots, f_n$ of m_y, the maximal ideal of $\widehat{\mathcal{O}_{Y,y}}$. The fact that $\widehat{\phi^*}(f_1), \ldots, \widehat{\phi^*}(f_n)$ generate $m_x/(m_x^2)$ implies that $\widehat{\phi^*}(f_1), \ldots, \widehat{\phi^*}(f_n)$ also generate m_x, as a consequence we get that for i the map $m_y^i/m_y^{i+1} \to m_x^i/m_x^{i+1}$ is surjective, hence by the completeness of $\widehat{\mathcal{O}_{Y,y}}$ we also have that $\widehat{\phi^*}$ is surjective. □

There is one important property of formal immersions that we will use and that is the following.

Proposition 5.11. *Let X, Y be noetherian schemes. Let R be a discrete valuation ring, m be its maximal ideal and $k = R/m$ be its residue field. Suppose $\phi\colon X \to Y$ is morphism of schemes that is a formal immersion at a point $x \in X(k)$ and suppose $P, Q \in X(R)$ are two points such that $x = P_k = Q_k$ and $f(P) = f(Q)$. Then $P = Q$.*

Proof. Let $y = f(x)$ and view P, Q as morphisms $\operatorname{Spec} R \to X$ and hence write $f \circ P$ instead of $f(P)$. The morphisms P, Q and f induce maps on the local rings, call these P_m^*, Q_m^* and f_x^* respectively:

$$\begin{array}{ccccc} R & \underset{Q_m^*}{\overset{P_m^*}{\leftleftarrows}} & \mathcal{O}_{X,x} & \xleftarrow{f_x^*} & \mathcal{O}_{Y,y} \\ \downarrow & & \downarrow & & \downarrow \\ \widehat{R} & \underset{\widehat{Q_m^*}}{\overset{\widehat{P_m^*}}{\leftleftarrows}} & \widehat{\mathcal{O}_{X,x}} & \xleftarrow{\widehat{f_x^*}} & \widehat{\mathcal{O}_{Y,y}} \end{array}$$

Since $f \circ P = f \circ Q$ we also know that $\widehat{P_m^*} \circ \widehat{f_x^*} = \widehat{Q_m^*} \circ \widehat{f_x^*}$. Now f is a formal immersion at x. This means $\widehat{f_x^*}$ is surjective and hence that $\widehat{P_m^*} = \widehat{Q_m^*}$. Now since $R \to \widehat{R}$ is injective we also get $P_m^* = Q_m^*$. The proposition now follows from the following commuting diagrams:

$$\begin{array}{ccc} & & X \\ & \overset{P}{\nearrow} & \uparrow \\ \operatorname{Spec} R & \xrightarrow{P_m} & \operatorname{Spec} \mathcal{O}_{X,x} \end{array} \qquad \begin{array}{ccc} & & X \\ & \overset{Q}{\nearrow} & \uparrow \\ \operatorname{Spec} R & \xrightarrow{Q_m} & \operatorname{Spec} \mathcal{O}_{X,x} \end{array}$$

□

This proposition will be applied later in the setting of 5.6 with $P = s_{H,l}^{(d)}$ and $Q = \sigma$ to show $s_{H,l}^{(d)} = \sigma$.

5.3.2 Proof of 5.9 (Kamienny's Criterion)

The general proof for this proposition involves some slightly more involved notation then the proof for the case $\mathcal{X}_H = \mathcal{X}_0(p)$. However all the main ideas are already in the proof for the case $\mathcal{X}_H = X_0(p)$. So for better understandability we will prove the criterion only for $\mathcal{X}_0(p)$. For a full proof of the proposition one can just check that the proof of proposition 2.8 in [Parent, 2000] given for the case $\mathcal{X}_H = \mathcal{X}_\mu(p)$ copies over verbatim to this slightly more general situation. In proving the main result of this thesis (theorem 3.1) I only used the criterion 5.9 with either $\mathcal{X}_H = \mathcal{X}_\mu(p)$ or $\mathcal{X}_H = \mathcal{X}_0(p)$.

First we restate the proposition 5.9 in the case $\mathcal{X}_H = \mathcal{X}_0(p)$ since the proposition itself also becomes easier.

Proposition 5.12. *Let $f\colon \mathcal{X}_0(p)^{(d)} \to J_0(p)$ be the canonical map normalized by $f(\infty^{(d)}) = 0$ and let t be a Hecke operator then $t \circ f$ is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ if and only if the d Hecke operators*

$$T_1 t, \ldots, T_d t$$

are $\mathbb{F}_l$ linearly independent in $\mathbb{T}_{\Gamma_0(p)} \otimes \mathbb{F}_l$.

Proof. We have $k(t \circ f(\infty_{\mathbb{F}_l}^{(d)})) = k(0_{\mathbb{F}_l}) = \mathbb{F}_l = k(\infty_{\mathbb{F}_l}^{(d)})$ so we only need to check that the linear independence criterion is equivalent to

$$(t \circ f)^*\colon \operatorname{cot}_{0_{\mathbb{F}_l}}(J_0(p)) \to \operatorname{cot}_{\infty_{\mathbb{F}_l}^d} \mathcal{X}_0(p)^{(d)}$$

being surjective.

Now let q be the standard formal coordinate at $\infty_{\mathbb{Z}_l}$. Then $\widehat{\mathcal{O}}_{X_0(p),\infty_{\mathbb{Z}_l}} = \mathbb{Z}_l[[q]]$. Let q_i denote the formal coordinate at $\infty_{\mathbb{Z}_l}^d$ corresponding to the i-th factor of $X_0(p)_{\mathbb{Z}_l}^d$ then

$$\widehat{\mathcal{O}}_{X_0(p)^{(d)},\infty_{\mathbb{Z}_l}^{(d)}} = \mathbb{Z}_l[[q_1, \ldots, q_d]]^{S_d} = \mathbb{Z}_l[[\sigma_1, \ldots, \sigma_d]]$$

where $\sigma_1 = q_1 + \cdots + q_d$, $\sigma_2 = \ldots$ and $\sigma_d = q_1 q_2 \cdots q_d$ are the elementary symmetric functions in $q_1, \ldots, q_d$. So we see that $d\sigma_1, \ldots, d\sigma_d$ form an $\mathbb{Z}_l$ basis of $\operatorname{cot}_{\infty_{\mathbb{Z}_l}^{(d)}} \mathcal{X}_0(p)^{(d)}$.

Let $F\colon \mathcal{X}_0(p) \to J_0(p)$ be the canonical map normalized by $F(\infty) = 0$ then the isomorphism $H^0(\mathcal{X}_0(p)_{\mathbb{Z}_l}, \Omega^1) \xrightarrow{(F^*)^{-1}} H^0(J_0(p)_{\mathbb{Z}_l}, \Omega^1) \to \operatorname{cot}_{0_{\mathbb{Z}_l}}(J_0(p))$

allows us to associate to an element $\omega \in \cot_{0_{\mathbb{Z}_l}}(J_0(p))$ the q-expansion of $F^*(\omega)$ on $X_0(p)_{\mathbb{Z}_l}$. In fact this q-expansion determines ω uniquely. For an element $\omega \in \cot_{0_{\mathbb{Z}_l}}(J_0(p))$ we denote this q-expansion by $\sum_{i=1}^{\infty} a_i(\omega) q^i dq/q$. Now let $\pi\colon X_0(p)^d \to X_0(p)^{(d)}$ be the canonical map then

$$\pi^*((t \circ f)^*(\omega)) = \pi^* \circ f^*(t\omega) = \sum_{i=1}^{d} \sum_{n=1}^{\infty} a_n(t\omega) q_i^n dq_i/q_i =$$

$$= \sum_{n=1}^{\infty} a_n(t\omega) ds_n/n \in H^0(X_0(p)^d_{\mathbb{Z}_l}, \Omega^1)$$

where $s_n = \sum_{i=1}^{d} q_i^n$. Now for ease of notation define $\sigma_n = 0$ for all $n > d$. Then Newtons identities give for all $n \geq 0$:

$$s_n - \sigma_1 s_{n-1} + \sigma_2 s_{n-2} - \ldots + (-1)^{n-1} \sigma_{n-1} s_1 = (-1)^{n-1} n \sigma_n.$$

Since for $n \geq 2$ and $1 \leq i \leq n-1$ we have $d(\sigma_i s_{n-i}) = 0$ in $\cot_{\infty^d_{\mathbb{Z}_l}} \mathcal{X}_0(p)^{(d)}$ we get for $n \geq 1$ that $ds_n/n = (-1)^{n-1} d\sigma_n$ where the latter is zero if $n > d$. In particular we see that

$$(t \circ f)^*(\omega) = \sum_{n=1}^{d} a_n(t\omega)(-1)^{n-1} d\sigma_n =$$

$$= \sum_{n=1}^{d} a_1(T_n t\omega)(-1)^{n-1} d\sigma_n \quad \text{in } \cot_{\infty^{(d)}_{\mathbb{Z}_l}} \mathcal{X}_0(p)^{(d)}.$$

Reducing mod l shows that this relation also holds in $\cot_{\infty^{(d)}_{\mathbb{F}_l}} \mathcal{X}_0(p)^{(d)}$. Now since we can identify

$$S_2(\Gamma_0(p), \mathbb{F}_l) \cong H^0(X_0(p)_{\mathbb{F}_l}, \Omega^1) \cong \cot_{0_{\mathbb{F}_l}}(J_0(p))$$

and the pairing

$$S_2(\Gamma_0(p), \mathbb{F}_l) \times (\mathbb{T}_{\Gamma_0(p)} \otimes \mathbb{F}_l) \to \mathbb{F}_l$$

given by $(f, t') \mapsto a_1(t'f)$ is perfect we also see that the pairing

$$\cot_{0_{\mathbb{F}_l}}(J_0(p)) \times (\mathbb{T}_{\Gamma_0(p)} \otimes \mathbb{F}_l) \to \mathbb{F}_l$$

given by $(\omega, t') \mapsto a_1(t'\omega)$ is perfect. This means that if $T_1 t, \ldots T_d t \in \mathbb{T}_{\Gamma_0(p)} \otimes \mathbb{F}_l$ are $\mathbb{F}_l$ linearly independent then we can find $\omega_1, \ldots, \omega_d \in \cot_{0_{\mathbb{F}_l}}(J_0(p))$ such that $(t \circ f)^*(\omega_i) = d\sigma_i$. So we have shown one direction of the if and only if statement. The other direction is also clear, any linear relation between $T_1 t, \ldots T_d t$ will also give a linear relation between

$$a_1(T_1 t\omega)(-1)^{1-1}, \ldots, a_1(T_n t\omega)(-1)^{n-1}$$

that holds for all $\omega \in \cot_{0_{\mathbb{F}_l}}(J_0(p))$. $\square$

5.4 Putting it all together

Having completed all steps in the previous sections we can put them together to obtain the following version of Kamienny's criterion that helps us rule out case (v) of 3.2.

Theorem 5.13. *Let l, p be distinct primes, d an integer and $H \subseteq (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ be a subgroup. Suppose that for all partitions $d = n_0 + \cdots + n_k$ with*

$$n_0 \geq n_1 \geq \cdots \geq n_k$$

and all sets of pairwise distinct elements $\langle d_0\rangle, \ldots, \langle d_k\rangle \in (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}/H$ there are Hecke operators t_1 and t_2 in $\mathbb{T}_{\Gamma_H}$ as in 5.6 (i.e. $t_1 A_e = 0$ and if $l = 2$ then t_2 kills all μ_2 immersions in J_H) and that the d elements

$$\left(t_1 t_2 \langle d_i\rangle T_j\right)_{\substack{i\in 0,\ldots,k \\ j\in 1,\ldots,n_i}} \tag{5.4.1}$$

considered as elements $\mathbb{T}_{\Gamma_H}\otimes\mathbb{F}_l$ are $\mathbb{F}_l$ linearly independent. Then $p \notin S_l^{(v)}(d)$.

Note that we switched some quantifiers with respect to theorem 1.10 of [Parent, 2000]. In that version the t_1 and t_2 are not allowed to depend on the partition of d and the $\langle d_i\rangle$ while in this criterion they are allowed to depend on this. Further on we will not need this slightly stronger version of the theorem but this slight change of formulation might be useful if someone wants to check this criterion in other cases.

As an example I describe the easiest case, namely when $H = (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$.

Example 1. Suppose that there are Hecke operators t_1 and t_2 in $\mathbb{T}_{\Gamma_0}$ as in 5.6 such that the d elements

$$t_1 t_2 T_1, \ldots, t_1 t_2 T_d$$

considered as elements in $\Gamma_0\otimes\mathbb{F}_l$ are $\mathbb{F}_l$ linearly independent. Then $p \notin S_l^{(v)}(d)$.

In this example there is only 1 linear independency that we have to check. While in the case $H = 1$ there will be many. This means that when actually verifying the criterion we would much rather use $H = (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ than $H = 1$. This works in a lot of cases but sometimes we really have to use $H = 1$ because $H = (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ does not work. A way of making it computationally faster to check the criterion in the case $H = 1$ will therefore be discussed in the next section. But first we will prove the theorem.

Proof. Suppose for all partitions of d and all choices of $\langle d_i \rangle$ that there are t_1 and t_2 such that the d elements in equation 5.4.1 are $\mathbb{F}_l$ linearly independent. And assume for contradiction that also $p \in S_l^{(v)}(d)$. Now let E be an elliptic curve over a number field K of degree d and $P \in E(K)$ a point of order p satisfying (v) of proposition 3.2 and $s_{H,l} \in X_H(O_K)$ the point coming from the pair (E, P) as in proposition 5.1. Also let $\sigma = n_0\sigma_0 + \ldots + n_i\sigma_i$ be the ordered sum of cusps associated to $s^{(d)}_{H,l,\mathbb{F}_l}$ and $f\colon \mathcal{X}_H \to J_H$ be the canonical map normalized by $f(\sigma) = 0$. Then by 5.6 we have $t_1 \circ t_2 \circ f(s^{(d)}_{H,l}) = t_1 \circ t_2 \circ f(\sigma)$. Now let $\langle d_0 \rangle, \ldots, \langle d_k \rangle$ be as in proposition 5.9. Because the linear independence criterion is satisfied we get that $t_1 \circ t_2 \circ f$ is a formal immersion at $\sigma_{\mathbb{F}_l}$, but this means that $s^{(d)}_{H,l} = \sigma$ contradicting the fact that $s^{(d)}_{H,l}$ comes from an elliptic curve with a point of order p. So $p \notin S_l^{(v)}(d)$. □

5.5 Making Kamienny's criterion for $X_\mu(p)$ faster

As we have already seen Kamienny's criterion for $\mathcal{X}_\mu(p)$ requires the testing of a lot of linear independence relations while Kamienny's criterion for $\mathcal{X}_0(p)$ requires testing only 1 linear independence relation. To be more precise what we mean by a lot, suppose that d is the degree and p is the torsion order for which we want to check the Kamienny's criterion and we only consider the ordered sums of cusps $n_0\sigma_0, \ldots, n_i\sigma_i$ where the multiplicities $n_0, \ldots, n_i$ are all equal to 1 (hence $i = d - 1$) then there are already $\binom{(p-3)/2}{d-1}$ different linear independencies we need to verify. So when doing actual computations using a computer we rather use $\mathcal{X}_0(p)$ instead of $\mathcal{X}_\mu(p)$ whenever possible. It turned out while doing the explicit computations that the $\mathcal{X}_0(p)$ version of the criterion sometimes fails for primes which are too big to make it practical to just try the $\mathcal{X}_\mu(p)$ criterion for all possible ordered cups sums. For example I was unable to find t_1 and t_2 such that the $\mathcal{X}_0(p)$ version of the criterion was satisfied for $d = 7$ and $p = 193$. In this case the $\mathcal{X}_\mu(p)$ version would require verifying more than 869 million linear independencies and the matrices involved are 1457 by 1457. But luckily we can do something smarter.

We again restrict our attention to the ordered sums of cusps $n_0\sigma_0 + \cdots + n_i\sigma_i$ where the multiplicities $n_0, \ldots, n_i$ are all equal to 1. Checking Kamienny's criterion for all these sums of cusps comes down to checking whether

$$T_1\langle d_0 \rangle t, \ldots, T_1\langle d_i \rangle t$$

are linearly independent for each set of pairwise distinct diamond operators $\langle d_0 \rangle, \ldots, \langle d_i \rangle$ where the first one is the identity. However, equivalently we can also check that all linear dependencies over $\mathbb{F}_l$ between the Hecke operators $T_1\langle 1 \rangle t, \ldots, T_1\langle (p-1)/2 \rangle t$ involve at least $d+1$ nonzero coefficients. It turned

out that the dimension of this space of linear dependencies was often zero or of very low dimension, so it takes no time at all to use a brute force approach and just calculate the number of nonzero coefficients of all linear dependencies. The following lemma generalizes this example to the case where the $n_0, \ldots, n_i$ are not necessarily equal to 1. This trick makes it more feasible to check the $\mathcal{X}_\mu(p)$ version of the criterion on the computer.

Lemma 5.14. *Let d be an integer and $t \in \mathbb{T}_{\Gamma_1(p)}$. Define for all integers r the following multiset*

$$D_r := \{\!\{t\langle 1\rangle T_j \mid d - r < j \leq r\}\!\} \uplus \{\!\{t\langle k\rangle T_j \mid 1 \leq j \leq d-r, 1 \leq k \leq \frac{p-1}{2}\}\!\}$$

where T_i denotes the i'th Hecke operator in $\mathbb{T}_{\Gamma_1(p)}$. Suppose that for all r with $\lfloor \frac{d}{2} \rfloor \leq r \leq d$ the multiset D_r does not contain a sub-multiset of size d which is linearly dependent over $\mathbb{F}_l$. Then $t \circ f \colon \mathcal{X}_\mu(p)^{(d)} \to J_\mu(p)$ is a formal immersion at $\sigma_{\mathbb{F}_l}$ for all ordered sums of cusps $\sigma := n_0\sigma_0 + \cdots + n_k\sigma_k$ of degree d with the σ_i lying above $\infty \in \mathcal{X}_0(p)$.

Proof. Suppose that there is an ordered cusp sum $\sigma := n_0\sigma_0 + \cdots + n_k\sigma_k$ of degree d such that $t \circ f$ is not a formal immersion at $\sigma_{\mathbb{F}_l}$. Then write $\sigma_0 = \langle d_k\rangle\sigma_k$ for some integers $1 \leq d_0, d_1, \ldots, d_k \leq (p-1)/2$ then by 5.9 we see that the d vectors in the following multiset

$$S := \{\!\{t\langle d_i\rangle T_j \mid 0 \leq i \leq k,\ 1 \leq j \leq n_i\}\!\}$$

are $\mathbb{F}_l$ linearly dependent in $\mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{F}_l$. We know that

$$\min(n_0, d - n_0) \geq n_1 \geq n_2 \geq \ldots \geq n_i.$$

So if $n_0 \geq \lfloor \frac{d}{2} \rfloor$ then $S \subseteq D_{n_0}$ and if $n_0 \leq \lfloor \frac{d}{2} \rfloor$ then $S \subseteq D_{d-n_0}$ so both cases lead to a contradiction. □

5.6 Testing the criterion

Using a computer program written in Sage I first tested the criterion for $\mathcal{X}_0(p)$. The program and the output generated by it will be available at `http://www.math.leidenuniv.nl/nl/theses/`, the location where this thesis is published. The results of testing the criterion are summarised in the following propositions.

Proposition 5.15. *If $p = 131, 139, 149, 151, 167, 173, 179, 181, 191$ or p is a prime with $193 < p < 2282$ then there are $t_1, t_2 \in \mathbb{T}_{\Gamma_0(p)}$ as in 5.6 such that $t_1t_2T_1, \ldots, t_1t_2T_7$ are $\mathbb{F}_2$ linearly independent in $\mathbb{T}_{\Gamma_0(p)} \otimes \mathbb{F}_2$.*

Proof. I tested the criterion for all $17 \leq p \leq 2282$ using different choices of t_1 and t_2. I tried $t_1 = t_1(t)$ (see proposition 5.8) using $t = T_2, \ldots, T_{60}$. And I tried $t_2 = T_q - q - 1$ for all primes $2 < q < 20$ with $q \neq p$. For all primes mentioned above I found at least one pair t_1, t_2 such that the linear independence holds. The total time used was about 2 hours when checking the criterion for about 8 primes in parallel so it could be used to check the criterion for bigger d and p[8]. □

Testing the fast version of the criterion for $X_\mu(p)$ gives the following proposition:

Proposition 5.16. *For all pairs (p, d) with p a prime $17 \leq p \leq 193$ and $3 \leq d \leq 7$ not satisfying any of the following conditions:*

- *$d = 3$ and $p \in \{17\}$*
- *($d = 4$ or $d = 5$) and $p \in \{17, 19, 29\}$*
- *($d = 6$ or $d = 7$) and $p \in \{17, 19, 23, 29, 31, 37\}$*

there are t_1 and t_2 as in proposition 5.6 such that for $t = t_1 t_2$ the D_r as in lemma 5.14 do not contain a subset of size d which is linearly dependent over $\mathbb{F}_2$.

Proof. This was again verified using the computer. This time I tried $t_1 = t_1(t)$ using $t = T_2, \ldots, T_{20}$ and I tried $t_2 = T_q - q - \langle q \rangle$ for the primes $2 < q < 20$ only trying new choices of t_1 and t_2 if no succesful pair combination of t_1 and t_2 had been found yet. The most time was spend on the case $p = 193$ which took about 14 hours.[8]And that while only one combination of t_1 and t_2 was tried since $t_1 = t_1(T_2)$ and $t_2 = T_3 - 3 - \langle 3 \rangle$ already gave the desired result. □

Because $\lfloor (3^{7/2} + 1)^2 \rfloor = 2281$ these computations together with 5.13 immediately give the following result .

Corollary 5.17. *If* $\max(S(7)) \leq 2281$ *then the inclusions of sets as listed in table 5.1 hold.*

[8]This is not a very precise timing and meant for indicative purposes only.

$$S_2^{(v)}(3) \subseteq \text{Primes}(17)$$
$$S_2^{(v)}(4) \subseteq \text{Primes}(19) \cup \{29\}$$
$$S_2^{(v)}(5) \subseteq \text{Primes}(19) \cup \{29\}$$
$$S_2^{(v)}(6) \subseteq \text{Primes}(41)$$
$$S_2^{(v)}(7) \subseteq \text{Primes}(41)$$

Table 5.1: Some bounds on $S_2^{(v)}(d)$.

The computations for this thesis where done using Sage 5.2 [Stein et al., 2012] and Magma 2.17-8 [Bosma et al., 1997].

A Calculations of the $\mathbb{F}_2$ gonality of $\mathcal{X}_1(N)$ using Magma

The calculations in this section are all based on proposition 2.14. What is calculated is the minimum occurring in that proposition for d large enough to prove the needed lower bound on the gonality. Upper bounds will follow from actually finding functions of low degree during these computations. The set S of divisors that dominate all functions of degree $\leq d$ needed for proposition 2.14 is obtained by applying 2.16 to the set $S_{d-n} + D$ obtained by using proposition 2.15.

Throughout the entire calculation I will use the fact that the diamond operators act transitively on $\mathcal{X}_1(N)(\mathbb{F}_2)$ as soon as $\#\mathcal{X}_1(N)(\mathbb{F}_2) = \#(\mathbb{Z}/N\mathbb{Z})^* \{\pm 1\}$. This is because this means that the elements of $\mathcal{X}_1(N)(\mathbb{F}_2)$ are precisely the cusps corresponding to the Néron N-gons. This allows us to use 2.16 to reduce the size of $S_{d-n} + D$ a factor slightly smaller then $\#(\mathbb{Z}/N\mathbb{Z})^* / \{\pm 1\}$.

For the calculation we use one custom function. It takes as input a divisor and gives as output the degrees of all nonzero functions in the associated Riemann-Roch space. The magma code of this function is as follows:

```
function FunctionDegrees(divisor)
    space,map := RiemannRochSpace(divisor);
    return [Degree(map(i)) : i in space | i ne 0 and map(i) ne 1];
end function;
```

The files x1_N.m , which are loaded in the magma code below, have the following structure:

```
A<x,y> := PolynomialRing(GF(2),2);
P,homogenize := Homogenization(A);
f := x^13+x^12*y+...; \\this line contains an equation for X_1(N)
f := homogenize(f);
XF2 := Scheme(ProjectiveSpace(P),f);
FF := FunctionField(XF2);
AFF := AlgorithmicFunctionField(FF);
plc1 := Places(AFF,1);
divgrp := DivisorGroup(AFF);
div1 := [divgrp ! i : i in plc1];
cuspsum := &+ div1;
```

The equations were taken from `http://www-math.mit.edu/~drew/X1_curves.txt`. The files x1_N.m are part of the supplementary files published together with this thesis at `http://www.math.leidenuniv.nl/nl/theses/`.

Most commands below are finished in a matter of seconds. For $N = 29, 31$ there are a few commands that take about a minute. For $N = 31$ there is one command that takes up 12 minutes, so this is where most of the computing time is spend.

A.1 $N = 17$

```
> load "x1_17.m";
Loading "x1_17.m"
> [#Places(AFF,i) : i in [1..10]];
[ 8, 0, 0, 3, 8, 8, 8, 33, 64, 92 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(8/3)=3 so S=S_{3-3}+cuspsum={cuspsum}
> //dominates all functions of deg <=3
> Min(FunctionDegrees(cuspsum));
4 1
> //minimum is 4 at index 1 so indeed there are no degree <=3 maps!
```

A.2 $N = 19$

```
> load "x1_19.m";
Loading "x1_19.m"
> [#Places(AFF,i) : i in [1..10]];
[ 9, 0, 0, 0, 9, 13, 18, 27, 38, 117 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(9/3)=3 so S=S_{4-3}+cuspsum
> //dominates all functions of deg <=4
> //Case cuspsum+p with p a place of degree 1.
> //We can assume p=div1[1].
> Min(FunctionDegrees(cuspsum+div1[1]));
5 1
> //minimum is 5 at index 1 so indeed there are no degree <=4 maps!
```

A.3 $N = 21$

```
> load "x1_21.m";
Loading "x1_21.m"
> [#Places(AFF,i) : i in [1..10]];
[ 6, 3, 2, 1, 6, 1, 18, 42, 48, 99 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(6/3)=2 so S=S_{3-2}+cuspsum
> //dominates all functions of deg <=3
> //Case  cuspsum+p with p a places of degree 1.
```

```
> //We can assume p=div1[1].
> Min(FunctionDegrees(cuspsum+div1[1]));
4 3
> //minimum is 4 at index 3 so indeed there are no degree <=3 maps!
```

A.4 $N = 23$

```
> load "x1_23.m";
Loading "x1_23.m"
> [#Places(AFF,i) : i in [1..10]];
[ 11, 0, 0, 0, 0, 0, 33, 33, 55, 88 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(11/3)=4 so S=S_{6-4}+cuspsum
> //dominates all functions of deg <=4
> //Case cuspsum+p+q with p,q places of degree 1.
> //We can assume p=div1[1].
> Min(&cat[FunctionDegrees(cuspsum+div1[1]+q) : q in div1]);
7 7
> //minimum is 7 at index 7 so indeed there are no degree <=6 maps!
```

A.5 $N = 25$

```
> load "x1_25.m";
Loading "x1_25.m"
> [#Places(AFF,i) : i in [1..10]];
[ 10, 0, 0, 2, 1, 5, 10, 45, 50, 121 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(10/3)=4 so S=S_{4-4}+cuspsum={cuspsum}
> //dominates all functions of deg <=4
> FunctionDegrees(cuspsum);
[ 5, 5, 10, 10, 5, 5 ]
> //minimum is 5 so indeed there are no degree <=4 maps!
```

A.6 $N = 27$

```
> load "x1_27.m";
Loading "x1_27.m"
> [#Places(AFF,i) : i in [1..10]];
[ 9, 3, 0, 0, 0, 10, 9, 18, 92, 99 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(9/3)=3 so S=S_{5-3}+cuspsum
> //dominates all functions of deg <=5
> //Case cuspsum+p+q with p,q distinct places of degree 1.
```

```
> //We can assume p=div1[1].
> Min(&cat[FunctionDegrees(cuspsum+div1[1]+q) : q in div1]);
6 1
> //Case D' = p with p a place of degree 2.
> Min(&cat[FunctionDegrees(cuspsum+p) : p in Places(AFF,2)]);
6 1
> //minimum is 6 so indeed there are no degree <=5 maps!
```

A.7 $N = 29$

```
> load "x1_29.m";
Loading "x1_29.m"
> [#Places(AFF,i) : i in [1..10]];
[ 14, 0, 0, 0, 0, 21, 17, 28, 56, 119 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(14/3)=5 so S=S_{10-5}+cuspsum
> //dominates all functions of deg <=10
> //Case cuspsum+4p+q with p,q places of degree 1.
> //We can assume p=div1[1].
> Min(&cat [FunctionDegrees(cuspsum + div1[1]*4 + q)
> : q in div1]);
11 1
> //Case cuspsum+3p+2q with p,q distinct places of degree 1.
> //We can assume p=div1[1].
> Min(&cat [FunctionDegrees(cuspsum + div1[1]*3 + q*2)
> : q in div1[2..14]]);
12 1
> //Case cuspsum+3p+q+r with p,q,r distinct places of degree 1.
> //We can assume p=div1[1].
> Min(&cat[FunctionDegrees(cuspsum + div1[1]*3 + &+qr)
> : qr in Subsets(SequenceToSet(div1[2..14]),2)]);
11 3
> //Case cuspsum+2p+2q+r with p,q,r distinct places of degree 1.
> //We can assume r=div1[1].
> Min(&cat[FunctionDegrees(cuspsum + div1[1] + 2*&+pq)
> : pq in Subsets(SequenceToSet(div1[2..14]),2)]);
11 13
> //Case cuspsum+2p+q+r+s with p,q,r,s distinct places of degree 1.
> Min(&cat[FunctionDegrees(cuspsum + 2*div1[1] + &+qrs)
> : qrs in Subsets(SequenceToSet(div1[2..14]),3)]);
11 15
> //Case cuspsum+p+q+r+s+t with p,q,r,s,t distinct places of degree 1.
> //Here we use that f' or f'-1 has a zero at a rational point u
```

```
> //if it has degree 13 or less. We can assume u=div1[1].
> Min(FunctionDegrees(cuspsum*2-3*div1[1]));
12 1
> //minimum is 11 so indeed there are no degree <=10 maps!
```

A.8 $N = 31$

```
> load "x1_31.m";
Loading "x1_31.m"
> [#Places(AFF,i) : i in [1..10]];
[ 15, 0, 0, 0, 3, 15, 15, 30, 50, 94 ]
> //indeed only #(Z/NZ)*/{1,-1} rational points
> //n=ceil(15/3)=5 so S=S_{11-5}+cuspsum
> //dominates all functions of deg <=11
> //Case cuspsum+5p +q with p,q places of degree 1.
> //We can assume p=div1[1].
> Min(&cat [FunctionDegrees(cuspsum+div1[1]*5+ q) :
> q in div1]);
13 1
> //Case cuspsum+4p+2q with p,q distinct places of degree 1.
> //We can assume p=div1[1].
> &cat [FunctionDegrees(cuspsum+div1[1]*4 + q*2)
> : q in div1];
[]
> //Case cuspsum+4p+q+r with p,q,r distinct places of degree 1.
> //We can assume p=div1[1].
> Min(&cat[FunctionDegrees(cuspsum + div1[1]*4 + &+qr)
>  : qr in Subsets(SequenceToSet(div1[2..15]),2)]);
12 1
> //Case cuspsum+3p+3q with p,q distinct places of degree 1.
> //We can assume p=div1[1].
> &cat [FunctionDegrees(cuspsum+div1[1]*3 + q*3)
> : q in div1];
[]
> //Case cuspsum=3p+2q+r and cuspsum+2p+2q+2r with p,q,r distinct
> //places of degree 1 follow from cuspsum+3p+2q+2r.
> //we can assume p=div1[1].
> Min(&cat[FunctionDegrees(cuspsum + div1[1]*3 + 2*&+qr)
> : qr in Subsets(SequenceToSet(div1[2..15]),2)]);
12 3
> //Case cuspsum+3p+q+r+s, cuspsum+2p+q+r+s+t and cuspsum+p+q+r+s+t+u
> //with p,q,r,s,t,u distinct places of degree 1.
> //Here we use that either f' or f'-1 has zero at a rational point v
```

```
> //if it has degree 14 or less. We can assume v=div1[1].
> Min(&cat [FunctionDegrees(cuspsum*2-3*div1[1]+2*p)
> : p in div1]);
12 38
> //Case cuspsum+2p+2q+2r has already been handled
> //Case cuspsum+2p+2q+r+s whith p,q,r,s distinct places of degree 1.
> //This is the hardest case and takes almost 12 minutes
> //while other cases take about a minute.
> //We can assume p=div1[1].
> Min(&cat[&cat [FunctionDegrees(cuspsum+2*div1[1]+2*q+&+rs)
> : q in div1[2..15] | q notin rs ]
> : rs in Subsets(SequenceToSet(div1[2..15]),2)]);
13 3
> //Case cuspsum+p+q with deg p=1 and deg q=5.
> //We can assume p=div1[1].
> &cat[FunctionDegrees(cuspsum+div1[1]+q) : q in Places(AFF,5)];
[]
> //Case cuspsum+p with deg p=6.
> &cat[FunctionDegrees(cuspsum+q) : q in Places(AFF,6)];
[]
> //minimum is 12 so indeed there are no degree <=11 maps!
```

References

Dan Abramovich. A linear lower bound on the gonality of modular curves. *Internat. Math. Res. Notices*, (20):1005–1011, 1996. ISSN 1073-7928. doi: 10.1155/S1073792896000621. URL http://dx.doi.org/10.1155/S1073792896000621.

Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi: 10.1006/jsco.1996.0125. URL http://dx.doi.org/10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993).

J.G. Bosman. Explicit computations with modular Galois representations, 2008. URL http://www.math.leidenuniv.nl/nl/theses/131/.

Pete L. Clark, Brian Cook, and James Stankewicz. Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice). *International Journal of Number Theory*. doi: 10.1142/S1793042112501436. URL http://www.worldscientific.com/doi/abs/10.1142/S1793042112501436. accepted for publication.

Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. Torsion points on elliptic curves over number fields of small degree. in preparation.

Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

Gerhard Frey. Curves with infinitely many points of fixed degree. *Israel Journal of Mathematics*, 85:79–83, 1994. ISSN 0021-2172. URL http://dx.doi.org/10.1007/BF02758637. 10.1007/BF02758637.

Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. ISBN 0-387-90244-9. Graduate Texts in Mathematics, No. 52.

S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *Internat. Math. Res. Notices*, (6):129–133, 1992a. ISSN 1073-7928. doi: 10.1155/S107379289200014X. URL http://dx.doi.org/10.1155/S107379289200014X.

S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992b. ISSN 0020-9910. doi: 10.1007/BF01232025. URL http://dx.doi.org/10.1007/BF01232025.

S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228):3, 81–100, 1995. ISSN 0303-1179. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. ISSN 0303-1179. Cohomologies p-adiques et applications arithmétiques. III.

Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985. ISBN 0-691-08349-5; 0-691-08352-5.

V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989. ISSN 0234-0852.

Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. ISBN 0-19-850284-2. Translated from the French by Reinie Erné, Oxford Science Publications.

B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. ISSN 0073-8301. URL http://www.numdam.org/item?id=PMIHES_1977__47__33_0.

B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978. ISSN 0020-9910. doi: 10.1007/BF01390348. URL http://dx.doi.org/10.1007/BF01390348.

Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996. ISSN 0020-9910. doi: 10.1007/s002220050059. URL http://dx.doi.org/10.1007/s002220050059.

J. Oesterlé. Torsion des courbes elliptiques sur les corps de nombres. not published.

Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999. ISSN 0075-4102. doi: 10.1515/crll.1999.009. URL http://dx.doi.org/10.1515/crll.1999.009.

Pierre Parent. Torsion des courbes elliptiques sur les corps cubiques. *Ann. Inst. Fourier (Grenoble)*, 50(3):723–749, 2000. ISSN 0373-0956. URL http://www.numdam.org/item?id=AIF_2000__50_3_723_0.

Pierre Parent. No 17-torsion on elliptic curves over cubic number fields. *J. Théor. Nombres Bordeaux*, 15(3):831–838, 2003. ISSN 1246-7405. URL http://jtnb.cedram.org/item?id=JTNB_2003__15_3_831_0.

Bjorn Poonen. Gonality of modular curves in characteristic p. *Math. Res. Lett.*, 14(4):691–701, 2007. ISSN 1073-2780.

W. A. Stein et al. *Sage Mathematics Software (Version 5.2)*. The Sage Development Team, 2012. URL http://www.sagemath.org.

Andrew V. Sutherland. Constructing elliptic curves over finite fields with prescribed torsion. *Math. Comp.*, 81(278):1131–1147, 2012. ISSN 0025-5718. doi: 10.1090/S0025-5718-2011-02538-X. URL http://dx.doi.org/10.1090/S0025-5718-2011-02538-X.

William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969. ISSN 0012-9593.