Torsion points on elliptic curves over number fields of small degree

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 21 september 2016
klokke 11:15 uur

door

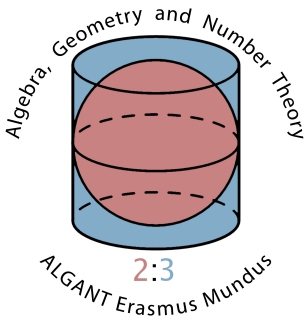
Maarten Derickx
geboren te Voorst, Nederland,
in 1986

Promotor: Prof. dr. Sebastian J. Edixhoven
Copromotor: Prof. dr. Lambertus van Geemen (Università d.s. di Milano)
Copromotor: dr. Pierre Parent (Université de Bordeaux)

Samenstelling van de promotiecommissie:

Prof. dr. Adrianus W. van der Vaart
Prof. dr. Samir Siksek (Warwick University)
Prof. dr. Loic Merel (Universite Paris Diderot)
dr. Marusia Rebolledo (Universite Blaise Pascal Clermont-Ferrand)
Prof. dr. Bart de Smit
dr. Peter Bruin

This work was funded by Algant-Doc Erasmus-Mundus and was carried out at Universiteit Leiden, Université de Bordeaux and Università degli studi di Milano



université de BORDEAUX

Contents

Preface

The main subject of this thesis is the study of torsion points on elliptic curves over number fields. This is a subject of study that goes as far back as 1906, where it starts with the work of Beppo Levi who studied torsion points on elliptic curves over $\mathbb{Q}$. He showed that for each of the groups

$$\mathbb{Z}/N\mathbb{Z} \quad \text{for } N = 1, 2, \ldots, 10, \text{ or } 12 \tag{1}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{for } N = 1, 2, 3, \text{ or } 4 \tag{2}$$

over $\mathbb{Q}$ there are infinitely many non isomorphic elliptic curves whose torsion subgroup is isomorphic to that group. In addition he also showed that the group structures $\mathbb{Z}/N\mathbb{Z}$ for $N = 14, 16, 20$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 10, 12$ do not occur as the torsion group of an elliptic curve over $\mathbb{Q}$. Bepo Levi shared his ideas on what would happen for larger values of N on the 1908 International Mathematical conference in Rome. He believed that the groups in (1) and (2), with the possible addition of $\mathbb{Z}/24\mathbb{Z}$, are the only groups that can occur as the torsion subgroup of an elliptic curve over $\mathbb{Q}$. However this conjecture seems to have been forgotten and it has been restated by Trygve Nagell in 1952 and by Andrew Ogg in 1970. As a result the conjecture that the groups in the lists (1) and (2) are the only groups that can occur as a torsion group of an elliptic curve over $\mathbb{Q}$ came to be known as Ogg's conjecture. This conjecture was later proven by Barry Mazur in his breaktrough paper[1]. A very nice exposition of the above history of the study of torsion points on elliptic curves over $\mathbb{Q}$, can be found in article [7] on Beppo Levi's life and mathematical work.

After Mazur's proof of Beppo Levi's conjecture which was later restated by Nagell and Ogg, the study moved to torsion points on elliptic curves over number fields other than $\mathbb{Q}$. Sheldon Kamienny generalized the techniques of Mazur to number fields of higher degree[2] and together with Mazur he determined all group structures that can occur as the torsion subgroup of an elliptic curve over a quadratic field[3], and

[1] B. Mazur. "Modular curves and the Eisenstein ideal". In: *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186 (1978).

[2] S. Kamienny. "Torsion points on elliptic curves over fields of higher degree". In: *Internat. Math. Res. Notices* 6 (1992), pp. 129–133.

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

the list of all such groups turned out to be finite again. This phenomenon continues to hold in higher degrees. In fact, building on the ideas of Mazur an Kamienny, Loïc Merel proved that if $d > 0$ is an integer then the list of groups that occur as the torsion group of an elliptic curve over a number field of degree d is finite[4]. Degrees 1 and 2 are the only degrees for which this finite list is known, although the list of primes that can divide the order of the torsion group is also known for degree 3 by work of Parent[5][6].

This thesis contains several new results considering which group structures can occur as the torsion subgroup of an elliptic curve over a number field of small degree. This thesis consist of four chapters, the first of which is introductory and contains no new results. The three other chapters are research articles that have been written together with several co-authors to whom I am very grateful for their successful collaboration. The three articles all contain original ideas both from my co-authors as well ones from myself and ones that came up during the many fruitful discussions we had on the subject. What follows is a short summary of the main results of each of the three research article chapters.

Chapter 2 is an article that has been published in the Journal of Algebra and is joint work with Mark van Hoeij. In this chapter the torsion groups of the form $\mathbb{Z}/N\mathbb{Z}$ are studied over number fields of degree 5,6,7, and 8. For of these degrees the explicit list of all integers N such that the torsion structure $\mathbb{Z}/N\mathbb{Z}$ occurs for infinitely many non isomorphic elliptic curves is determined, where the study of degrees ≤ 4 was omitted because here the answer was already known.

Chapter 3 is an article that is joint work with Sheldon Kamienny, William Stein and Michael Stoll, this article is not yet published but will soon be submitted for publication. In this article the primes that can divide the order of a torsion group of an elliptic curve over a number field of degree d are determined for degrees $4, 5$, and 6. Aside from the main result it also contains a section in which theory is developed that allows one to determine the set of all rational points on symmetric powers of a curve in certain situations. The Appendix of this chapter contains a proof of Joseph Oesterlé's Theorem that states that if an elliptic curve over a number field of degree d contains a torsion point of order p, then $p < (3^{d/2} + 1)^2$. It is included because a proof of this statement has not yet been published. The appendix closely follows Oesterlé's unpublished notes which he made available to me, although it contains some minor simplifications using literature that did not exists yet at the time that Oesterlé proved his Theorem.

---

[4]L. Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". In: *Invent. Math.* 124.1-3 (1996), pp. 437–449.

[5]P. Parent. "Torsion des courbes elliptiques sur les corps cubiques". In: *Ann. Inst. Fourier (Grenoble)* 50.3 (2000), pp. 723–749.

[6]P. Parent. "No 17-torsion on elliptic curves over cubic number fields". In: *J. Théor. Nombres Bordeaux* 15.3 (2003), pp. 831–838.

The final chapter is an article that will appear in a memorial volume for Fumiyuki Momose. It is co-authored by Barry Mazur and Sheldon Kamienny. In this article the question is asked what one can still do if d, N are integers such that there are infinitely many non isomorphic elliptic curves over number fields of degree d with a torsion point of order N. Can one somehow still find all of them? As a first start in answering this question is done by an explicit case study, namely the question is answered for $N = 17$ and $d = 4$. This value of d is the smallest integer for which there exist infinitely many elliptic curves over a number field of degree d with a point of order 17.

CHAPTER 1

Modular curves and modular forms

MODULAR CURVES AND MODULAR FORMS

MAARTEN DERICKX

Contents

1. Elliptic curves

There are two ways in which one can look at modular curves, one is the standpoint of complex geometry and the other is the standpoint of algebraic geometry. These two standpoints meet at the place where one starts to do algebraic geometry over $\mathbb{C}$. In this section the theory of both sides is discussed in parallel.

A complex elliptic curve is pair $(E, 0)$ of a compact Riemann surface E of genus 1 together with a base point $0 \in \mathbb{C}$. In both the complex and the algebraic setting we will just write E instead of $(E, 0)$ in the rest of this text.

Let $\Lambda \subset \mathbb{C}$ be a lattice, i.e. a discrete subgroup of maximal rank, meaning rank 2 in this case. Then

$$E_\Lambda := \mathbb{C}/\Lambda$$

together with the equivalence class of $0 \in \mathbb{C}$ is an elliptic curve. The holomorphic one form $\mathrm{d}z$ on $\mathbb{C}$ is invariant under translation by Λ and hence descends to a nonzero holomorphic one form on $\mathbb{C}/\Lambda$.

Conversely if $\omega \in \Omega^1(E)$ is a nonzero holomorphic one form, then there exists a unique lattice $\Lambda_{E,\omega} \subset \mathbb{C}$ and a unique isomorphism

$$f : E \xrightarrow{\sim} \mathbb{C}/\Lambda_{E,\omega}$$

such that $f^*(\mathrm{d}z) = \omega$.

Using the isomorphism f, the elliptic curve E gets a group law, the group law is independent of the choice of $\mathrm{d}z$ since scalar multiplication $\mathbb{C} \to \mathbb{C}$ is a group homomorphism.

Let S be a scheme, an algebraic elliptic curve over S is a pair $(E, 0)$ where E is a scheme that is smooth of relative dimension 1 and proper over S such that all its geometric fibers are irreducible genus one curves and $0 \in E(S)$.

Let R be a commutative $\mathbb{Z}[\frac{1}{6}]$-algebra, and $a_4, a_6 \in R$ such that

$$-16(4a_4^3 + 27a_6^2) \in R^*,$$

then the projective curve E_{a_4,a_6} given by

$$y^2 = x^3 + a_4 x + a_6$$

together with ∞ is an elliptic curve and

$$\omega_{a_4,a_6} := (3x^2 + a_4)^{-1}\mathrm{d}y = (2y)^{-1}\mathrm{d}x$$

is a global one form.

Suppose $\operatorname{Spec} R \subset S$ is an affine open with $6 \in R^*$ such that there exist a nowhere vanishing 1 form $\omega \in \Omega^1_{E/R}(E)$ then there are unique $a_4, a_6 \in R$ and a unique

$$f : E \xrightarrow{\sim} E_{a_4,a_6}$$

such that $f^*\omega_{a_4,a_6} = \omega$

One can put a group scheme structure on E by dentifying E with $\mathrm{Pic}^0_{E/S}$ by sending $P \in E(T)$ to the line bundle T $\mathcal{O}_{E_T}(P - 0_T)$ for all S schemes T.

The story on the algebraic side can be generalized to the case of $\mathbb{Z}$-algebras with a little bit more effort. Also one can mimic the definition of the group structure in the complex case by first putting a group scheme structure on E_{a_4,a_6} using explicit equations, and use f to give E a group scheme structure as well. So we have seen that both complex and algebraic elliptic curves, although defined by abstract properties can always be written down explicitly, and that they automatically inherit a group (scheme) structure.

If E_a is an algebraic elliptic curve over $\mathbb{C}$ then $E_a(\mathbb{C})$ is a complex elliptic curve and if E_c is a complex elliptic curve then one write $E_c \cong \mathbb{C}/\Lambda$. Define

$$\begin{aligned} \wp_\Lambda : \mathbb{C} \setminus \Lambda &\to \mathbb{C} \\ z &\mapsto \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{(-\lambda)^2} \right) \end{aligned} \tag{1}$$

$$G_{2k}(\Lambda) := \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^{2k}}, \quad \text{for } k \in \mathbb{Z}_{\geq 2} \tag{2}$$

$$g_2(\Lambda) := 60 G_4(\Lambda), \quad g_3(\Lambda) := 140 G_6(\Lambda). \tag{3}$$

The function $\wp_\Lambda$ is called the Weierstrass P-function. The function $\wp_\Lambda$ and its derivative satisfy the following equation

$$(\tfrac{1}{2}\wp'_\Lambda(z))^2 = \wp_\Lambda(z)^3 - \tfrac{1}{4} g_2(\Lambda) \wp_\Lambda(z) - \tfrac{1}{4} g_3(\Lambda).$$

The functions $\wp_\Lambda$ and $\wp'_\Lambda$ are invariant under translation by Λ so they induce a map

$$\begin{aligned} f_\Lambda : \mathbb{C}/\Lambda &\to E_{\frac{1}{4}g_2, \frac{1}{4}g_3}(\mathbb{C}) \\ z &\mapsto \wp_\Lambda(z), \tfrac{1}{2}\wp'_\Lambda(z), \end{aligned} \tag{4}$$

where the equivalence class $0 + \Lambda$ is sent to ∞. The map f_Λ is an isomorphism of elliptic curves, and it is even compatible with the choice of one forms since

$$f_\Lambda^*(\frac{\mathrm{d}x}{2y}) = \frac{\mathrm{d}\wp(z)}{\wp'(z)} = \mathrm{d}z. \tag{5}$$

Two elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if an only if there exists a u in $\mathbb{C}^*$ such that $\Lambda_2 = u\Lambda_1$. Define the j-invariant of $\mathbb{C}/\Lambda$ by

$$j(\Lambda) := 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}.$$

Using the fact that $g_2(u\Lambda) = u^{-4} g_2(\Lambda)$ and $g_3(u\Lambda) = u^{-6} g_3(\Lambda)$ it follows that j only depends on the isomorphism class of $\mathbb{C}/\Lambda$ and one can even show that j determines the isomorphism class uniquely.

Let R be a $\mathbb{Z}[\frac{1}{6}]$ algebra and $a_4, a_6, a'_4, a'_6 \in R$ such that E_{a_4,a_6} and $E_{a'_4,a'_6}$ are elliptic curves. These curves are isomorphic over R if and only if there exists an $u \in R^*$ such that $a'_4 = u^{-4} a_4$ and $a'_6 = u^{-6} a_6$. Define

$$j(a_4, a_6) := 1728 \frac{4a_4^3}{4a_4^3 + 27 a_6^2}.$$

Then $j(a_4, a_6)$ only depends on the isomorphism class of E_{a_4,a_6} and if R is an algebraically closed field then j even determines it uniquely.

This shows that both the complex and the algebraic way of looking at elliptic curves agree, if in the algebraic world one restricts to elliptic curves over $\mathbb{C}$.

1.1. **Some q-expansions.** Two elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if there exists a $c \in \mathbb{C}$ such that $c\Lambda = \Lambda'$. Now chose two generators λ_1, λ_2 of Λ. By scaling with λ_2^{-1} one sees that $\mathbb{C}/\Lambda$ is isomorphic to $\mathbb{C}/(\lambda_1/\lambda_2\mathbb{Z} + \mathbb{Z})$. In

particular, by replacing λ_1/λ_2 by $-\lambda_1/\lambda_2$ if necessary, one sees that there is always a $\tau \in \mathbb{H} := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$ such that $\mathbb{C}/\Lambda \cong \mathbb{C}/\tau\mathbb{Z} + \mathbb{Z}$. For $\tau \in \mathbb{H}$ define $\Lambda_\tau := \tau\mathbb{Z} + \mathbb{Z}$. By additionally defining $\wp(z, \tau) := \wp_{\Lambda_\tau}(z)$, $G_{2k}(\tau) := G_{2k}(\Lambda_\tau)$ and $g_i(\tau) = g_i(\Lambda)$ for $i = 2, 3$ one can view $\wp$ as a meromorphic function on $\mathbb{C} \times \mathbb{H}$ and G_{2k} and g_i as holomorphic functions on $\mathbb{H}$. All these functions are invariant under translation by 1 on the τ coordinate since Λ_τ and $\Lambda_{\tau+1}$ are the same lattice. Also z and $z + 1$ define the same point in $\mathbb{C}/\Lambda_\tau$ showing that $\wp$ is also invariant under translation by 1 in the z coordinate. This means that all these functions can be written as power series in $q := e^{2\pi i\tau}$ whose coefficients are Laurent series in $u := e^{2\pi iz}$. See for example [Silverman(1994), I §6,§7]. The resulting power series are

$$\wp(z, \tau) = (2\pi i)^2 \left(\sum_{n\in\mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} + \frac{1}{12} - 2\sum_{n=1}^{\infty} \frac{q^n}{(1 - q^n)^2} \right) \tag{6}$$

$$G_{2k}(\tau) = (2\pi i)^{2k} \left(\frac{-B_{2k}}{(2k)!} + \frac{2}{(2k-1)!} \sum_{n=1}^{\infty} \frac{n^{2k-1} q^n}{1 - q^n} \right), \tag{7}$$

where $B_k \in \mathbb{Q}$ are the Bernoulli numbers, which are defined as the coefficients of the Taylor series $\frac{t}{e^t-1} = \sum_{k=1}^{\infty} B_k \frac{t^k}{k!}$. Applying $\frac{\partial}{\partial z} = 2\pi i u \frac{\partial}{\partial u}$ to $\wp$ one obtains the formula[1]

$$\frac{\partial \wp(z, \tau)}{\partial z} := -(2\pi i)^3 \sum_{n\in\mathbb{Z}} \frac{q^n u(1 + q^n u)}{(1 - q^n u)^3} \tag{8}$$

The formula's for $G_{2k}(\tau)$ and $g_i(\tau)$ are often rewritten using the auxiliary functions

$$\sigma_k(n) := \sum_{d|n, d>0} d^k, \quad s_k(q) := \sum_{n=1}^{\infty} \frac{n^k q^n}{1 - q^n} = \sum_{n=1}^{\infty} \sigma_k(n) q^n. \tag{9}$$

One has $B_4 = -\frac{1}{30}$ and $B_6 = \frac{1}{42}$ so that the q-expansion of $\frac{1}{4}g_2(\tau)$ and $\frac{1}{4}g_3(\tau)$ are

$$\frac{1}{4}g_2(\tau) := (2\pi i)^4 (\frac{1}{48} + 5s_3(q)) \text{ and } \frac{1}{4}g_3(\tau) := (2\pi i)^6 (-\frac{1}{864} + \frac{7}{12}s_5(q)). \tag{10}$$

1.2. **Tate Curve.** Let τ be in the upper half plane, then the elliptic curve $y^2 = x^3 - \frac{1}{4}g_2(\tau)x - \frac{1}{4}g_3(\tau)$ has j-invariant $j(\tau) := j(\Lambda_\tau)$ and discriminant $\Delta(\tau) : g_2(\tau)^3 - 27g_3(\tau)^2$. Using the above formulas for q-expansion one can show that

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c(n) q^n, \quad c(n) \in \mathbb{Z}, \text{ and} \tag{11}$$

$$\Delta(\tau) = (2\pi i)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24} \tag{12}$$

[1]This differs by a minus sign from the formula in [Silverman(1994), I Thm 6.2], where there is a sign mistake.

Define $\tilde{g}_2 = (2\pi i)^{-4} g_2$, $\tilde{g}_3 := (2\pi i)^{-6} g_3$, $\tilde{\wp} := (2\pi i)^{-2}\wp$, and $\tilde{\Delta} := (2\pi i)^{-12}\Delta$. With these definitions the elliptic curve $y^2 = x^3 - \frac{1}{4}\tilde{g}_2(\tau)x - \frac{1}{4}\tilde{g}_3(\tau)$ is isomorphic to $\mathbb{C}/\Lambda_\tau$ via $(x,y) = (\tilde{\wp}(z,\tau), \frac{1}{2}\frac{\partial}{\partial z}\tilde{\wp}(z,\tau))$. This model of $\mathbb{C}/\Lambda_\tau$ over $\mathbb{H}$ has not only a j-invariant whose q-expansion has integral coefficients, but the coefficients of the q-expansion of its discriminant $\tilde{\Delta}$ are integral as well. The functions $\tilde{g}_2$ and $\tilde{g}_3$ do not have integral q-expansions, although they are almost integral since they are fractions whose denominator is a divisor of $864 = 2^3 \cdot 3^3$ as formula (10) shows. Substituting $x = x' + \frac{1}{12}$ and $y = y' + \frac{1}{2}x'$ gives the curve

$$y'^2 + x'y' = x'^3 + a_4 x' + a_6, \quad a_4 := -5s_3, \quad a_6 := -\frac{5s_3 + 7s_5}{12} \tag{13}$$

It is clear that a_4 has integral coefficients in its q-expansion. For any integer n one has $5n^3 + 7n^5 \equiv 0 \mod 12$ so that a_6 also has integral coefficients. The *Tate curve* E_q is the curve (13) over $\mathbb{Z}[[q]]$ where one uses q-expansion to see a_4 and a_6 as elements of $\mathbb{Z}[[q]]$. It is not an elliptic curve since its fiber above $q = 0$ is singular, however since $\tilde{\Delta}$ is a unit in $\mathbb{Z}[[q]][\frac{1}{q}]$ it is an elliptic curve over $\mathbb{Z}[[q]][\frac{1}{q}]$. The Tate curve is useful since it allows one to study elliptic curves over p-adic fields, i.e. finite extensions of $\mathbb{Q}_p$. This is captured in the following Theorem due to Tate whose statement can be obtained by combining [Silverman(1994), V Thm 3.1 and Lemma 5.1]

Theorem 1.1 (Tate)**.** *Let K be a p-adic field and $q_0 \in K^*$ with $|q_0| < 1$ then the power series a_4 and a_6 converge in q_0. Let E_{q_0} be the curve given by*

$$y'^2 + x'y' = x'^3 + a_4(q_0)x' + a_6(q_0)$$

then $E_{q_0}(\overline{K})$ is isomorphic to $\overline{K}^*/q_0$ as $\mathrm{Gal}(\overline{K}/K)$ modules. The curve E_{q_0} has $|j(E_{q_0})| > 1$ and for every elliptic curve E over K with $|j(E_{q_0})| > 1$ there is a unique $q_0 \in K$ such that $E \cong E_{q_0}$ over $\overline{K}$.

The isomorphism between $\overline{K}^*/q_0$ and $E_{q_0}(\overline{K})$ is obtained by using formula's 6 and 8 to find the q-expansions of $x' = \tilde{\wp} - \frac{1}{12}$ and $y' = \frac{1}{2}\frac{\partial}{\partial z}\tilde{\wp} - \frac{1}{2}\tilde{\wp} - \frac{1}{12}$. With this isomorphism one sees that the invariant differentials

$$2\pi i \mathrm{d}z = \frac{\mathrm{d}u}{u} = \frac{\mathrm{d}x'}{2y' + x'},$$

are equal, where the left most differential only makes sense in the complex world. The above theorem is the p-adic analogue of the fact that every elliptic curve over $\mathbb{C}$ can be written as $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \cong \mathbb{C}^*/e^{2\pi i \tau^{\mathbb{Z}}}$.

1.3. **Néron polygons.** The fiber of the Tate curve E_q over $\mathbb{Z}[[q]]$ at $q = 0$ is not an elliptic curve although it is still a curve, in fact it's special fiber is isomorphic to $\mathbb{P}^1$ with two points glued together. The special fiber is an example of a Néron 1-gon. In general if N is an integer and R is a ring then the *Néron N-gon* $\mathcal{N}_N$ over R is defined to be the singular projective curve over R that one obtains by

taking a copy X_i of $\mathbb{P}^1_R$ for each $i \in \mathbb{Z}/N\mathbb{Z}$ and glueing the point ∞ of X_i to the point 0 of X_{i+1} in such a way that the intersections become ordinary double points. Using the identification $\mathbb{G}_{m,R} = \mathbb{P}^1_R \setminus \{0, \infty\}$ one sees that the smooth locus of the Néron N-gon over R is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{G}_{m,R}$, turning the smooth locus of the Néron N-gon into a group scheme. Morphisms between Néron N-gons are the scheme morphisms that induce group-scheme homomorphisms when restricted to the smooth locus, so in particular they should map the smooth locus to itself. If K is a field of characteristic co-prime to N then one can make $\mu_N(K)$ act on $\mathbb{Z}/N\mathbb{Z} \times \mathbb{P}^1_K$ by $\zeta_N(i, (a : b)) := (i, (\zeta_N^i a : b))$ and one can make $\{\pm 1\}$ act on it by $-(i, (a : b)) := (i, (b : a))$. Both these actions are group homomorphisms when restricted to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{G}_{m,K} \subseteq \mathbb{Z}/N\mathbb{Z} \times \mathbb{P}^1_K$ and they are compatible with the identifications of ∞ on the i-th component with 0 on the $i+1$-th component. Since these actions commute, one gets that automorphism group of $\mathcal{N}_N$ contains

$$\mu_N(K) \times \{\pm 1\}.$$

The above group is actually the entire automorphism group.

1.4. **Generalized Elliptic curves.** Theorem 1.1 shows that the Tate curve E_q over $\mathbb{Z}[[q]]$ can be used to study elliptic curves over p-adic fields with $|j| > 1$ and $j \neq \infty$. Its special fiber at $q = 0$ is not an elliptic curve but it is still a Néron N-gon. Generalized elliptic curves are curves where we also allow the geometric fibers to be Néron N-gons, to be more precise.

Definition 1.2. Let S be a scheme, a *generalized elliptic curve* over S is a scheme E that is proper, flat and of finite presentation over S together with a group scheme structure on E^{sm}, such that each of the geometric fibers $E_{\overline{K}}$ of E is isomorphic to either an elliptic curve over K or the Néron N-gon over K.

In the above definition E^{sm} denotes the locus of E that is smooth over S and the isomorphisms of the geometric fibers should respect the group scheme structure on $E^{sm}_{\overline{K}}$. A point of order N on a generalized elliptic curve E/S is understood to be an element $P \in E(S)$ of order N such that all geometric fibers of P also have order N and furthermore such that the subgroup generated by P meets all components of all geometric fibers.

2. Modular curves

2.1. **The modular curve $Y_1(N)$.** Modular curves are curves whose points correspond to elliptic curves with some extra structure. The modular curve $Y_1(N)$ is the curve whose points correspond to an elliptic curve with a torsion point of order N. To avoid technical difficulties we assume that $N > 4$ is an integer. Let (E_1, P_1) and (E_2, P_2) be pairs of an elliptic curve together with a point of order N, then an isomorphism from (E_1, P_1) to (E_2, P_2) is defined to be an isomorphism of elliptic curves $f : E_1 \to E_2$ such that $f(P_1) = f(P_2)$. This definition will be used for both complex and algebraic elliptic curves.

Let $\mathbb{H}$ be the complex upper half plane. To $\tau \in \mathbb{H}$ one can associate the elliptic curve $E_\tau := \mathbb{C}/(\tau\mathbb{Z}+\mathbb{Z})$. If $E = \mathbb{C}/\Lambda$ is an elliptic curve and ω_1, ω_2 are generators of Λ such that $\mathrm{Im}(\omega_1/\omega_2) > 0$ then division by ω_2 gives an isomorphism $E \cong E_{\omega_1/\omega_2}$ showing that every elliptic curve is isomorphic to some E_τ.

Let $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{H}$ by $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\tau = \frac{a\tau+b}{c\tau+d}$. Then the sequence of isomorphisms

$$\begin{aligned} E_\tau &\cong \mathbb{C}/\left((a\tau+b)\mathbb{Z}+(c\tau+d)\mathbb{Z}\right) \\ &\cong \mathbb{C}/\left(\tfrac{a\tau+b}{c\tau+d}\mathbb{Z}+\mathbb{Z}\right) = E_{\frac{a\tau+b}{c\tau+d}}. \end{aligned}$$

shows that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $E_{\gamma\tau} \cong E_\tau$. One can even show that if $\tau_1, \tau_2 \in \mathbb{H}$ then $E_{\tau_1} \cong E_{\tau_2}$ if and only if there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_2 = \gamma\tau_1$.

The point $\frac{1}{N} \in E_\tau$ has order N, and because $N > 3$ one can show that E_τ has no automorphisms that fix $\frac{1}{N}$. Now

$$\tfrac{c\tau+d}{N} \equiv \tfrac{1}{N} \mod \tau Z + \mathbb{Z}$$

if and only if $(c,d) \equiv (0,1) \mod N$, so if one defines $\Gamma_1(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ to be the set of matrices with $(c,d) \equiv (0,1) \mod N$ then the isomorphism

$$\left(E_{\frac{a\tau+b}{c\tau+d}}, \tfrac{1}{N}\right) \cong \left(E_\tau, \tfrac{c\tau+d}{N}\right)$$

shows that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $(E_{\gamma\tau}, 1/N) \cong (E_\tau, 1/N)$ if and only if $\gamma \in \Gamma_1(N)$. So that $\mathbf{Y}_1(N) := \Gamma_1(N)\backslash\mathbb{H}$ can be interpreted as the set of isomorphism classes of pairs (E,P) where E is an elliptic curve and $P \in E$ a point of order N.

Let R be a ring and $b, c \in R$, then $E_{b,c}$ is the curve defined by

$$y^2 + (1-c)xy - by = x^3 - bx^2.$$

Define $R_{b,c} := \mathbb{Z}[b, c, \frac{1}{\Delta_{b,c}}]$ where $\Delta_{b,c}$ is the discriminant of the curve $E_{b,c}$ and define $Y := \operatorname{Spec} R_{b,c}$. The curve $E_{b,c}$ is an elliptic curve over Y and

$$P_0 := (0:0:1) \in E_{b,c}(Y).$$

Let $\Phi_N, \Psi_N, \Omega_N \in R_{b,c}$ be such that

$$(\Phi_N\Psi_N : \Omega_N : \Psi_N^3) = NP_0.$$

The equation $\Psi_N = 0$ is equivalent to P_0 having order dividing N. One can show that if $d \mid N$ then $\Psi_d \mid \Psi_N$. Define F_N by removing all factors coming form the Ψ_d with $d \mid N, d \neq N$ from Ψ_N, and

$$Y_1(N) := \operatorname{Spec} R_{b,c}[\tfrac{1}{N}]/F_N.$$

Let $\bar{b}, \bar{c} \in \operatorname{Spec} R_{b,c}[\frac{1}{N}]/F_N$ denote the equivalence classes of b, c and define $E_1(N) := E_{\bar{b},\bar{c}}$, it is an elliptic curve over $Y_1(N)$ and $P_1(N) := (0:0:1)$ is a point on it.

Let S be a scheme over $\mathbb{Z}[\frac{1}{N}]$ and $X \in Y_1(N)(S)$, then $E_1(N) \times_X S$ is an elliptic curve over R and the order of $P_1(N) \times_X S$ as well as that of all its geometric fibers is N. Conversely if E is an elliptic curve over S and $P \in E(R)[N]$ is such that the order of P is N in all geometric fibers, then there exist unique $b, c \in \mathcal{O}_R$ such that $F_N(b,c) = 0$ and $(E,P) \cong (E_{b,c}, P_0)$, furthermore this isomorphism is unique. So the pair b, c defines a point $X \in Y_1(N)(S)$ such that $(E,P) \cong (E_1(N)_S, P_1(N)_S)$.

We have seen that in the complex world the points of $\mathbf{Y}_1(N)$ correspond to pairs (E,P) where E is elliptic curves over $\mathbb{C}$ and P a point of order N. In the algebraic world we have seen that if R is a $\mathbb{Z}[\frac{1}{N}]$ algebra, then the points in $Y_1(N)(R)$ correspond to pairs (E,P) where E is an elliptic curve over R and $P \in E(R)[N]$

is such that the order of P is also N in all geometric fibers, in other words $Y_1(N)$ represents the functor which takes an R algebra to the set of isomorphism classes of pairs (E, P) of elliptic curve over R together with a point of order N. Taking $R = \mathbb{C}$ one obtains an isomorphism $\mathbf{Y}_1(N) \cong Y_1(N)(\mathbb{C})$ of Riemann surfaces. The curve $Y_1(N)$ is smooth over $\mathbb{Z}[\frac{1}{N}]$ and has geometrically irreducible fibers, see [Deligne and Rapoport(1975), Ch. IV].

2.1.1. *The universal elliptic curve with a point of order N.* In the above discussion we have seen that the pair $(E_1(N), P_1(N))$ is pair of an elliptic curve over $Y_1(N)$ together with a point $P_1(N) \in E_1(N)(Y_1(N))$ of order N all whose geometric fibers are also of order N. And we have even seen for R a $\mathbb{Z}[1/N]$-algebra that every pair (E, P) where E is an elliptic curve over R and $P \in E(R)$ a point of order N all whose geometric fibers also have order N can be obtained as the base change of $(E_1(N), P_1(N))$ along a unique morphism $X : \operatorname{Spec} R \to Y_1(N)$. The pair $(E_1(N), P_1(N))$ is called the universal elliptic curve with a point of order N. Now $(E_1(N)(\mathbb{C}), P_1(N)(\mathbb{C}))$ is a smooth family of elliptic curves with a smooth family of points of order N over $Y_1(N)(\mathbb{C})$ and this family can actually also be constructed directly in the complex world. Let $\mathbb{Z}^2$ act on $\mathbb{C} \times \mathbb{H}$ by $(m, n)(z, \tau) = (z + m\tau + n, \tau)$. Then the fiber of $(\mathbb{C} \times \mathbb{H})/\mathbb{Z}^2$ above $\tau \in \mathbb{H}$ is the elliptic curve E_τ, and the map $\mathbf{P}_1(N) : \mathbb{H} \to (\mathbb{C} \times \mathbb{H})/\mathbb{Z}^2$ which sends τ to $(1/N \mod \mathbb{Z}\tau + \mathbb{Z}, \tau)$ is a point of order N. If one lets $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{C} \times \mathbb{H}$ by

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) \times (\mathbb{C} \times \mathbb{H}) &\to \mathbb{C} \times \mathbb{H} \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, (z, \tau) \right) &\mapsto \left(\frac{z}{c\tau + d}, \frac{a\tau + b}{c\tau + d} \right) \end{aligned} \tag{14}$$

Then one can make the semi-direct product $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{C} \times \mathbb{H}$ by

$$((m, n), \gamma)(z, \tau) = (m, n)(\gamma(z, \tau)).$$

Now define $\mathbf{E}_1(N) := (\mathbb{Z}^2 \rtimes \Gamma_1(N)) \backslash (\mathbb{C} \times \mathbb{H})$. The map $\mathbf{E}_1(N) \to \mathbf{Y}_1(N)$ which sends $(\mathbb{Z}^2 \rtimes \Gamma_1(N))(z, \tau)$ to $\Gamma_1(N)\tau$ makes $\mathbf{E}_1(N)$ into a family of curves over $\mathbf{Y}_1(N)$. Using $N > 4$ one sees that the stabilizer of τ in $\Gamma_1(N)$ is trivial for all $\tau \in \mathbb{H}$. This triviality of the stabilizers implies that the fiber of $\mathbf{E}_1(N) \to \mathbf{Y}_1(N)$ above $\Gamma_1(N)\tau$ is isomorphic to E_τ for all $\tau \in \mathbb{H}$. One checks that the map $\mathbf{P}_1(N) : \mathbb{H} \to (\mathbb{C} \times \mathbb{H})/\mathbb{Z}^2$ induces a map $\mathbf{P}_1(N) : \mathbf{Y}_1(N) \to \mathbf{E}_1(N)$ by taking the quotient by $\Gamma_1(N)$ on both sides. The pair $(\mathbf{E}_1(N), \mathbf{P}_1(N))$ is the universal elliptic curve with a point of order N in the complex setting. And it is isomorphic to $(E_1(N)(\mathbb{C}), P_1(N)(\mathbb{C}))$.

2.2. **The modular curve $X_1(N)$.** The curve $\mathbf{Y}_1(N)$ of the previous section is not compact and the curve $Y_1(N)$ is not proper over $\mathbb{Z}[\frac{1}{N}]$. But compactness and properness are properties that are useful for studying curves (and higher dimensional varieties/schemes). The modular curves $\mathbf{X}_1(N)$, respectively $X_1(N)$ that will be defined in this section are compact, respectively proper over $\mathbb{Z}[\frac{1}{N}]$. The curves $\mathbf{Y}_1(N)$ respectively $Y_1(N)$ will be open and dense parts of them.

The j-invariant induces a holomorphic map $j : \mathbf{Y}_1(N) \to \mathbb{C}$ by sending (E, P) to $j(E)$. This turns $\mathbf{Y}_1(N)$ into a finite ramified cover of $\mathbb{C}$. See $\mathbb{C}$ as an open in $\mathbb{P}^1(\mathbb{C})$ whose complement is the point ∞. Take $D \subseteq \mathbb{P}^1(\mathbb{C})$ a punctured disc centered at ∞. By choosing D small enough one can assure that $j^{-1}(D)$ is a disjoint union of punctured discs. The Riemann surface $\mathbf{X}_1(N)$ is the Riemann surface obtained from the Riemann surface $\mathbf{Y}_1(N)$ by filling the holes in these punctured discs. The map j turns $\mathbf{X}_1(N)$ into a finite ramified cover of $\mathbb{P}^1(\mathbb{C})$. One has $j^{-1}(\infty) = \mathbf{X}_1(N) \setminus \mathbf{Y}_1(N)$. The set $j^{-1}(\infty)$ is a finite set and its elements are called the cusps.

The j-invariant induces a morphism of $\mathbb{Z}[\frac{1}{N}]$-schemes $j : Y_1(N) \to \mathbb{A}^1_{\mathbb{Z}[1/N]}$ which sends $(E, P) \in Y_1(N)(T)$ to $j(E) \in \mathcal{O}_T$ for all $\mathbb{Z}[\frac{1}{N}]$-schemes T. See $\mathbb{A}^1_{\mathbb{Z}[1/N]}$ as an open subscheme of $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ whose complement is the closed subscheme ∞. The generic point of $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ is $\operatorname{Spec} \mathbb{Q}(j)$ and by viewing j as element of $\mathbb{Q}(Y_1(N))$ we see that $\mathbb{Q}(j) \subseteq \mathbb{Q}(Y_1(N))$ is a finite extension of fields. The curve $X_1(N)$ is defined as the normalization of $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ in $\mathbb{Q}(Y_1(N))$. The map j turns $X_1(N)$ into a finite ramified cover of $\mathbb{P}^1_{\mathbb{Z}[1/N]}$. One has $j^{-1}(\infty) = X_1(N) \setminus Y_1(N)$. The scheme $j^{-1}(\infty)_{\mathbb{Z}[1/N,\zeta_N]\cap\mathbb{R}}$ is a disjoint union of copies of $\operatorname{Spec} \mathbb{Z}[\frac{1}{N}, \zeta_N] \cap \mathbb{R}$.

In the complex world there is also a second way to construct the underlying topological space of the Riemann surface $\mathbf{X}_1(N)$. For this one first defines $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and one extends the action of $\mathrm{SL}_2(\mathbb{Z})$ to $\mathbb{H}^*$ still using the formula $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \tau = \frac{a\tau+b}{c\tau+d}$, where one defines $\frac{a\infty+b}{c\infty+d} = \frac{a}{c}$ and $\frac{az+b}{cz+d} = \infty$ if $cz + d = 0$. One can show that $\mathrm{SL}_2 \mathbb{Z}$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$. One topologizes $\mathbb{H}^*$ by saying that $\mathbb{H}_{\operatorname{im} Z > x} \cup \{\infty\}$ with $x \in \mathbb{R}_{>0}$ forms a basis of open neighbourhoods of ∞ and requiring that the topology is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. One can show that there is a unique isomorphism of topological spaces between $\mathbf{X}_1(N)$ and $\Gamma_1(N)\backslash\mathbb{H}^*$ that is the identity on $Y_1(N) := \Gamma_1(N)\backslash\mathbb{H}$. This allows one to identify the cusps of $\mathbf{X}_1(N)$ with $\Gamma_1(N)\backslash\mathbb{P}^1(\mathbb{Q})$.

2.2.1. *Moduli interpretation of the cusps.* In Section 2.1 we saw that there exists an elliptic curve $E_1(N)$ over $Y_1(N)$ which has a point of order N that also has order N in all geometric fibers, and that for every $\mathbb{Z}[\frac{1}{N}]$ algebra R every elliptic curve over R together with a point of order N that also has order N in all geometric fibers is the base change of $E_1(N)$ to R for a unique morphism $X : \operatorname{Spec} R \to Y_1(N)$. Using the notion of generalized elliptic curve this story extends to $X_1(N)$. There is a unique extension $(E'_1(N), P'_1(N))$ of the pair $(E_1(N), P_1(N))$ over $Y_1(N)$ to $X_1(N)$ such that the geometric fibers of $E'_1(N)$ over $X_1(N)$ are generalized elliptic curves, the point $P'_1(N)$ lies in the smooth locus of $E'_1(N)$, the geometric fibers of $P'_1(N)$ are all points of order N and for each geometric fiber $P'_1(N)$ is a generator of the component group.

Theorem 2.1. *[Deligne and Rapoport(1975), Ch. IV] This pair $(E'_1(N), P'_1(N))$ mentioned above is universal, meaning that if S is a scheme over $\mathbb{Z}[\frac{1}{N}]$ and (E, P) is a pair where E is an elliptic curve over S and $P \in E(S)$ a point of order N such*

that all the geometric fibers of P are also of order N and generate the component group of their fiber, then there exists a unique $X : S \to X_1(N)$ such that (E, P) is isomorphic to the base change of $(E'_1(N), P'_1(N))$.

In particular, if K is an algebraically closed field and $s \in (X_1(N) \setminus Y_1(N))(K)$, then $E'_1(N)_s$ is a Néron d-gon for some integer d and $P'_1(N)_s$ is a point of order N that generates the component group of the Néron d-gon. Since the component group of a Néron d-gon is $\mathbb{Z}/d\mathbb{Z}$ this means that $d \mid N$.

The Tate curve given by Eq. (13) gives a way to study the curve $E'_1(N)$ over $X_1(N)$ in the neighbourhood of the cusps. Let $d \mid N$ be an integer and denote by $E_{q,d}$ the base change of E_q to $\mathbb{Z}[[q^{1/d}]]$. The scheme $E_{q,d}$ is not smooth over $\mathbb{Z}[[q^{1/d}]]$, but if $d = 1$ then it is at least still a regular scheme. If $d > 1$ then the singularities of $E_{q,d}$ can be resolved by blowing up the point $(q, x', y') = (0, 0, 0)$ exactly $\lfloor \frac{d}{2} \rfloor$ times, let $\tilde{E}_{q,d}$ denote the resulting scheme, its fiber over $q^{1/d} = 0$ is the Néron d-gon over $\mathbb{Z}$, and for every field K one has that $\tilde{E}_{q,d,K[[q^{1/d}]]}$ is the minimal regular model of $E_{q,d,K[[q^{1/d}]]}$. Consider x' and y' of Eq. (13) as elements of $\mathbb{Z}((u))[[q]]$ and let i, j be two integers. Evaluating x' and y' at $u = q^i\zeta_N^j$ gives a $\mathbb{Z}[\frac{1}{N}, \zeta_N][[q^{1/d}]]$ point of $\tilde{E}_{q,d}$, which we will denote by $P_{d,i,j}$. This point lies in the smooth locus and its order is a divisor of N. Actually the map

$$\alpha : \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to \tilde{E}^{sm}_{q,d}(\mathbb{Z}[\tfrac{1}{N}, \zeta_N][[q^{\frac{1}{d}}]]) \tag{15}$$

$$i, j \mapsto P_{d,i,j} \tag{16}$$

is a well defined injective group homomorphism. The point $\alpha(1, 0)$ is a generator of the component group at $q^{1/d} = 0$ and $\alpha(0, 1)$ lies in the identity component. Define $A_d \subset \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ to be the set of elements of order N whose first coordinate generates $\mathbb{Z}/d\mathbb{Z}$. The set A_d is exactly the set of (i, j) such that the pair $(\tilde{E}_{q,d}, \alpha(i, j))$ gives a point $s_{d,i,j} \in X_1(N)(\mathbb{Z}[\frac{1}{N}, \zeta_N][[q^{1/d}]])$. Let $s'_{d,i,j} \in X_1(N)(\mathbb{Z}[\zeta_N])$ be the point obtained by setting $q^{1/d} = 0$, then $s'_{d,i,j}$ is a cusp, and the map $s_{d,i,j} : \operatorname{Spec} \mathbb{Z}[\zeta_N][[q^{1/d}]] \to X_1(N)$ induces an isomorphism between $\mathbb{Z}[\zeta_N][[q^{1/d}]]$ and the completion of $X_1(N)_{\mathbb{Z}[\frac{1}{N}, \zeta_N]}$ along $s'_{d,i,j}$. Every Néron d-gon together with a point of order N that generates the component group is obtained from some $s'_{d,i,j}$ with $(i, j) \in A_d$, showing that $\left\{s'_{d,i,j} | d \mid N, (i, j) \in A_d\right\}$ is exactly the set of cusps of $X_1(N)_{\mathbb{Z}[\frac{1}{N}\zeta_N]}$, however two different elements of A_d might give the same cusp, indeed one can make $\mu_d(\mathbb{Z}[\frac{1}{N}, \zeta_d]) \times \{\pm 1\}$ act on A_d by $\zeta_d(i, j) = (i, j + iN/d)$ and $-(i, j) = (-i, -j)$. This action is compatible with the action of $\mu_d \times \{\pm 1\}$ on the set of points of order N of the Néron d-gon, showing that $s'_{d_1,i_1,j_1} = s'_{d_2,i_2,j_2}$ if and only if $d_1 = d_2$ and (i_1, j_1) and (i_2, j_2) are in the same orbit under this action.

3. Modular forms

Let $k > 0$ be an integer, $f : \mathbb{H} \to \mathbb{C}$ be a holomorphic function and $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, define $f[\gamma]_k : \mathbb{H} \to \mathbb{C}$ to be the function given by $f[\gamma]_k(\tau) := (c\tau+d)^{-k} f(\gamma\tau)$. The map $f \to f[\gamma]_k$ defines a right action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of all holomorphic functions $\mathbb{H} \to \mathbb{C}$ called the weight k action.

Definition 3.1. Let $k > 0$ be an integer and $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a finite index subgroup, then a modular form of weight k for Γ is a continuous function $f : \mathbb{H}^* \to \mathbb{C}$ such that:

(1) f is invariant under the weight k action of Γ, i.e. $f = f[\gamma]_k$ for all $\gamma \in \Gamma$.
(2) f is holomorphic when restricted to $\mathbb{H}$.

The function f is called a cusp form if $f(x) = 0$ for all $x \in \mathbb{P}^1(\mathbb{Q})$.

Where one should note that in this definition f is required to be continuous on all of $\mathbb{H}^*$. If one instead just requires f to be continuous on $\mathbb{H}$ one needs to add an extra condition that is called being "holomorphic at the cusps". This complex analytic definition of modular forms does not carry over to the algebraic world, however it can be reinterpreted in a way that does make sense in the algebraic world. Namely one can define $\omega_{\Gamma,k}$ to be the sheaf on $X(\Gamma) := \Gamma\backslash\mathbb{H}^*$ whose functions on $\Gamma\backslash U$ are the continuous functions $f : U \to \mathbb{C}$ invariant under the weight k action of Γ that are holomorphic when restricted to $\mathbb{H} \cap U$ for all open $U \subset \mathbb{H}^*$ that are invariant under Γ. If either k is even or Γ acts freely on $\mathbb{H}$ then the sheaf $\omega_{\Gamma,k}$ is a line bundle on $X(\Gamma)$, i.e. it is a sheaf of $\mathcal{O}_{X(\Gamma)}$ modules that is locally free of rank 1. The global sections of $\omega_{\Gamma,k}$ are exactly the modular forms of weight k. This line bundle $\omega_{\Gamma,k}$ is the object that does generalize to the algebraic world, at least if one requires that Γ is a congruence subgroup:

Definition 3.2. Let N be an integer and define

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

A *congruence subgroup* is a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ such that there exists an integer N for which $\Gamma(N) \subseteq \Gamma$.

For simplicity we will restrict ourselves to congruence subgroups Γ that contain $\Gamma_1(N)$ as a normal subgroup for some N in the discussion below. First we will discuss modular forms of weight k for $\Gamma_1(N)$ with $N > 4$ and only later will we discuss it for its groups that contain $\Gamma_1(N)$.

3.1. Modular forms for $\Gamma_1(N)$.

Let $N > 4$ be an integer. Over the curve $\mathbf{X}_1(N)$ we have the universal curve $\mathbf{E}_1(N)$, and we have the zero section $0 : \mathbf{X}_1(N) \to \mathbf{E}_1(N)$. This means we can look at the sheaf $\Omega^1_{\mathbf{E}_1(N)/\mathbf{X}_1(N)}$ of relative differential forms on $\mathbf{E}_1(N)$, this sheaf is locally free of rank 1 when restricted to the locus of

$\mathbf{E}_1(N)$ where it is smooth over $\mathbf{X}_1(N)$. Define

$$\omega_{\mathbf{E}_1(N)/\mathbf{X}_1(N)} := 0^*\Omega^1_{\mathbf{E}_1(N)/\mathbf{X}_1(N)}.$$

One has that $\omega_{\mathbf{E}_1(N)/\mathbf{X}_1(N)} \cong \omega_{\Gamma_1(N),1}$ and more generally $\omega^{\otimes k}_{\mathbf{E}_1(N)/\mathbf{X}_1(N)} \cong \omega_{\Gamma_1(N),k}$. Indeed, let $\pi : \mathbb{H}^* \to X_1(N)$ be the quotient map, then $\pi^*\omega_{\omega_{\mathbf{E}_1(N)/\mathbf{X}_1(N)}}$ is a free sheaf of rank 1 when restricted to $\mathbb{H}$. This is because one has $\pi^*\omega_{\Gamma_1(N)} \cong 0^*\Omega^1_{((\mathbb{C}\times\mathbb{H})/\mathbb{Z}^2))/\mathbb{H})}$ and the latter is generated by $\mathrm{d}z$ where z is the coordinate on $\mathbb{C}$. Since

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathrm{d}z = \mathrm{d}\frac{z}{c\tau + d} = \frac{1}{c\tau + d}\mathrm{d}z$$

it follows that $f \mapsto 2\pi i f \mathrm{d}z = f\frac{\mathrm{d}u}{u}$ gives an isomorphism between $\omega^{\otimes k}_{\mathbf{E}_1(N)/\mathbf{X}_1(N)}$ and $\omega_{\Gamma_1(N),k}$ on $\mathbf{Y_1(N)}$. Using the Tate curve over $\mathbb{C}$ one can show that $2\pi i \mathrm{d}z = \frac{\mathrm{d}u}{u}$ is also a generator of $\Omega^1_{\mathbf{E}_1(N)/\mathbf{X}_1(N)}$ in a neighbourhood of the 0 section at the cusps ($u = 1$ at the zero section), hence the isomorphism over $\mathbf{Y}_1(N)$ extends to one over $\mathbf{X}_1(N)$.

In the previous section it was already shown that modular forms of weight k for $\Gamma_1(N)$ can be seen as sections of $\omega_{\Gamma_1(N),k}$ and using the isomorphism $\omega^{\otimes k}_{\mathbf{E}_1(N)/\mathbf{X}_1(N)} \cong \omega_{\Gamma_1(N),k}$ one can even see them as sections of $\omega^{\otimes k}_{\mathbf{E}_1(N)/\mathbf{X}_1(N)}$. This last definition is the definition that carries over to the algebraic world.

Definition 3.3. Let $N > 4$ and k be integers and R a $\mathbb{Z}[\frac{1}{N}]$ algebra. Define

$$\omega_{X_1(N),R,k} := \left(0^*\Omega^1_{E_1(N)_R/X_1(N)_R}\right)^{\otimes k}.$$

An *R valued modular form of weight k for $X_1(N)$* is a global section f of $\omega_{X_1(N),R,k}$. A modular form f is called a cusp form if it has zeros at all cusps, i.e. it is zero on $X_1(N)_R \setminus Y_1(N)_R$.

The above discussion shows that if one takes $R = \mathbb{C}$ then this definition agrees with the complex analytic definition.

3.2. **Modular forms in weight 2.** In weight 2 there is even a different interpretation of modular forms. The reason for this is that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathrm{d}\tau = \mathrm{d}\frac{a\tau + b}{c\tau + d} = \frac{a(c\tau + d) - c(a\tau + b)}{(c\tau + d)^2}\mathrm{d}\tau = \frac{1}{(c\tau + d)^2}\mathrm{d}\tau,$$

showing that if f is a complex analytic modular form of weight 2 for some congruence subgroup Γ, then $2\pi i f \mathrm{d}\tau = f\frac{\mathrm{d}q}{q}$ is a differential on $\mathbb{H}$ that is invariant under the action of Γ. In particular, $f\frac{\mathrm{d}q}{q}$ descends to a differential on $Y_1(N)$. Using the description of the formal neighbourhoods of the cusps one can show that this differential has no poles at the cusps if and only if f is a cusp form, so that

$f \mapsto f\frac{\mathrm{d}q}{q}$ gives an isomorphism $\omega_{\Gamma_1(N),2} \cong \Omega^1_{\mathbf{X}_1(N)/\mathbb{C}}(cusps)$ called the Kodaira-Spencer isomorphism. This isomorphism extends to the algebraic world as an isomorphism $\omega_{X_1(N),\mathbb{Z}[1/N],2} \cong \Omega^1_{X_1(N)/\mathbb{Z}[1/N]}(cusps)$, where the isomorphism is given by $(\frac{\mathrm{d}u}{u})^{\otimes 2} \mapsto \frac{\mathrm{d}q}{q}$ at the Tate curve.

This discussion shows cusp forms of weight two for $X_1(N)$ over a ring R can be interpreted as global sections of $\Omega^1_{\mathbf{X}_1(N)/R}$.

4. The modular curves $X_0(N)$ and $X_\mu(N)$.

In the sections on $Y_1(N)$ and $X_1(N)$ we saw that these curves parametrize elliptic curves together with a point of order N. The curves $Y_0(N)$ and $X_0(N)$ are the curves that parametrize elliptic curves together with a cyclic subgroup of order N.

The complex setting will be described first. Define

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

and recall that if $\tau \in \mathbb{H}$, then E_τ denotes the curve $\mathbb{C}/(\tau\mathbb{Z}+\mathbb{Z})$. In the discussion on $\mathbf{Y}_1(N)$ it was shown that if $\tau_1, \tau_2 \in \mathbb{H}$ then pairs $(E_{\tau_1}, 1/N)$ and $(E_{\tau_2}, 1/N)$ are isomorphic if and only if there exists a γ in $\Gamma_1(N)$ such that $\tau_2 = \gamma\tau_1$. Similarly one can show, replacing the point $1/N \in E_\tau$ by the subgroup generated by $1/N$, that $(E_{\tau_1}, \langle 1/N\rangle)$ and $(E_{\tau_2}, \langle 1/N\rangle)$ are isomorphic if and only if there exists a $\gamma \in \Gamma_0(N)$ such that $\tau_2 = \gamma\tau_1$. This shows that over $\mathbb{C}$ the isomorphism classes of pairs (E, G) of elliptic curve together with a cyclic subgroup of order N are in one to one correspondence with $\Gamma_0\backslash\mathbb{H}$. So the modular curve $\mathbf{Y}_0(N)$ is defined to be $\Gamma_0\backslash\mathbb{H}$. One can compactify $\mathbf{Y}_0(N)$ in a similar way to $\mathbf{Y}_1(N)$ and the resulting compactification will be denoted by $\mathbf{X}_0(N) = \Gamma_0\backslash\mathbb{H}^*$.

Note that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$ so that we could also have constructed $\mathbf{Y}_0(N)$ and $\mathbf{X}_0(N)$ as quotients of $\mathbf{Y}_1(N)$ and $\mathbf{X}_1(N)$ by $\Gamma_0(N)/\Gamma_1(N)$. The map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ given by $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto d$ is a surjective group homomorphism whose kernel is $\Gamma_1(N)$ showing that $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$. One can even interpret the action of $(\mathbb{Z}/N\mathbb{Z})^*$ on $\mathbf{X}_1(N)$ directly, since $d \in (\mathbb{Z}/N\mathbb{Z})^*$ corresponds to sending the pair (E, P) of elliptic curve with point of order N to (E, dP). The automorphism of $X_1(N)$ corresponding to $d \in (\mathbb{Z}/N\mathbb{Z})^*$ is denoted by $\langle d\rangle$ and is called a *diamond operator*.

The action of $d \in (\mathbb{Z}/N\mathbb{Z})^*$ given by by $(E, P) \mapsto (E, dP)$ also makes sense in the algebraic world and gives an action on the $\mathbb{Z}[\frac{1}{N}]$-schemes $Y_1(N)$ and $X_1(N)$. One uses this action to define the modular curves $Y_0(N)$ resp. $X_0(N)$ to be $Y_1(N)/(\mathbb{Z}/N\mathbb{Z})^*$ resp. $X_1(N)/(\mathbb{Z}/N\mathbb{Z})^*$. We saw that $Y_1(N)(R)$ can be identified with the set of isomorphism classes of pairs (E, P) of elliptic curve together over R with a point of order N for all $\mathbb{Z}[\frac{1}{N}]$-algebras R. However for $Y_0(N)$ this property fails. A pair (E, G) of elliptic curve over R together with a cyclic subgroup of order N still gives rise to an R valued point on $Y_0(N)$, but non isomorphic pairs (E_1, G_1) and (E_2, G_2) might

give the same R point of $Y_0(N)$. Although in the case $R = \overline{K}$ is an algebraically closed field then $Y_0(N)(R)$ can still be identified with the set of isomorphism classes of elliptic curves with a point of order N, as we already saw over $\mathbb{C}$. An additional problem with $\mathbf{Y}_0(N)$ and $Y_0(N)$ is that there is no universal elliptic curve over them. If one tries to define the universal elliptic curve $\mathbf{E}_0(N) := (\mathbb{Z}^2 \rtimes \Gamma_0(N))\backslash(\mathbb{C} \times \mathbb{H})$ over $\mathbf{Y}_0(N)$, similar to what was done for $\mathbf{E}_1(N)$, then one runs into problems. This definition would still give a curve over $\mathbf{Y}_0(N) := \Gamma_0(N)\backslash\mathbb{H}$, however the proof that the fiber of $\mathbf{E}_1(N)$ over $\Gamma_1(N)\tau \in \mathbf{X}_1(N)$ is isomorphic to E_τ uses that $\Gamma_1(N)$ acts freely on $\mathbb{H}$ under the assumption $N > 4$. This is no longer true for $\Gamma_0(N)$, in fact since $-\mathrm{Id} := \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \in \Gamma_0(N)$ and $-\mathrm{Id}$ acts trivially on $\mathbb{H}$ we see that the fiber of $\mathbf{E}_0(N)$ above $\Gamma_0(N)\tau$ is a quotient of $E_\tau/\pm 1$ which is not an elliptic curve, but something isomorphic to $\mathbb{P}^1(\mathbb{C})$. One has similar problems with trying to construct the universal elliptic curve over $X_0(N)$,

4.1. **Modular forms on $X_0(N)$.** The complex analytic definition of a modular form in Definition 3.1 is general enough to also work if one takes $\Gamma = \Gamma_0(N)$. However the algebraic definition 3.3 for modular forms on $X_1(N)$ uses the existence of the universal elliptic curve $E_1(N)$ over $X_1(N)$. This leads to problems when trying to define modular forms on $X_0(N)$, since we saw previously that we have no universal elliptic curve in this case. However these problems can by solved. Namely let R be a $\mathbb{Z}[\frac{1}{N}]$-algebra and let $\pi : X_1(N) \to X_0(N)$ denote the quotient map, then $\pi_*\omega_{X_1(N),R,k}$ is a sheaf on $X_0(N)$ with an action of $(\mathbb{Z}/N\mathbb{Z})^*$, taking $(\mathbb{Z}/N\mathbb{Z})^*$ invariants gives the desired sheaf of $X_0(N)$.

Definition 4.1. Let $N > 4$ and k be integers and R a $\mathbb{Z}[\frac{1}{N}]$ algebra. Define

$$\omega_{X_0(N),R,k} := (\pi_*\omega_{X_1(N),R,k})^{(\mathbb{Z}/N\mathbb{Z})^*}.$$

An R *valued modular form of weight k for $X_0(N)$* is a global section f of $\omega_{X_1(N),R,k}$. A modular form f is called a cusp form if it has zeros at all cusps, i.e. it is zero on $X_0(N)_R \setminus Y_0(N)_R$.

Let R be a flat $\mathbb{Z}[\frac{1}{N}]$-algebra, then $\Omega^1_{X_0(N)/R} \cong (\pi_*\Omega^1_{X_1(N)/R})^{(\mathbb{Z}/N\mathbb{Z})^*}$. This means that the Kodaira-Spencer isomorphism $\omega_{X_1(N),\mathbb{Z}[1/N],2} \cong \Omega^1_{X_1(N)/\mathbb{Z}[1/N]}(cusps)$ descends to an isomorphism $\omega_{X_0(N),\mathbb{Z}[1/N],2} \cong \Omega^1_{X_0(N)/\mathbb{Z}[1/N]}(cusps)$, showing that one can still see cusp forms over R as one forms. However if R is a ring that is not flat over $\mathbb{Z}[\frac{1}{N}]$ there are some troubles that can arise, especially rings of characteristic 2 and 3 pose problems. More details on different ways of viewing cusp forms as differential forms and the difficulties that arise in characteristics 2 and 3 can be found in [Mazur(1977), §II.4].

4.2. **The modular curve $X_\mu(N)$.**. The modular curve $X_\mu(N)$ is just a slight variation on the modular curve $X_1(N)$. The curve $X_1(N)$ parametrizes pairs (E, P) of an elliptic curve together with a point of order N, or equivalently pairs (E, α) where $\alpha : \mathbb{Z}/N\mathbb{Z} \to E$ is a closed immersion of the constant group scheme into

E. The modular curve $X_\mu(N)$ parametrizes pairs (E,β) where $\beta : \mu_N \to E$ is a closed immersion of the group of N-th roots of unity into E. Since over $\mathbb{Z}[\frac{1}{N},\zeta_N]$ one has $\mu_N \cong \mathbb{Z}/N\mathbb{Z}$, one sees that $X_1(N)_{\mathbb{Z}[1/N,\zeta_N]} \cong X_\mu(N)_{\mathbb{Z}[1/N,\zeta_N]}$. This isomorphism shows in particular that $X_1(N)$ and $X_\mu(N)$ are isomorphic over all algebraically closed fields and that $X_\mu(N)$ and $X_1(N)$ are twists of each other over $\mathbb{Z}[\frac{1}{N},\zeta_N]$. Since $\zeta_N \in \mathbb{C}$ there is nothing that really changes in the complex world so that we still can see $X_\mu(N)(\mathbb{C})$ as $\mathbf{X}_1(N) = X_1(N)(\mathbb{C})$. However over rings not containing ζ_N there is a difference. The twisting of $X_1(N)$ that gives $X_\mu(N)$ can even be made explicit by the isomorphism

$$X_\mu(N) \cong \left(X_1(N) \times_{\mathbb{Z}[\frac{1}{N}]} \mathbb{Z}\left[\frac{1}{N},\zeta_N\right]\right)/(\mathbb{Z}/N\mathbb{Z})^*,$$

where $d \in (\mathbb{Z}/N\mathbb{Z})^*$ acts on $X_1(N)$ via the diamond operator $\langle d\rangle$ and on $\mathbb{Z}[\frac{1}{N},\zeta_N]$ via $\zeta_N \mapsto \zeta_N^d$. In contrast to $X_0(N)$, the modular curve $X_\mu(N)$ does have a universal elliptic curve over it. This universal elliptic curve is denoted by $E_\mu(N)$ and the entire story about modular forms on $X_1(N)$ translates directly to a description of the modular forms on $X_\mu(N)$. For a $\mathbb{Z}[\frac{1}{N}]$ algebra R one can define

$$\omega_{X_\mu(N),R,k} := \left(0^*\Omega^1_{E_\mu(N)_R/X_\mu(N)_R}\right)^{\otimes k}.$$

similar to Definition 3.3, and say that an R-valued modular form of weight k on $X_\mu(N)$ is a global section of $\omega_{X_\mu(N),R,k}$. Also the Kodaira-Spencer isomorphism $\omega_{X_\mu(N),\mathbb{Z}[1/N],2} \cong \Omega^1_{X_\mu(N)/\mathbb{Z}[1/N]}(cusps)$ continues to exist.

References

[Deligne and Rapoport(1975)] P. Deligne and M. Rapoport. Correction to: "Les schémas de modules de courbes elliptiques" (*modular functions of one variable, ii* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316, Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973). In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages p. 149. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[Mazur(1977)] 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`.

[Silverman(1994)] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ISBN 0-387-94328-5. doi: 10.1007/978-1-4612-0851-8. URL `http://dx.doi.org/10.1007/978-1-4612-0851-8`.

CHAPTER 2

Gonality of the modular curve $X_1(N)$

GONALITY OF THE MODULAR CURVE $X_1(N)$

MAARTEN DERICKX AND MARK VAN HOEIJ

Abstract. In this paper we compute the gonality over $\mathbb{Q}$ of the modular curve $X_1(N)$ for all $N \leqslant 40$ and give upper bounds for each $N \leqslant 250$. This allows us to determine all N for which $X_1(N)$ has infinitely points of degree d where d is either 5 or 6. We conjecture that the modular units of $\mathbb{Q}(X_1(N))$ are freely generated by $f_2, \ldots, f_{\lfloor N/2 \rfloor + 1}$ where f_k is obtained from the equation for $X_1(k)$.

1. Introduction

Notation 1. *If K is a field, and C/K is a curve*[1]*, then $K(C)$ is the function field of C over K. The gonality* $\mathrm{Gon}_K(C)$ *is* $\min\{\deg(f) \mid f \in K(C) - K\}$*. In this article we are interested in the case $C = X_1(N)$, and K is either $\mathbb{Q}$ or $\mathbb{F}_p$.*

It was shown in [Der12] that if $C/\mathbb{Q}$ is a curve and p is a prime of good reduction of then:

$$\mathrm{Gon}_{\mathbb{F}_p}(C) \leqslant \mathrm{Gon}_{\mathbb{Q}}(C). \tag{1}$$

A similar statement was given earlier in [Fre94] which attributes it to [Deu42]. We use (1) only for $C = X_1(N)$. The primes of good reduction of $X_1(N)$ are the primes $p \nmid N$.

The main goal in this paper is to compute $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$ for $N \leqslant 40$. The $\mathbb{Q}$-gonality for $N \leqslant 22$ was already known [Sut12, p. 2], so the cases $23 \leqslant N \leqslant 40$ are of most interest. For each N, it suffices to:

- Task 1: Compute a basis of $\mathrm{div}(\mathcal{F}_1(N))$, which denotes the set of divisors of modular units over $\mathbb{Q}$, see Definition 1 in Section 2 for details.
- Task 2: Use LLL techniques to search $\mathrm{div}(\mathcal{F}_1(N))$ for the divisor of a non-constant function g_N of lowest degree.
- Task 3: Prove (for some prime $p \nmid N$) that $\mathbb{F}_p(X_1(N)) - \mathbb{F}_p$ has no elements of degree $< \deg(g_N)$. Then (1) implies that the $\mathbb{Q}$-gonality is $\deg(g_N)$.

Table 1: $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$ for $N \leqslant 40$. Upper bounds for $N \leqslant 250$.

[1]In this paper, a *curve* over a field K is a scheme, projective and smooth of relative dimension 1 over $\mathrm{Spec}\, K$ that is geometrically irreducible.

N	1	2	3	4	5	6	7	8	9	10
gon $=$	1	1	1	1	1	1	1	1	1	1
N	11	12	13	14	15	16	17	18	19	20
gon $=$	2	1	2	2	2	2	4	2	5	3
N	21	22	23	24	25	26	27	28	29	30
gon $=$	4	4	7	4	5	6	6	6	11	6
N	31	32	33	34	35	36	37	38	39	40
gon $=$	12	8	10	10	12	8	18	12	14	12
N	41	42	43	44	45	46	47	48	49	50
gon $\leqslant$	22	12	24	15	18	19	29	16	21	15
N	51	52	53	54	55	56	57	58	59	60
gon $\leqslant$	24	21	37	18	30	24	30	31	46	24
N	61	62	63	64	65	66	67	68	69	70
gon $\leqslant$	49	36	36	32	42	30	58	36	44	36
N	71	72	73	74	75	76	77	78	79	80
gon $\leqslant$	66	32	70	51	40	45	60	42	82	48
N	81	82	83	84	85	86	87	88	89	90
gon $\leqslant$	54	58	90	48	72	64	70	60	104	48
N	91	92	93	94	95	96	97	98	99	100
gon $\leqslant$	84	66	80	83	90	56	123	63	90	60
N	101	102	103	104	105	106	107	108	109	110
gon $\leqslant$	133	72	139	84	96	105	150	72	156	90
N	111	112	113	114	115	116	117	118	119	120
gon $\leqslant$	114	96	167	90	132	105	126	120	144	96
N	121	122	123	124	125	126	127	128	129	130
gon $\leqslant$	132	139	140	120	125	96	211	112	154	126
N	131	132	133	134	135	136	137	138	139	140
gon $\leqslant$	225	120	180	156	144	144	246	132	253	144
N	141	142	143	144	145	146	147	148	149	150
gon $\leqslant$	184	189	210	128	210	184	168	171	291	120
N	151	152	153	154	155	156	157	158	159	160
gon $\leqslant$	299	180	216	180	240	168	323	234	234	184
N	161	162	163	164	165	166	167	168	169	170
gon $\leqslant$	264	162	348	210	240	240	365	192	260	216
N	171	172	173	174	175	176	177	178	179	180
gon $\leqslant$	270	231	392	210	240	240	290	274	420	192
N	181	182	183	184	185	186	187	188	189	190
gon $\leqslant$	429	252	310	264	342	240	360	276	288	270
N	191	192	193	194	195	196	197	198	199	200
gon $\leqslant$	478	224	488	328	336	252	508	240	519	240
N	201	202	203	204	205	206	207	208	209	210
gon $\leqslant$	374	382	420	288	420	398	396	336	450	288
N	211	212	213	214	215	216	217	218	219	220
gon $\leqslant$	583	351	420	396	462	288	480	445	444	360
N	221	222	223	224	225	226	227	228	229	230
gon $\leqslant$	504	342	651	384	360	444	675	360	687	396
N	231	232	233	234	235	236	237	238	239	240
gon $\leqslant$	480	420	711	336	552	435	520	432	748	384
N	241	242	243	244	245	246	247	248	249	250
gon $\leqslant$	761	396	486	465	504	420	630	480	574	375

Tasks 1–3 are only possible when:

(a) There is a modular unit g_N of degree $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$.
(b) There is a prime $p \nmid N$ for which $\mathrm{Gon}_{\mathbb{F}_p}(X_1(N)) = \mathrm{Gon}_{\mathbb{Q}}(X_1(N))$.

We have completed Tasks 1–3 for $1 < N \leqslant 40$, and hence (a),(b) are true in this range. We do not know if they hold in general.

We implemented two methods for Task 1. Our webpage [DvH] gives the resulting basis of $\mathrm{div}(\mathcal{F}_1(N))$ for $N \leqslant 300$. For Task 2, for each $4 \leqslant N \leqslant 300$ we searched $\mathrm{div}(\mathcal{F}_1(N))$ for short[2] vectors, and placed the best function we found, call it g_N, on our webpage [DvH]. The degree of any non-constant function is by definition an upper bound for the gonality. Table 1 gives $\deg(g_N)$ for $N \leqslant 250$.

Finding the shortest vector in a $\mathbb{Z}$-module is NP-hard. For large N, this forced us to resort to a probabilistic search (we randomly scale our vectors, apply an LLL search, and repeat). So we can not prove that every g_N on our webpage is optimal, even if we assume (a).

For certain N (e.g. $N = p^2$, see Section 4) there are other ways of finding functions of low degree. Sometimes a good function can be found in a subfield of $\mathbb{Q}(X_1(N))$ over $\mathbb{Q}(X_1(1))$, see [DvH]. All low degree functions we found with these methods were also found by our probabilistic LLL search. So the upper bounds in Table 1 are likely sharp when (a) holds (Question 1 in Section 2.2).

At the moment, our only method to prove that an upper bound is sharp is to complete Task 3, which we have done for $N \leqslant 40$. The computational cost of Task 3 increases drastically as a function of the gonality. Our range $N \leqslant 40$ contains gonalities that are much higher than the previous record, so in order to perform Task 3 for all $N \leqslant 40$ it was necessary to introduce several new computational ideas.

Upper bounds (Tasks 1 and 2) will be discussed in Section 2, and lower bounds (Task 3) in Section 3. We cover $N = 37$ separately (Theorem 1), this case is the most work because it has the highest gonality in our range $N \leqslant 40$. Sharp lower bounds for other $N \leqslant 40$ can be obtained with the same ideas. Our computational proof (Task 3) for each $N \leqslant 40$ can be verified by downloading the Magma files from [DvH].

Remark 1. *For each $N \leqslant 40$, the $\mathbb{Q}$-gonality happened to be the $\mathbb{F}_p$-gonality for the smallest prime $p \nmid N$. That was fortunate because the computational complexity of Task 3 depends on p.*

We can not expect the $\mathbb{F}_p$-gonality to equal the $\mathbb{Q}$-gonality for every p. For example, consider the action of diamond operator $<12>$ on $\mathbb{C}(X_1(29))$. The fixed field has index 2 and genus 8 (type: `GammaH(29,[12]).genus()` *in Sage). By Brill-Noether theory, this subfield contains a function f_{BN} of degree $\leqslant \lfloor (8+3)/2 \rfloor = 5$. Viewed as element of $\mathbb{C}(X_1(29))$, its degree is $\leqslant 2 \cdot 5$ which is less than the $\mathbb{Q}$-gonality[3] 11. By*

[2]We want vectors with small 1-norm because $\deg(g) = \frac{1}{2}||\mathrm{div}(g)||_1$.
[3]We do not know if there are other $N \leqslant 40$ with $\mathbb{C}$-gonality $\neq$ $\mathbb{Q}$-gonality.

Chebotarev's theorem, there must then be a positive density of primes p for which the $\mathbb{F}_p$-gonality of $X_1(29)$ is less than 11.

2. Modular equations and modular units

Definition 1. *A non-zero element of $\mathbb{Q}(X_1(N))$ is called a* modular unit *(see* [KL81]*) when all its poles and roots are cusps. Let $\mathcal{F}_1(N) \subset \mathbb{Q}(X_1(N))^*/\mathbb{Q}^*$ be the group of modular units mod $\mathbb{Q}^*$.*

There are $\lfloor N/2 \rfloor + 1$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps, denoted[4] *as $C_0, \ldots, C_{\lfloor N/2 \rfloor}$. Let*

$$\mathcal{D}_1(N) := \mathbb{Z}C_0 \oplus \cdots \oplus \mathbb{Z}C_{\lfloor N/2 \rfloor}$$

be the set of $\mathbb{Q}$-rational cuspidal divisors. The degree[5] *of $\sum n_i C_i$ is $\sum n_i \deg(C_i)$. Denote $\mathcal{D}_1^0(N)$ as the set of cusp-divisors of degree 0, and*

$$\mathcal{C}_1(N) := \mathcal{D}_1^0(N)/\mathrm{div}(\mathcal{F}_1(N)),$$

a finite group called the cuspidal class group*.*

Let E be an elliptic curve over a field K, and P be a point on E of order exactly N. If $N \geqslant 4$ and $\mathrm{char}(K) \nmid N$, one can represent the pair (E, P) in *Tate normal form:*

$$Y^2 + (1-c)XY - bY = X^3 - bX^2, \quad \text{with the point } (0,0). \tag{2}$$

This representation is unique and hence b, c are functions on pairs (E, P). The function field $K(X_1(N))$ is generated by b, c. Whenever we use the notation b or c, we implicitly assume $N \geqslant 4$, because the reduction to (2) succeeds if and only if $N \geqslant 4$. This implies (for $N \geqslant 4$) that poles of b, c must be cusps. The discriminant of (2) is $\Delta := b^3 \cdot (16b^2 + (1 - 20c - 8c^2)b + c(c-1)^3)$ so E degenerates when $\Delta = 0$. So all roots of Δ (and hence of b) are cusps. Poles of Δ, b are cusps because poles of b, c are cusps. So Δ, b are modular units, and hence

$$F_2 := b^4/\Delta \;=\; \frac{b}{16b^2 + (1 - 20c - 8c^2)b + c(c-1)^3} \quad \text{and} \quad F_3 := b$$

are modular units as well.

For $N \geqslant 4$, the functions b, c on $X_1(N)$ satisfy a polynomial equation $F_N \in \mathbb{Z}[b, c]$, namely (for $N = 4, 5, 6, 7, \ldots$) $\;c,\;\; b - c,\;\; c^2 + c - b,\;\; b^2 - bc - c^3, \ldots$

If $k \neq N$, the condition that the order of P is k is incompatible with the condition that the order is N. This, combined with the observation that all poles of b, c are

[4]Let $d|N$, $0 \leqslant i < d$, with $\gcd(i, d) = 1$ and let j be such that the point $P_{d,i,j} = (i, \zeta_N^j)$ has order N in the Neron d-gon $\mathbb{Z}/d\mathbb{Z} \times \mathbb{G}_m$. Let $C_{d,i,j}$ be the cusp corresponding to $P_{d,i,j}$, then $C_{d,i,j}$ and $C_{d',i',j'}$ are in the same Galois orbit iff $d = d'$ and $i \equiv \pm i' \bmod d$. We denote the Galois orbit of $C_{d,i,j}$ as C_n where $0 \leqslant n \leqslant N/2$ and $n \equiv \pm iN/d \bmod N$. With this numbering, the diamond operator $\langle i \rangle$ sends C_n to $C_{n'}$ where $n' \equiv \pm ni \bmod N$.

[5]The degree of C_i is as follows. Let $d = \gcd(i, N)$. If $i \in \{0, N/2\}$ then $\deg(C_i) = \lceil \phi(d)/2 \rceil$, otherwise $\deg(C_i) = \phi(d)$, where ϕ is Euler's function.

cusps, implies (for $N, k \geqslant 4$) that the *modular equation* F_k is a *modular unit* for $X_1(N)$. We define a subgroup of $\mathcal{F}_1(N)$ generated by *modular equations*[6]:

$$\mathcal{F}_1'(N) := < F_2, F_3, \ldots, F_{\lfloor N/2 \rfloor + 1} > \subseteq \mathcal{F}_1(N).$$

Conjecture 1. *$\mathcal{F}_1'(N) = \mathcal{F}_1(N)$ for $N \geqslant 3$. In other words, $\mathcal{F}_1(N)$ is freely generated by modular equations $F_2, \ldots, F_{\lfloor N/2 \rfloor + 1}$.*

We verified this for $N \leqslant 100$, see also Section 2.1. The conjecture holds for $N = 3$ because F_2 rewritten to j, x_0 coordinates generates $\mathcal{F}_1(3)$. The case $N = 2$ is a little different, clearly F_2 can not generate $\mathcal{F}_1(2)$ since it must vanish on $X_1(2)$. However, rewriting F_2F_4 to j, x_0 coordinates produces a generator for $\mathcal{F}_1(2)$. The conjecture is only for $\mathbb{Q}$; if $X_1(N)_K$ has more than $\lfloor N/2 \rfloor + 1$ Galois orbits of cusps, for example $X_1(5)_K$ with $K = \mathbb{C}$ or $K = \mathbb{F}_{11}$, then the rank of $\mathcal{F}_1'(N)$ would be too low.

2.1. **Computations.** As N grows, the size of F_N grows quickly. Sutherland [Sut12] obtained smaller equations by replacing b, c with other generators of the function field. For $6 \leqslant N \leqslant 9$, use r, s defined by

$$r = \frac{b}{c},\ s = \frac{c^2}{b-c},\quad b = rs(r-1),\ c = s(r-1)$$

and for $N \geqslant 10$, use x, y defined by

$$x = \frac{s-r}{rs-2r+1},\ y = \frac{rs-2r+1}{s^2-s-r+1},\quad r = \frac{x^2y-xy+y-1}{x(xy-1)},\ s = \frac{xy-y+1}{xy}.$$

The polynomial defining $X_1(N)$ is then written as $f_4 := c$, $f_5 := b - c$, $f_6 := s - 1$, $f_7 := s - r$, $f_8 := rs - 2r + 1$, $f_9 := s^2 - s - r + 1$, $f_{10} := x - y + 1$, $f_{11} := x^2y - xy^2 + y - 1$, $f_{12} := x - y$, $f_{13} := x^3y - x^2y^2 - x^2y + xy^2 - y + 1$, etc. Explicit expressions for $f_{10}, \ldots, f_{189} \in \mathbb{Z}[x, y]$ can be downloaded from Sutherland's website `http://math.mit.edu/~drew/X1_altcurves.html`.

The same website also lists upper bounds for the gonality for $N \leqslant 189$, that are often sharp when N is prime. Table 1 improves this bound for every composite $N > 26$, a few composite $N < 26$, but only three primes: 31, 67, and 101. When N is prime, we note that Sutherland's [Sut12] bound, $\deg(x)$, equals $[11N^2/840]$ where

[6]An equation is called a modular equation for $X_1(k)$ if it corresponds to P having order k. A computation is needed to show that F_2, F_3 are modular equations in this sense. The fact that F_2 and F_3 correspond to order 2 and 3 is obscured by the b, c coordinates, so we introduce j, x_0 coordinates for $X_1(N)$ that apply to any $N > 1$ provided that $j \notin \{0, 1728\}$. Here x_0 is the x-coordinate of a point P on $y^2 = 4x^3 - 3j(j-1728)x - j(j-1728)^2$. The condition that P has order 2 or 3 can be expressed with equations $\tilde{F}_2, \tilde{F}_3 \in \mathbb{Q}[j, x_0]$. These $\tilde{F}_2, \tilde{F}_3$ are functions on $X_1(N)$ for any $N > 1$. Hence they can (for $N > 3$) be rewritten to b, c coordinates. To obtain modular units, we have to ensure that all poles and roots are cusps, which requires an adjustment: $F_2 := \tilde{F}_2^2/(j^2(j-1728)^3)$ and $F_3 := \tilde{F}_3^3/\tilde{F}_2^4$.

the brackets denote rounding to the nearest integer ($[11N^2/840]$ is a valid upper bound for any $N > 6$, but it is not very sharp for composite N's).

Let $f_2 := F_2$ and $f_3 := F_3$. Then $F_k/f_k \in < f_2, \dots, f_{k-1} >$ for each $k \geqslant 2$. In particular

$$\mathcal{F}_1'(N) = < f_2, f_3, \dots f_{\lfloor N/2 \rfloor + 1} > .$$

For each $3 \leqslant N \leqslant 300$ and $2 \leqslant k \leqslant \lfloor N/2 \rfloor + 1$ we calculated $\mathrm{div}(f_k) \in \mathcal{D}_1(N)$. This data can be downloaded (in row-vector notation) from our webpage [DvH]. This data allows one to determine $\mathcal{D}_1^0(N)/\mathrm{div}(\mathcal{F}_1'(N))$ for $N \leqslant 300$. If that is $\cong \mathcal{C}_1(N)$, then the conjecture holds for N. We tested this by computing $\mathcal{C}_1(N)$ with Sage[7] for $N \leqslant 100$. The $\mathrm{div}(f_k)$-data has other applications as well:

Example 1. *Let $N = 29$. Suppose one wants to compute explicit generators for the subfield of index 2 and genus 8 mentioned in Remark 1. Let $\tilde{x}, \tilde{y}$ denote the images of x, y under the diamond operator $<12>$. Clearly $\tilde{x}x$, $\tilde{y}y$ are in our subfield, which raises the question: How to compute $\tilde{x}, \tilde{y}$?*

Observe that $x = f_7/f_8$ and $y = f_8/f_9$ (The relations $1-x = f_5f_6/(f_4f_8)$, $1-y = f_6f_7/f_9$, $1-xy = f_6^2/f_9$ may be helpful for other examples.) So we can find $\mathrm{div}(x)$ by subtracting the (7-1)'th and (8-1)'th row-vector listed at [DvH] *for $N = 29$. We find $(0, -1, -2, -3, -1, 0, 0, 0, 3, 2, -1, -3, 2, 3, 1)$ which encodes $\mathrm{div}(x) =$*

$$-C_1 - 2C_2 - 3C_3 - C_4 + 3C_8 + 2C_9 - C_{10} - 3C_{11} + 2C_{12} + 3C_{13} + C_{14}.$$

The diamond operator $<12>$ sends C_i to $C_{\pm 12i \bmod N}$ and hence $\mathrm{div}(\tilde{x}) =$

$$2C_1 - C_4 - 2C_5 + C_6 - 3C_7 + 2C_8 + 3C_9 - C_{10} + 3C_{11} - C_{12} - 3C_{13}.$$

Since $\mathrm{div}(f_2), \dots, \mathrm{div}(f_{15})$ are listed explicitly at [DvH]*, solving linear equations provides $n_2, \dots, n_{15}$ for which $\mathrm{div}(\tilde{x}) = \sum n_i \mathrm{div}(f_i)$. Setting $g := \prod f_i^{n_i} =$*

$$\frac{(x^2y - xy + y - 1)(x-1)^2(x - y + 1)(x^2y - xy^2 - x^2 + xy - x + y - 1)^4y^3}{(y-1)^2(xy-1)(x-y)(x^2y - xy^2 - xy + y^2 - 1)^4x^4},$$

it follows that $\tilde{x} = cg$ for some constant c (c is not needed here, but it can be determined easily by evaluating $\tilde{x}$ and g at a point.) Repeating this computation for y, we find explicit expressions for $\tilde{x}x$, $\tilde{y}y$. An algebraic relation can then be computed with resultants; it turns out that $\tilde{x}x$, $\tilde{y}y$ generate the subfield.

2.2. **Explicit upper bound for the gonality for $N \leqslant 40$.** The following table lists for each $10 < N \leqslant 40$ a function of minimal degree. We improve the upper bound from Sutherland's website (mentioned in the previous section) in 16 out of these 30 cases.

11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
x	x	x	x	x	y	x	h_1	x	x	h_1	x	x	h_1	h_2
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
y	h_3	h_3	x	h_5	h_1	h_4	h_6	h_1	h_7	h_8	x	h_2	h_9	h_5

[7]The $\mathbb{Z}$-module of modular units is computed with modular symbols by determining the $\sum n_i c_i \in \mathbb{Z}^{\mathrm{cusps}}$ of degree 0 with $\sum n_i \{c_i, \infty\} \in H_1(X_1(N)(\mathbb{C}), \mathbb{Z}) \subset H_1(X_1(N)(\mathbb{C}), \mathbb{Q})$.

Here

$$h_1 = \frac{x^2y - xy^2 + y - 1}{(x-y)x^2y}, \quad h_2 = \frac{x(1-y)(x^2y - xy^2 - xy + y^2 - 1)}{(x-y+1)(x^2y - xy^2 + y - 1)},$$
$$h_3 = \frac{(1-x)(x^2y - xy^2 - xy + y^2 - 1)}{(x-y)(x^2y - xy^2 + y - 1)}, \quad h_4 = \frac{(1-x)(x^2y - xy^2 + y - 1)}{x(1-y)},$$
$$h_5 = \frac{(1-y)(x^2y - xy^2 - xy + y^2 - 1)}{(x-y)y(x-y+1)}$$
$$h_6 = \frac{f_{10}f_{11}f_{12}}{f_{17}}, \quad h_7 = \frac{f_{17}}{f_{18}}, \quad h_8 = \frac{f_{14}f_{17}^2}{f_{19}^2}, \quad h_9 = \frac{f_{12}f_{13}f_{14}}{f_{19}}.$$

Each $h_1, \ldots, h_9$ is in the multiplicative group $< f_2, f_3, \ldots >$. To save space, we only spelled out $h_1, \ldots, h_5$ in x, y-notation (the f_{19} that appears in h_9 is substantially larger than the f_{11} that appears in h_1). Similar expressions for $N \leqslant 300$ are given on our website [DvH].

Question 1. *Does $\mathbb{Q}(X_1(N))$ always contain a modular unit of degree equal to the $\mathbb{Q}$-gonality?*

It does not suffice to restrict to rational cusps (C_i's of degree 1) because then $N = 36$ would be the first counter example. Question 1 may seem likely at first sight, after all, it is true for $N \leqslant 40$. However, we do not conjecture it because the function $f_{\mathrm{BN}} \in \mathbb{C}(X_1(29))$ from Remark 1 is not a modular unit over $\mathbb{C}$, but unlike Conjecture 1, there is no compelling reason to restrict Question 1 to $\mathbb{Q}$.

3. Lower bound for the gonality

Task 3 is equivalent to showing that the Riemann-Roch space $H^0(X_1(N), D)$ is $\mathbb{F}_p$ for every divisor $D \geqslant 0$ of degree $< \deg(g_N)$. This is a finite task, because over $\mathbb{F}_p$, the number of such D's is finite. For $N = 37$, the $\mathbb{Q}$-gonality is 18, and the number of D's over $\mathbb{F}_2$ with $D \geqslant 0$ and $\deg(D) < 18$ is far too large to be checked one by one on a computer. So we will need other methods to prove:

Theorem 1. *Let $f \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$. Then $\deg(f) \geqslant 18$.*

Definition 2. *Let $f \in K(X_1(N))$. The support $\mathrm{Supp}(\mathrm{Div}(f))$ is $\{P \in X_1(N)_K \mid v_P(f) \neq 0\}$, i.e., the set of places where f has a non-zero valuation (a root or a pole). Let $\mathrm{mdeg}_K(f)$ denote $\max\{\deg_K(P) \mid P \in \mathrm{Supp}(\mathrm{Div}(f))\}$. Likewise, if $D = \sum n_i P_i$ is a divisor, then $\mathrm{mdeg}_K(D) := \max\{\deg_K(P_i) \mid n_i \neq 0\}$.*

Overview of the proof of Theorem 1:
We split the proof in two cases: Section 3.2 will prove Theorem 1 for the case $\mathrm{mdeg}(f) = 1$. Section 3.3 will introduce notation, and prove Theorem 1 for the case $\mathrm{mdeg}(f) > 1$. (Task 3 for the remaining $N \leqslant 40$ is similar to Section 3.3 but easier, and will be discussed in Section 3.4.)

3.1. **The $\mathbb{F}_2$ gonality of $X_1(37)$.** In [Der12] there are already tricks for computing the $\mathbb{F}_p$ gonality of a curve in a computationally more efficient way than the brute force method from earlier papers. These tricks were not efficient enough to compute the $\mathbb{F}_2$ gonality of $X_1(37)$. However, by subdividing the problem, treating one part with lattice reduction techniques, and the other part with tricks from [Der12], the case $N = 37$ becomes manageable on a computer. We divide the problem as follows:

Proposition 1. *If there is a $g \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ with $\deg(g) \leqslant 17$ then there is an $f \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ with $\deg(f) \leqslant 17$ that satisfies at least one of the following conditions:*

1. $\mathrm{mdeg}(f) = 1$
2. *all poles of f are rational cusps, and f has $\geqslant 10$ distinct poles.*
3. *f has a pole at $\geqslant 5$ rational cusps and at least one non-rational pole.*

Proof. $X_1(37)$ has 18 $\mathbb{F}_2$-rational places, all of which are cusps. View g as a morphism $X_1(37)_{\mathbb{F}_2} \to \mathbb{P}^1_{\mathbb{F}_2}$. For all $h \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_2})$ we have $\deg(g) = \deg(h \circ g)$. If there is $h \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_2})$ such that $\mathrm{mdeg}(h \circ g) = 1$ then take $f = h \circ g$ and we are done. Now assume that such h does not exist. Then at least two of the three sets $g^{-1}(\{0\}), g^{-1}(\{1\}), g^{-1}(\{\infty\})$ contain a non-rational place. If all three do, then the one with the most rational cusps has at least $18/\#\mathbb{P}^1(\mathbb{F}_2) = 6 > 5$ rational cusps and we can take $f = h \circ g$ for some $h \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_2})$. Otherwise we can assume without loss of generality that $g^{-1}(\{\infty\})$ only contains rational cusps. If $g^{-1}(\{\infty\})$ contains at least 10 elements then we can take $f = g$. If $g^{-1}(\{\infty\})$ contains at most 9 elements then $g^{-1}(\{0\}) \cup g^{-1}(\{1\})$ contains at least $18 - 9 = 9$ rational cusps, so either $g^{-1}(\{0\})$ or $g^{-1}(\{1\})$ contains at least 5, and we can take $f = 1/g$ or $f = 1/(1-g)$. □

3.2. **The case $N = 37$ and mdeg = 1.**

Proposition 2. *Every $f \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ with $\mathrm{mdeg}(f) = 1$ has $\deg(f) \geqslant 18$.*

Proof. Let $M = \mathbb{Z}^{X_1(37)(\mathbb{F}_2)} \subset \mathrm{Div}(X_1(37)_{\mathbb{F}_2})$ be the set of all divisors D with $\mathrm{mdeg}(D) = 1$. Let $N = \ker(M \to \mathrm{Pic}\, X_1(37)_{\mathbb{F}_2})$, i.e. principal divisors in M. Magma can compute N directly from its definition, an impressive feat considering the size of the equation! First download the file `X1_37_AFF.m` from our web-page [DvH]. It contains the explicit equation for $X_1(37)$ over $\mathbb{F}_2$, and assigns it to `AFF` with the Magma command AlgorithmicFunctionField.

```
> load "X1_37_AFF.m";
> plc1 := Places(AFF, 1); //18 places of degree 1, all cusps.
> M := FreeAbelianGroup(18);  gen := [M.i : i in [1..18]];
> ClGrp, m1, m2 := ClassGroup(AFF); //takes about 3 hours.
> N := Kernel(Homomorphism(M, ClGrp, gen, [m2(i) : i in plc1]));
```

Let $\|\_\|_1$ and $\|\_\|_2$ be the standard 1 and 2 norm on M with respect to the basis $X_1(37)(\mathbb{F}_2)$ (i.e. `plc1`). For a divisor $D \in N$ with $D = \mathrm{Div}(g)$ we have $\deg(g) =$

$\frac{1}{2}\|D\|_1$. So we need to show that N contains no non-zero D with $\|D\|_1 \leqslant 2 \cdot 17$. The following calculation shows that N contains no divisors $D \neq 0$ with $\|D\|_2^2 \leqslant 2(14^2+3^2) = 410$ and $\frac{1}{2}\|D\|_1 \leqslant 17$.

```
> //Convert N to a more convenient data-structure.
> N := Lattice(Matrix( [Eltseq(M ! i) : i in Generators(N)] ));
> SV := ShortVectors(N,410);
> Min([&+[Abs(i) : i in Eltseq(j[1])]/2 : j in SV]);
18 1
```

From this we can conclude two things. First, there is a function f of degree 18 with $\mathrm{mdeg}(f) = 1$. We already knew that from our LLL search of $\mathrm{div}(\mathcal{F}_1(37))$, but this is nevertheless useful for checking purposes (see Remark 2 below). Second, if there is a non-constant function f of degree $\leqslant 17$ and $\mathrm{mdeg}(f) = 1$ then $\|\mathrm{Div}\, f\|_2^2 > 2(14^2+3^2)$ so either f or $1/f$ must have a pole of order $\geqslant 15$ at a rational point. Then either f or $1/f$ is in a Riemann-Roch space $H^0(X_1(N)_{\mathbb{F}_2}, 15p+q+r)$ with p, q, r in $X_1(37)(\mathbb{F}_2)$. Since the diamond operators act transitively on $X_1(37)(\mathbb{F}_2)$ we can assume without loss of generality that p is the first element of $X_1(37)(\mathbb{F}_2)$ returned by Magma. The proof of the proposition is then completed with the following computation:

```
> p := plc1[1];
> Max([Dimension(RiemannRochSpace(15*p+q+r)) : q,r in plc1]);
1 1
```

□

Remark 2. *Computer programs could have bugs, so it is reasonable to ask if Magma really did compute a proof of Proposition 2. The best way to check this is with independent verification, using other computer algebra systems.*

We computed $\mathrm{div}(f_k)$*, for* $k = 2, \ldots, \lfloor 37/2 \rfloor + 1$*, in Maple with two separate methods. One is based on determining root/pole orders by high-precision floating point evaluation at points close to the cusps. The second method is based on Puiseux expansions. The resulting divisors are the same. Next, we searched the* $\mathbb{Z}$*-module spanned by these divisors for vectors with a low 1-norm. Maple and Magma returned the same results, but what is important to note is that this search (in characteristic 0) produced the same vectors as the divisors of degree-18 functions (in characteristic 2) that Magma found in the computation for Proposition 2.*

We made similar checks throughout our work. Magma's RiemannRochSpace command never failed to find a function whose existence was known from a computation with another computer algebra system. The structure of Magma's ClassGroup also matched results from computations in Sage and Maple.

The key programs that the proofs of our lower bounds depend on are Magma's RiemannRochSpace program (needed for all non-trivial N*'s), and ClassGroup program (needed for* $N = 37$*). We have thoroughly tested these programs, and are confident that they compute correct proofs.*

3.3. **The case $N = 37$ and mdeg > 1.** It remains to treat cases 2 and 3 of Proposition 1. Let $S_2 \subseteq \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ be the set of all functions f with $\deg(f) \leqslant 17$ such that all poles of f are rational and f has at least 10 distinct poles. Similarly let $S_3 \subseteq \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ be the set of all functions f with $\deg(f) \leqslant 17$ such that f has a pole at at least 5 distinct rational points and a pole at at least 1 non-rational point. To complete the proof of Theorem 1 we need to show:

Proposition 3. *The sets S_2 and S_3 are empty.*

We will prove this with Magma computations, using ideas similar to those in [Der12]. The main new idea is in the following definition:

Definition 3. *Let C be a curve over a field $\mathbb{F}$ and $S \subseteq \mathbb{F}(C) - \mathbb{F}$ a set of non-constant functions. We say that a set of divisors $A \subset \operatorname{Div} C$* dominates *$S$ if for every $f \in S$ there is a $D \in A$ such that $f \in \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C)$ (i.e. $f = g \circ f' \circ h$ for some $g \in \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}})$, $f' \in H^0(C, D)$, and $h \in \operatorname{Aut}(C)$).*

It follows directly from this definition that

$$S \subseteq \bigcup_{D \in A} \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C)$$

and hence:

Proposition 4. *Let C be a curve over a field $\mathbb{F}$, $S \subseteq \mathbb{F}(C) - \mathbb{F}$ and $A \subset \operatorname{Div} C$. Suppose that A dominates S, and that:*

$$\forall_{D \in A}\ S \cap \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C) = \emptyset. \tag{3}$$

Then $S = \emptyset$.

Proof of Proposition 3. Appendix A.1 gives two sets A_2 and A_3 that dominate S_2 and S_3 respectively. The Magma computations given there show that

$$\forall_{D \in A_2 \cup A_3} \min\{\deg(f) \mid f \in H^0(C, D) - \mathbb{F}_2\} \geqslant 18$$

where $C = X_1(37)_{\mathbb{F}_2}$. Since $\deg(f)$ is invariant under the actions of $\operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}})$ and $\operatorname{Aut}(C)$ it follows (for $i = 2, 3$ and $D \in A_i$) that $S_i \cap \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C) = \emptyset$ so we can apply Proposition 4. □

3.4. **The cases $N \leqslant 40$ and $N \neq 37$.** Subdividing the problem into three smaller cases as in Proposition 1 was not necessary for the other $N \leqslant 40$. Instead we used an easier approach which is similar to the case $N = 37$ and mdeg > 1.

For an integer N let p_N denote the smallest prime p such that $p \nmid N$. Let $d_N = \deg(g_N)$ denote the degree of the lowest degree function we found for N (Section 2.2 or online [DvH]). Now in order to prove $\operatorname{Gon}_{\mathbb{Q}}(X_1(N)) \geqslant d_N$ we will prove $\operatorname{Gon}_{\mathbb{F}_{p_N}}(X_1(N)) \geqslant d_N$. We have done this by applying Proposition 4 directly with S the set of all functions of degree $< d_N$. To verify hypothesis (3) from Proposition 4 with a computer for $A = \operatorname{Div}^+_{d_N - 1}(X_1(N)_{\mathbb{F}_{p_N}})$ (i.e. all effective divisors of degree $d_N - 1$) was unfeasible in a lot of cases. Instead we used the following

proposition to obtain a smaller set A of divisors that still dominates all functions of degree $< d_N$.

Proposition 5. *Let C be a curve over a finite field $\mathbb{F}_q$ and d an integer. Let $n := \lceil \#C(\mathbb{F}_q)/(q+1) \rceil$ and*

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

then

$$A := \mathrm{Div}^+_{d-n}(C) + D = \left\{ s' + D \mid s' \in \mathrm{Div}^+_{d-n}(C) \right\}$$

dominates all functions of degree $\leqslant d$.

Proof. For all $f \colon C \to \mathbb{P}^1_{\mathbb{F}_q}$ we have $f(C(\mathbb{F}_q)) \subseteq \mathbb{P}^1(\mathbb{F}_q)$. By the pigeon hole principle, there is a point p in $\mathbb{P}^1(\mathbb{F}_q)$ whose pre-image under f has at least n points in $C(\mathbb{F}_q)$. Moving p to ∞ with a suitable $g \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_q})$, the function $g \circ f$ has at least n distinct poles in $C(\mathbb{F}_q)$. So if $\deg(f) \leqslant d$ then $\mathrm{Div}(g \circ f) \geqslant -s - D$ for some $s \in \mathrm{Div}^+_{d-n}(C)$. □

Proposition 5 reduces the number of divisors to check, but increases their degrees. However, for our case $C = X_1(N)$ the gonality is generally much lower then the genus, so the Riemann-Roch spaces from equation (3) are still so small that it is no problem to enumerate all their elements, and compute their degrees to show $S \cap \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \mathrm{Aut}(C) = \emptyset$.

As a further optimization we can make A even smaller by using the orbits under diamond operators. The Magma computations [DvH] show that hypothesis (3) in Proposition 4 is satisfied for S, the set of functions of degree $< d_N$ in $\mathbb{F}_{p_N}(X_1(N)) - \mathbb{F}_{p_N}$, and A, an explicit set of divisors dominating S.

Despite all our tricks to reduce the number of divisors, the number of divisors for $N = 37$ (due to its high gonality) remained far too high for our computers, specifically, divisors consisting of rational places. We handled those by using the relations between rational places in the Jacobian. That idea (worked out in Section 3.2) allowed us to complete $N = 37$ and thus all $N \leqslant 40$.

4. Patterns in the gonality data

Definition 4. *Let $\Gamma \subseteq \mathrm{PSL}_2(Z)$ be a congruence subgroup and $X(\Gamma) := \mathbb{H}^*/\Gamma$ be the corresponding modular curve over $\mathbb{C}$. The* improvement factor *of a function $f \in \mathbb{C}(X(\Gamma)) - \mathbb{C}$ is the ratio*

$$[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma] / \deg(f) = \deg(j) / \deg(f).$$

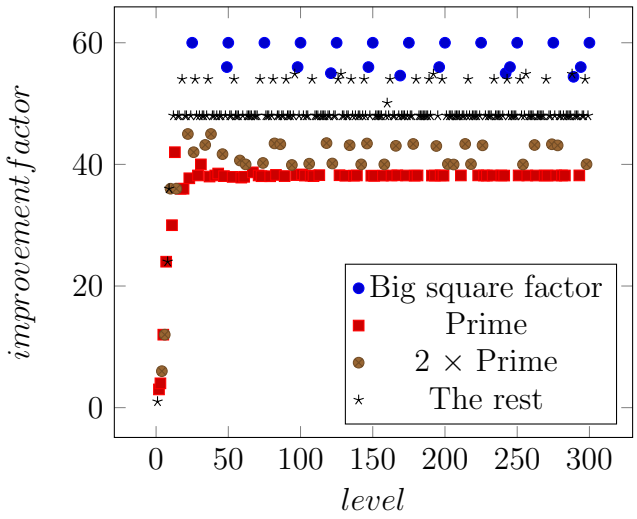
The definition is motivated by a well known bound from Abramovich:

Theorem 2 ([Abr96])**.**

$$\mathrm{Gon}_{\mathbb{C}}(X(\Gamma)) \geqslant \frac{7}{800} [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma].$$

If Selbergs eigenvalue conjecture is true then $7/800$ can be replaced by $1/96$.

The theorem says that an improvement factor can not exceed 800/7, for any Γ, even over $\mathbb{C}$. To compare this with $X_1(N)$ (over $\mathbb{Q}$), we plotted the improvement factors of our g_N's from [DvH]. This revealed a remarkable structure:



What immediately pops out is that our best improvement factor is often 48 (in 151 out of 300 levels N). Levels $N > 9$ with an improvement factor < 48 are either of the form $N = p$ or $N = 2p$ for a prime p. For prime levels, our improvement factor converges to 420/11.

Levels of the form $N = kp^2$ with $p > 3$ prime stand out in the graph, with improvement factors significantly higher than 48. To explain this, first observe that improvement factors for kp^2 are $\geqslant$ those of p^2 because:

Remark 3. *If $\Gamma \subseteq \Gamma'$ are two congruence subgroups, $\pi : X(\Gamma) \to X(\Gamma')$ denotes the quotient map and $f \in \mathbb{C}(X(\Gamma'))$ then f and $f \circ \pi$ have the same improvement factor. So improvement factors for $X(\Gamma')$ can not exceed those for $X(\Gamma)$.*

It remains to explain the high observed improvement factors at levels $N = p^2$:

level	5^2	7^2	11^2	13^2	17^2
improvement	60	56	55	$54\frac{3}{5}$	$54\frac{2}{5}$

The best (lowest degree, highest improvement factor) modular units g_N we found for these five cases turned out to be invariant under a larger congruence subgroup $\Gamma_0(p^2) \cap \Gamma_1(p) \supseteq \Gamma_1(p^2)$. Now

$$\Gamma_0(p^2) \cap \Gamma_1(p) = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma(p) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}^{-1}.$$

This suggests to look at $X(p)$ to find high improvement factors for $X_1(p^2)$.

5. Points of degree 5 and 6 on $X_1(N)$

The values of N for which the curve $X_1(N)$ has infinitely many places of degree d over $\mathbb{Q}$ are known for $d = 1$ (Mazur), $d = 2$ [K86], $d = 3$ [JKL11a] and $d = 4$ [JKL11b]. In this section, we extend this to $d = 5$ and $d = 6$.

Theorem 3. *$X_1(N)$ has infinitely many places of degree $d = 5$ resp. $d = 6$ over $\mathbb{Q}$ if and only if*

- *for $d = 5$: $N \leqslant 25$ and $N \neq 23$.*
- *for $d = 6$: $N \leqslant 30$ and $N \neq 23, 25, 29$.*

The case $X_1(25)$ is by far the most interesting (and the most work) because its set of non-cuspidal places of degree $d = 6$ is finite[8] even though 6 is larger than the $\mathbb{Q}$-gonality of $X_1(25)$! The remainder of this section contains the proof of Theorem 3 and a remark on larger d's.

Lemma 1.

(1) *Let $C/\mathbb{Q}$ be a curve. If C has a function f over $\mathbb{Q}$ of degree d then C has infinitely many places of degree d over $\mathbb{Q}$.*
(2) *If the Jacobian $J(C)(\mathbb{Q})$ is finite, then the converse holds as well. To be precise, if C has more than $\#J(C)(\mathbb{Q})$ places of degree d, then $\mathbb{Q}(C)$ contains a function of degree d.*
(3) *If $N \leqslant 60$ and $N \neq 37, 43, 53, 57, 58$ then $J_1(N)(\mathbb{Q})$ is finite.*
(4) *If $N > 60$ or $N = 37, 43, 53, 57, 58$ then $X_1(N)$ has finitely many places of degree $\leqslant 6$.*

Proof. (1) Hilbert's irreducibility theorem shows that there are infinitely many places of degree d among the roots of $f - q = 0$, $q \in \mathbb{Q}$.

(2) If $n = \#J(C)(\mathbb{Q}) < \infty$ and $P_1, \ldots, P_{n+1}$ are distinct places of degree d, then by the pigeon hole principle, there exist $i \neq j$ with $P_i - P_1 \sim P_j - P_1$. The function giving this linear equivalence has degree d.

(3) Magma has a provably correct algorithm to determine if $L(J_1(N), 1)$ is 0 or not. It shows $L(J_1(N), 1) \neq 0$ for each N in item 3. By a result of Kato this implies that $J_1(N)(\mathbb{Q})$ has rank zero and hence is finite.

(4) The case $N = 58$ follows from the map $X_1(58) \to X_1(29)$ and the fact that $X_1(29)$ has only finitely many points of degree $\leqslant 6$ (by items 3, 2 and Table 1). $\mathrm{Gon}_{\mathbb{Q}}(X_1(37)) = 18$, and a similar computation shows $\mathrm{Gon}_{\mathbb{Q}}(X_1(43)) \geqslant 13$ (this bound is not sharp, but the computational effort increases if we try to prove a better bound). For $N = 53, 57$ or > 60, we find $\frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] > 12$, and Abramovich's bound (Section 4) implies $\mathrm{Gon}_{\mathbb{Q}}(X_1(N)) \geqslant 13$. Now item 4 follows from the main theorem of [Fre94] which states that a curve $C/\mathbb{Q}$ with $C(\mathbb{Q}) \neq \emptyset$ has finitely many places of degree $< \mathrm{Gon}_{\mathbb{Q}}(C)/2$. □

[8] and not empty, we found an explicit example [DvH]

Items 4, 3, 2, and 1 of Lemma 1 reduce Theorem 3 step by step to:

Proposition 6. *$X_1(N)$ has a function over $\mathbb{Q}$ of degree $d = 5$ resp. $d = 6$ if and only if:*

- *for $d = 5$: $N \leqslant 25$ and $N \neq 23$.*
- *for $d = 6$: $N \leqslant 30$ and $N \neq 23, 25, 29$.*

Proof. For each N, d listed here, our divisor data [DvH] makes it easy to find an explicit function in $\mathcal{F}_1(N)$ (Section 2) of degree d. So it suffices to show that there are no such functions in the other cases.

- $N > 40$ and $N \neq 42$: In these cases $\frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] > 6$, so it follows from Abramovich's bound (Section 4).
- $N \leqslant 40$ or $N = 42$ and $(N, d) \neq (25, 6)$: For $N \leqslant 40$ see Table 1. A similar computation (Proposition 5 with $q = 5$, $d = 6$) shows $\mathrm{Gon}_{\mathbb{Q}}(X_1(42)) > 6$.
- $(N, d) = (25, 6)$: We prove this by verifying conditions 1–5 of Proposition 7 below with $C = X_1(25)$, $d = 6$ and $p = 2$.
  1. The rank of $J_1(25)(\mathbb{Q})$ is 0 and $\#J_1(25)(\mathbb{F}_3) = 2503105$ is odd. So $\#J_1(25)(\mathbb{Q})$ is finite and odd and hence $J_1(25)(\mathbb{Q}) \hookrightarrow J_1(\mathbb{F}_2)$.
  2,3 We verified this using a Magma computation (files at [DvH]).
  4. Since $6 - \mathrm{Gon}_{\mathbb{F}_2} X_1(25) = 1$ we only need to show surjectivity of $W_5^1(\mathbb{Q}) \to W_5^1(\mathbb{F}_2)$. A Magma computation shows $\#W_5^1(\mathbb{F}_2) = 1$, and $W_5^1(\mathbb{Q}) \neq \emptyset$ by Table 1.
  5. This is true because $X_1(25)(\mathbb{F}_2)$ consists exactly of the 10 cusps that come from the rational cusps in $X_1(25)(\mathbb{Q})$.

□

For $N \leqslant 40$, applying a `ShortVectors`-search to our divisor data [DvH] shows that $\mathbb{Q}(X_1(N))$ has a function of degree $d \geqslant \mathrm{Gon}_{\mathbb{Q}}(X_1(N))$ if $(N, d) \notin S = \{(25, 6), (25, 7), (32, 9), (33, 11), (35, 13), (39, 15), (40, 13)\}$. The search also showed that there are no modular units with $(N, d) \in S$. Ruling out degree-d functions other than modular units is more work:

Proposition 7. *Let $C/\mathbb{Q}$ with $C(\mathbb{Q}) \neq \emptyset$ be a smooth projective curve with good reduction at a prime p. Let $W_d^r(K)$ denote the closed subscheme of $\mathrm{Pic}^d C(K)$ corresponding to the line bundles $\mathcal{L}$ of degree d whose global sections form a K-vectorspace of dimension $\geqslant r + 1$. Suppose that:*

(1) *$J(C)(\mathbb{Q}) \to J(C)(\mathbb{F}_p)$ is injective.*
(2) *$\mathbb{F}_p(C)$ contains no functions of degree d.*
(3) *$W_d^2(\mathbb{F}_p) = \emptyset$.*
(4) *$W_{d-i}^1(\mathbb{Q}) \to W_{d-i}^1(\mathbb{F}_p)$ is surjective for all $1 \leqslant i \leqslant d - \mathrm{Gon}_{\mathbb{F}_p}(C)$.*
(5) *$C^{(i)}(\mathbb{Q}) \to C^{(i)}(\mathbb{F}_p)$ is surjective for all $1 \leqslant i \leqslant d - \mathrm{Gon}_{\mathbb{F}_p}(C)$.*

Then $\mathbb{Q}(C)$ contains no functions of degree d.

Proof. Item 1 and $C(\mathbb{Q}) \neq \emptyset$ imply that $\mathrm{Pic}^k C(\mathbb{Q})$ to $\mathrm{Pic}^k C(\mathbb{F}_p)$ is injective for all k. To show that $\mathbb{Q}(C)$ has no function of degree d it suffices to show for all $\mathcal{L}$ in $W_d^1(\mathbb{Q})$ that every 2-dimensional subspace $V \subset \mathcal{L}(C)$ has a base point.

Let $\mathcal{L} \in W_d^1(\mathbb{Q})$. Item 3 implies $\dim_{\mathbb{F}_p} \mathcal{L}_{\mathbb{F}_p}(C_{\mathbb{F}_p}) = 2$ and so $\dim_{\mathbb{Q}} \mathcal{L}(C) = 2$. Let $D_{\mathbb{F}_p}$ be the divisor of basepoints of $\mathcal{L}_{\mathbb{F}_p}$ and let i be its degree. Item 2 implies $i \geqslant 1$ and because $\mathcal{L}_{\mathbb{F}_p}(-D_{\mathbb{F}_p}) \in W_{d-i}^1(\mathbb{F}_p)$ we have $i \leqslant d - \mathrm{Gon}_{\mathbb{F}_p}(C)$. By item 5 there is a $D \in C^{(i)}(\mathbb{Q})$ that reduces to $D_{\mathbb{F}_p}$. By the injectivity of $\mathrm{Pic}^{d-i} C(\mathbb{Q}) \to \mathrm{Pic}^{d-i} C(\mathbb{F}_p)$, we know that $\mathcal{L}(-D)$ is the unique point lying above $\mathcal{L}_{\mathbb{F}_p}(-D_{\mathbb{F}_p})$. Then item 4 gives the following inequalities

$$2 \leqslant \dim_{\mathbb{Q}} \mathcal{L}(-D)(C) \leqslant \dim_{\mathbb{Q}} \mathcal{L}(C) = 2.$$

In particular, the unique 2-dimensional $V \subset \mathcal{L}(C)$ has the points in D as base points. □

Remark 4. *To extend Theorem 3 to $d = 7, 8$, we can use the same mathematical arguments; the main difficulty is computational. Our Magma files for Proposition 7 cover $(N, d) = (25, 6)$ and $(25, 7)$. Our divisor data* [DvH] *makes it easy*[9] *to find functions of degree 7 on $X_1(N)$ for $N = 1 \ldots 24, 26, 27, 28, 30$ and functions of degree 8 for $N = 1 \ldots 28, 30, 32, 36$. To prove that these are the only values for which $X_1(N)$ has infinitely many points of degree 7 resp. 8, we need to compute higher lower-bounds for the gonality, specifically*[10] *for $N = 42, 43, 53$ (for $d = 7$) and $N = 42, 43, 44, 46, 48, 53, 57$ (for $d = 8$). For $d = 7$, the lower-bound needed for Frey's theorem is 15, which is 3 less than the bound we managed to compute in Theorem 1. So the number of Riemann Roch spaces needed for $d = 7$ is manageable, however, each Riemann Roch computation for $N = 53$ will likely be slow (we did not attempt this). For $d = 8$, the number of Riemann Roch computations will be much higher.*

New mathematical problems arise for $d = 9$. $X_1(37)$ has a Jacobian with positive rank, and the $\mathbb{Q}$-gonality is 18 so we can not use Frey's theorem to rule out infinitely many places of degree 9. $J_1(37)$ has only one simple abelian sub-variety of positive rank, namely an elliptic curve E isogenous to $X_0^+(37)$. So the question whether $X_1(37)$ has infinitely many places of degree 9 is equivalent to the question whether $W_9^0(X_1(37))$ contains a translate of E. Higher values of d lead to additional mathematical problems, for instance, when $X_1(N)$ has infinitely many places of degree d but no function of degree d.

Appendix A. Magma Calculations

We use one custom function. It takes as input a divisor and gives as output the degrees of all non-constant functions in the associated Riemann-Roch space.

[9] This part takes little CPU time and can easily be done for much larger (N, d)'s.

[10] All but finitely many values of N are handled by an improvement to Abramovich's bound (Remark 4.5 in [BGGP05]) and $N = 58$ is again handled by its map to $X_1(29)$.

```
function FunctionDegrees(divisor)
    constantField := ConstantField(FunctionField(divisor));
    space,map := RiemannRochSpace(divisor);
    return [Degree(map(i)) : i in space | map(i) notin constantField];
end function;
```

We divide the computation according to *type*:

Definition 5. *Write D as*

$$\sum_{i=1}^{k} n_i p_i$$

with p_i distinct places and $n_i \in \mathbb{Z} - \{0\}$ such that $(\deg(p_1), n_1) \geqslant (\deg(p_2), n_2) \geqslant \cdots \geqslant (\deg(p_k), n_k)$ where $\geqslant$ is the lexicographic ordering on tuples. Then type(D) is defined to be the ordered sequence of tuples

$$((\deg(p_1), n_1), (\deg(p_2), n_2), \ldots, (\deg(p_k), n_k)).$$

If $\deg(p_i) = 1$ for all i then $(n_1, \ldots, n_k)$ is a shorter notation for type(D).

For example if $D = P_1 + 3P_2$ where P_1 is a place of degree 5 and P_2 a place of degree 1 then

$$type(D) = ((5, 1), (1, 3)).$$

The type of a divisor is stable under the action of $\mathrm{Aut}(C)$.

A.1. The case $N = 37$ and mdeg > 1.

A.1.1. *Dominating the set S_2.* Let

$$\texttt{cuspsum} := \sum_{p \in X_1(37)(\mathbb{F}_2)} p$$

(short for rational-cusp-sum) be the sum of all $\mathbb{F}_2$ rational places. Then the set

$$A_2' := \{\texttt{cuspsum} + D \mid D = p_1 + \cdots + p_7 \text{ with } p_1, \ldots, p_7 \in X_1(37)(\mathbb{F}_2)\}$$

dominates S_2. However, A_2' contains many divisors. Using divisors of higher degree, of the form $k \cdot \texttt{cuspsum} + \cdots$ for $k = 1, 2, 3$ depending on type(D), we can dominate S_2 with much fewer divisors. To prove:

$$\min\{\deg(f) \mid f \in H^0(X_1(37)_{\mathbb{F}_2}, \texttt{cuspsum} + D) - \mathbb{F}_2\} \geqslant 18 \tag{4}$$

for all $\texttt{cuspsum} + D$ in A_2' we divide the computation: The table below list for each type(D) (a partition of 7) from which Magma calculation we can conclude inequality (4) for that type.

type(D)	calculation
(7), (6, 1) and (5, 2)	1
(5, 1, 1), (4, 3), (4, 2, 1), (4, 1, 1, 1) and (3, 3, 1)	2
(3, 2, 2)	3
(3, 2, 1, 1) and (3, 1, 1, 1, 1)	2
(2, 2, 2, 1), (2, 2, 1, 1, 1), (2, 1, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1)	4

As in Section 3.2, start the computation by loading the file `X1_37_AFF.m`. Next, load the program `FunctionDegrees` and then run the following:

```
> //calculation 1
> p := plc1[1];
> [Dimension(cuspsum + 6*p + 2*P) : P in plc1];
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
> //calculation 2
> Min(&cat[FunctionDegrees(2*cuspsum + 4*p + 2*P) : P in plc1]);
18 105
> //calculation 3
> s := Subsets(SequenceToSet(plc1[2..18]),2);
> &cat[FunctionDegrees(cuspsum + 3*p + 2*(&+PQ)) : PQ in s];
[]
> //calculation 4
> Min(FunctionDegrees(3*cuspsum - 4*p);
18 48
```

The set A_2 in the proof of Proposition 3 is the set of divisors occurring in the four calculations above. Calculation 4 used that if $f \in \mathbb{F}_2(X_1(37))$ has $\deg(f) \leqslant 17$ then at least one of $f, f+1$ has an $\mathbb{F}_2$-rational root since $\#X_1(37)(\mathbb{F}_2) = 18$.

A.1.2. *Dominating the set S_3.* The set

$$A_3' := \{\texttt{cuspsum} + D \mid D \geqslant 0,\ \deg(D) = 12 \text{ with } \geqslant 1 \text{ nonrational place}\}$$

dominates all functions in S_3. This time we break up the computation into the following types where we use the following shorthand notation

$$a(c,d) := \underbrace{(c,d),\ldots,(c,d)}_{a}$$

type(D) covered by calculation #c	c
((12,1)) and ((11, 1),(1,1))	1
((10,1),(1,2)) and ((10,1),(1,1),(1,1))	2
((9,1)(1,3))	3
((9,1),(1,2),(1,1)) and ((9,1),(1,1),(1,1),(1,1))	4
((7,1),(1,5)), ((7,1),(1,4),(1,1)) and ((7,1),(1,3),(1,2))	5
((7,1),(1,3),(1,1),(1,1)) and ((7,1),(1,2),(1,2),(1,1))	6
((7,1),(1,2),3(1,1)) and ((7,1),5(1,1))	7
((6,2)) and ((6,1),(6,1))	8
((6,1),(1,6)), ((6,1),(1,5),(1,1)), ((6,1),(1,4),(1,2)), ((6,1),(1,3),(1,3))	9
((6,1),(1,4),2(1,1)), ((6,1),(1,3),(1,2),(1,1)), ((6,1),3(1,2))	10
((6,1),2(1,2),2(1,1)),((6,1),(1,3),3(1,1)),((6,1),(1,2),4(1,1)),((6,1),6(1,1))	11

$X_1(37)_{\mathbb{F}_2}$ has no places of degrees 2–5 and 8. So any non-rational place contributes at least 6 to $\deg(D)$, a fortunate fact that reduces the number of divisors to a

manageable level. The Magma commands to cover these 11 cases are similar to those in Section A.1.1 and can be copied from [DvH].

Theorem 4. *The values in Table 1 are upper bounds for the gonality of $X_1(N)$ over $\mathbb{Q}$. For $N \leqslant 40$ they are exact values.*

Proof. The functions listed at [DvH] are explicit proofs for the upper bounds in Table 1. Section 3, Appendix A, and the accompanying Magma files on [DvH] prove that the bounds are sharp for $N \leqslant 40$. □

References

[Abr96] D. Abramovich. A linear lower bound on the gonality of modular curves. *Internat. Math. Res. Notices*, **20**:1005–1011, 1996.

[BGGP05] M.H. Baker, E. Gonzalez-Jimenez, J. Gonzalez, B. Poonen. Finiteness results for modular curves of genus at least 2. *American J. of Math.*, **127**(6):1325–1387, 2005.

[Der12] M. Derickx. Torsion points on elliptic curves and gonalities of modular curves. Master's thesis, Universiteit Leiden, 2012.

[Deu42] M. Deuring. Reduktion algebraischer funktionenkörper nach primdivisoren des konstantenkörpers. *Mathematische Zeitschrift*, **47**(1):643–654, 1942.

[DvH] M. Derickx and M. van Hoeij. `www.math.fsu.edu/~hoeij/files/X1N` Files: `gonality` (upper bounds with explicit functions g_N, and an overview), `Subfields` (other sources of upper bounds) `cusp_divisors` (divisors of $f_2, f_3, \ldots$), and folder `LowerBoundsGonality` (Magma files for proving lower bounds).

[Fre94] G. Frey. Curves with infinitely many points of fixed degree. *Israel Journal of Mathematics*, **85**(1-3):79–83, 1994.

[JKL11a] D. Joen, C.H. Kim, and Y. Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Mathematics of Computation*, **80**, 579–591, 2011.

[JKL11b] D. Joen, C.H. Kim, and Y. Lee. Families of elliptic curves over quartic number fields with prescribed torsion subgroups. *Mathematics of Computation*, **80**, 2395–2410, 2011.

[K86] S. Kamienny. Torsion points on elliptic curves over all quadratic fields. *Duke Mathematics Journal*, **53**, 157–162, 1986.

[KL81] D. Kubert and S. Lang. *Modular Units (Grundlehren der mathematischen Wissenschaften)*. Springer, 1981.

[Sut12] A.V. Sutherland. Constructing elliptic curves over finite fields with prescribed torsion. *Math. Comp.*, **81**(278):1131–1147, 2012.

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.

E-mail address: `maarten@mderickx.nl`

Department of Mathematics, Florida State University, Tallahassee, Florida 32306, USA.

Supported by NSF grants 1017880 and 1319547.

E-mail address: `hoeij@math.fsu.edu`

CHAPTER 3

Torsion points on elliptic curves over number fields of small degree

TORSION POINTS ON ELLIPTIC CURVES OVER NUMBER FIELDS OF SMALL DEGREE

MAARTEN DERICKX, SHELDON KAMIENNY, WILLIAM STEIN, AND MICHAEL STOLL

Abstract. We determine the set $S(d)$ of possible prime orders of K-rational points on elliptic curves over number fields K of degree d, for $d = 4, 5$ and 6.

1. Introduction

For an integer $d \geq 1$, we let $S(d)$ be the set of primes p such that there exists an elliptic curve E over a number field K of degree d with a K-rational point of order p in $E(K)$. The notation Primes(n) will be used to denote the set of all primes $\leq n$. Mazur [1977, 1978] has famously proved that

$$S(1) = \text{Primes}(7).$$

Kamienny [1992b] showed that

$$S(2) = \text{Primes}(13)$$

and Parent [2000, 2003], extending the techniques used by Mazur and Kamienny, proved that

$$S(3) = \text{Primes}(13).$$

In fact $S(d)$ is finite for every d as proven in Merel [1996], and Merel even gave an explicit but super exponential bound on the largest element of $S(d)$. Shortly after Merel proved the finiteness of $S(d)$, Oesterlé managed to improve upon Merel's bound by showing $S(d) \subseteq \text{Primes}((3^{d/2}+1)^2)$ if $d > 3$ and $S(3) \subseteq \text{Primes}(37) \cup \{43\}$. The result of Parent mentioned earlier depends on Oesterlé's bound for $S(3)$ and a hypothesis Parent denoted by $(*)_p$ [Parent, 2000, p. 724] for the primes $p \leq 43$. The hypothesis $(*)_p$ is that the rank of the winding quotient $J^{\mathbf{e}}_\mu(p)$ is zero. Parent already mentioned that $(*)_p$ probably holds for all primes and that this result would follow from results announced by Kato, but these results were not yet published at the time that Parent wrote is article. These results have now indeed been published as Kato [2004]. Details on $J^{\mathbf{e}}_\mu(p)$ and how to do derive $(*)_p$ from the work of Kato are given in Section 4. Oesterlé never published his results, but was kind enough to give us his unpublished notes so that the gap in the literature could be filled. The Appendix of this article contains his arguments for showing that $S(d) \subseteq \text{Primes}((3^{d/2}+1)^2)$ for $d \geq 6$ and $S(d) \subseteq \text{Primes}(410)$ for $d = 3, 4, 5$ as stated in Theorem A.2. His notes also included a section where he further improved the bound on $S(d)$ with

Date: September 7, 2016.

$d = 3, 4, 5$, but these are omitted since we have found it easier to deal with these cases using the techniques developed in the main text.

Theorem 1.1. *Suppose that* $S(d) \subseteq \text{Primes}(2281)$ *for* $3 \leq d \leq 7$*, then*

$$\begin{aligned} S(3) &= \text{Primes}\,(13), \\ S(4) &= \text{Primes}\,(17), \\ S(5) &= \text{Primes}\,(19), \\ S(6) &= \text{Primes}\,(19) \cup \{37\} \qquad \textit{and} \\ S(7) &\subseteq \text{Primes}\,(23) \cup \{37, 43, 59, 61, 67, 71, 73, 113, 127\}\,. \end{aligned}$$

The reason for including the condition $S(d) \subseteq \text{Primes}(2281)$ in the statement is to make it possible for us to give a proof that does not use Oesterlé's bound (Theorem A.1 of the appendix). Theorem A.2 of the appendix tells us that condition $S(d) \subseteq \text{Primes}(2281)$ is satisfied for $3 \leq d \leq 7$ so the conclusion of the above Theorem holds unconditionally. Theorem A.1 actually also implies $S(d) \subseteq \text{Primes}(2281)$ for $3 \leq d \leq 7$, but the proof given in the appendix depends on Theorem 1.1, so we need to use Theorem A.2 to avoid creating circular references. Additionally the reason for reproving the already known result on $S(3)$ is because the results of Parent [2000, 2003] depend on the unpublished results of Oesterlé. We cannot cite Parent in the appendix in order to prove $S(3) \subseteq \text{Primes}(43)$, since we want to give a proof of Oesterlé's unpublished results in the appendix.

From our computation it even follows that $S(7) \subseteq \text{Primes}\,(23) \cup \{37\}$ if the condition $(**)_{d,p,\ell}$ holds for $d = 7$, $p = 43, 59, 61, 67, 71, 73, 113, 127$ and $\ell = 2$.

$$\left.\begin{array}{l}\text{The effective divisors } D \subseteq X_1(p)^{(d)}(\mathbb{F}_\ell) \text{ such that the associated line} \\ \text{bundle } \mathcal{O}_{X_1(p)_{\mathbb{F}_\ell}}(D) \text{ lifts to } \mathbb{Z}_{(\ell)} \text{ are exactly the effective divisors whose} \\ \text{support consists of the cusps mapping to the cusp } 0_{\mathbb{F}_\ell} \text{ of } X_0(p)(\mathbb{F}_\ell).\end{array}\right\} \quad (**)_{d,p,\ell}$$

This condition is easily seen to be true if $p > (\ell^{d/2} + 1)^2$, see Section 5.3, and we managed even to verify it for many $p \leq (2^{d/2} + 1)^2$ and $d \leq 7$. However the verifying of the condition for the $p \leq (2^{d/2} + 1)^2$ and $d \leq 7$ was done using explicit calculations and careful case by case studies. Finding a theoretical argument that also works for $p \leq (\ell^{d/2} + 1)^2$ is of interest though, since if there exists a function $P^{**} : \mathbb{N}_{>0} \to \mathbb{R}$ such that for every integer $d > 0$ and prime p with $p > P^{**}(d)$ one can find an $\ell > 2$ such that $(**)_{d,p,\ell}$ holds, then [Parent, 1999, Thm. 1] shows that $S(d) \subseteq \text{Primes}(\max(P^{**}(d), 65(2d)^6))$. So from the existence of a function $P^{**}(d) < (3^{d/2} + 1)^2$ as above one obtains an improvement upon Oesterlé's bound.

Let $S'(d)$ be the set of primes p such that there exist infinitely many elliptic curves E with a point of order p and pairwise distinct j-invariants over a number field K of degree d. One of course has $S'(d) \subseteq S(d)$. For $d = 1, 2$ or 3 one even has an equality $S'(d) = S(d)$ Mazur [1977], Kamienny [1992b], Jeon et al. [2011a]. There are a lot more $S'(d)$ known, indeed $S'(4) = \text{Primes}(17)$ Jeon et al. [2011b], $S'(5) = S'(6) = \text{Primes}(19)$ and $S'(7) = S'(8) = \text{Primes}(23)$ Derickx and van

Hoeij [2014]. These results, together with the fact that a twist of the elliptic curve $y^2 + xy + y = x^3 + x^2 - 8x + 6$ has a point of order 37 over the degree 6 number field $\mathbb{Q}(\sqrt{5}, \cos(2\pi/7))$ [Elkies, 1998, Eq. 108], show that we only need to prove $\subseteq$ instead of $=$ in Theorem 1.1.

The $\subseteq$ inclusions are obtained by studying the points on $X_1(p)$ over number fields of degree d. Indeed if E is an elliptic curve over a number field K of degree d and $P \in E(K)$ a point of order p, then the pair (E, P) gives rise to a point $s \in X_1(p)(K)$. If one lets $\sigma_1, \ldots, \sigma_d : K \to \overline{\mathbb{Q}}$ be the d different embeddings of K in $\overline{\mathbb{Q}}$ then

$$s^{(d)} := \sum_{i=1}^{(d)} \sigma_i(s) \in X_1(p)^{(d)}(\mathbb{Q}) \tag{1}$$

is a $\mathbb{Q}$ rational point on the d-th symmetric power of $X_1(p)$. Conversely, every point in $X_1(p)^{(d)}(\mathbb{Q})$ can be written as $\sum_{i=1}^{m} n_i s_i^{(d_i)}$ with $s_i \in X_1(K_i)$, K_i a number field of degree d_i and $n_i \in \mathbb{N}_{>0}$. So the question whether $p \in S(d)$ can be answered if one can find all $\mathbb{Q}$ rational points on $X_1(p)^{(d)}$.

In Section 3 some general theory is developed that, if certain conditions are met, allows one to find all rational points on the symmetric powers of a curve. This theory is similar to the Chabauty for symmetric powers of curves in Siksek [2009], except for the fact that we use formal immersions, as done in Mazur [1978] and Kamienny [1992a], instead of the p-adic integration used by Siksek. As we will see later, this allows us to work over discrete valuation ring with smaller residue characteristic than Siksek. The discussion of Mazur and Kamienny is specific to modular curves, whereas in Section 3 we took care to write down how their arguments work out for arbitrary curves. The most essential part of Section 3 for obtaining Theorem 1.1 is the trick of Parent [2000] that allows one to also work over discrete valuation rings in characteristic 2: this trick is the use of assumption (3) instead of assumption (1) of Proposition 3.4 .

In Section 5 we spell out very explicitly what the results of Section 3 mean when applied to modular curves, giving several variations on the strategies of finding all rational points on symmetric powers of modular curves as a corollary of Section 3. We even work out the strategy explicitly enough so that it can be tested by a computer program written in Sage [2014]. Most cases were handled quite easily by this computer program, although the proof that $29, 31, 41 \notin S(d)$ for $d \leq 7$ and $73 \notin S(6)$ required some extra attention.

Acknoweldgements. We would like to thank Barry Mazur and Bas Edixhoven for their many valuable comments and suggestions, Pierre Parent for his suggestion to look at CM elliptic curves in order to show that $73 \notin S(6)$, and Tessa Schild for her proofreading.

2. Formal Immersions

Definition / Proposition 2.1 (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 one of 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 $\phi^*\colon \mathrm{Cot}_y(Y) \to \mathrm{Cot}_x(X)$ 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 $\mathrm{Cot}_y(Y)$ 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 all 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:

Lemma 2.2. *Let X, Y be Noetherian schemes. Let R be a Noetherian local ring, with maximal ideal m and residue field $k = R/m$. Suppose $f\colon X \to Y$ is a 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, we will 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 $\widehat{P_m^*} = \widehat{Q_m^*}$. Because R is Noetherian local ring, the map $R \to \widehat{R}$ is injective and hence $P_m^* = Q_m^*$. The proposition now follows from the following commuting diagrams:

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

□

3. Rational points on symmetric powers of curves

This section contains a very general discussion on rational points on symmetric powers of curves similar to [Siksek, 2009, §3]. There is a huge overlap where both the results of [Siksek, 2009, §3] and this section are applicable. However, both Siksek's and our own results are applicable in situations where the others result is not; both the overlap and differences will be discussed.

Throughout this section R will be a discrete valuation ring whose residue field k is perfect. Its fraction field will be denoted by K and its maximal ideal by $\mathfrak{m}$. If C is a smooth and projective curve over R, such that C_K is geometrically irreducible, then its Jacobian J exists. Let J^0 be the fiberwise connected component of 0, which is isomorphic to $\mathrm{Pic}^0_{C/R}$ and semi-Abelian [Bosch et al., 1990, §9.7 Cor. 2]. Since C is smooth over R, actually $J^0 = J$ and the special fiber of J is an Abelian variety, hence J is an Abelian scheme over R.

For any R-scheme S and any $x \in C^{(d)}(S)$, define

$$f_{d,x} : C^{(d)}_S \to J_S \tag{2}$$

as the map that for all S-schemes T and all $D \in C^{(d)}_S(T)$ sends D to the class of $\mathcal{O}_{C_T}(D - x_T)$ in $J_S(T)$, where we use [Bosch et al., 1990, §9.3 Prop. 3] to see the points in $C^{(d)}_S(T)$ as effective relative Cartier divisors of degree d on C_T over T.

The following Lemma is the key Lemma which will be used throughout this paper to study the rational points on $C^{(d)}$.

Lemma 3.1. *Let C be a smooth and projective curve over R with geometrically irreducible generic fiber and Jacobian J. Let $t : J \to A$ be a map of Abelian schemes* [1] *over R. Let $y \in C^{(d)}_k(k)$ and assume that the following conditions hold:*

1. *$t(J^1(R)) = \{0\}$, where $J^1(R) := \ker\left(J(R) \overset{\mathrm{red}}{\to} J(k)\right)$,*
2. *the map $t \circ f_{d,y} : C^{(d)}_k \to A_k$ is a formal immersion at y.*

Then there is at most one point in $C^{(d)}(R)$ whose reduction is y.

Proof. If there is no point in $C^{(d)}(R)$ whose reduction is y, then there is nothing to prove, so let $x \in C^{(d)}(R)$ be a point whose reduction is y. Then condition 2 above ensures that $t \circ f_{d,x} : C^{(d)} \to A$ is a formal immersion at y. Indeed, both $\mathrm{Cot}_y C^{(d)} / \mathrm{Cot}_y C^{(d)}_k$ and $\mathrm{Cot}_y A / \mathrm{Cot}_y A_k$ are canonically isomorphic with $\mathfrak{m}/\mathfrak{m}^2 = \mathrm{Cot}_k R$, hence the surjectivity of ${t \circ f_{d,x}}^* : \mathrm{Cot}_0 A \to \mathrm{Cot}_y C^{(d)}$ follows from the surjectivity of $(t \circ f_{d,y})^* : \mathrm{Cot}_0 A_k \to \mathrm{Cot}_y C^{(d)}_k$. Now let $x' \in C^{(d)}(R)$ be a point

[1] one could even more generally take t to be a map from the formal group of J to a formal group F over R, and replace $f_{d,y}$ by $\widehat{f_{d,y}} : \mathrm{Spf}\,\widehat{\mathcal{O}_{C^{(d)}_k,y}} \to \mathrm{Spf}\,\widehat{\mathcal{O}_{J_k,0}}$. But in the case where we want to apply this lemma the Abelian variety J_K is of GL_2 type and hence J had enough endomorphisms to not need to use the formal group version

whose reduction is y, then condition 1 together with $f_{d,x}(x')_k = 0_k = f_{d,x}(x)_k$ imply that $t \circ f_{d,x}(x') = 0_R = t \circ f_{d,x}(x)$. Finally, according to Lemma 2.2 the fact that $t \circ f_{d,x}$ is a formal immersion implies $x' = x$. □

The most straightforward way to turn the above Lemma into a way to determine all rational points in $C^{(d)}(R)$ is the following:

Theorem 3.2. *Let C be a curve that is smooth and projective over R such that C_K is geometrically irreducible, and let J denote its Jacobian over R. Let d be a positive integer and $S \subseteq C^{(d)}(R)$ be a finite set. Let $t : J \to A$ be a map of Abelian schemes over R, denote by red_k the reduction to k map and $\mu : C^{(d)} \to \mathrm{Pic}^d_{C/R}$ the map sending a divisor to its associated line bundle. Assume that the following conditions hold:*

1. *$t(J^1(R)) = \{0\}$, where $J^1(R) := \ker\left(J(R) \overset{red}{\to} J(k)\right)$,*
2. *the map $t \circ f_{d,s} : C^{(d)}_k \to A_k$ with $f_{d,s}$ as in Eq. (2) is a formal immersion at all $s \in \mathrm{red}_k(S)$ and*
3. *$\mathrm{red}_k(S) = \mu^{-1}(\mathrm{red}_k(\mathrm{Pic}^d_{C/R}(R)))$.*

Then $S = C^{(d)}(R)$.

Proof. Condition 3 ensures that $\mathrm{red}_k(C^{(d)}(R)) = \mathrm{red}_k(S)$, and the first two conditions together with Lemma 3.1 ensure that every point in $\mathrm{red}_k(S)$ has exactly one point in $C^{(d)}(R)$ reducing to it. □

In the above theorem however the set S might be huge, and it might get impractical to verify condition 2 explicitly in concrete examples. It turned out that this is the case in the situation where we want to apply it. However in our setup there will often exist a map of curves $\phi : C \to D$ such that the set S for which we want to prove $S = C^{(d)}(R)$ is the inverse image of a single point under $\phi^{(d)} : C^{(d)}(R) \to D^{(d)}(R)$. The following generalization of the above theorem whose proof is similar will be useful in these cases.

Theorem 3.3. *Let C and D be smooth and projective curves over R whose generic fibers are geometrically irreducible. Let $\phi : C \to D$ be a non constant map. Denote by J the Jacobian of D over R. Let d be a positive integer and $S \subseteq C^{(d)}(R)$ and $T \subseteq D^{(d)}(R)$ be finite sets such that $S = {\phi^{(d)}}^{-1}(T) \subseteq C^{(d)}(R)$. Let $t : J \to A$ be a map of Abelian schemes over R, denote by $\mu : C^{(d)} \to \mathrm{Pic}^d_{C/R}$ the map sending a divisor to its associated line bundle. Assume that the following conditions hold:*

1. *$t(J^1(R)) = \{0\}$, where $J^1(R) := \ker\left(J(R) \overset{\mathrm{red}}{\to} J(k)\right)$,*
2. *the map $t \circ f_{d,s} : D^{(d)}_k \to A_k$ with $f_{d,s}$ as in Eq. (2) is a formal immersion at all $s \in \mathrm{red}_k(T)$ and*
3. *$\phi^{(d)}(\mu^{-1}(\mathrm{red}_k(\mathrm{Pic}^d_{C/R}(R)))) \subseteq \mathrm{red}_k(T)$.*

Then $S = C^{(d)}(R)$.

$$\begin{array}{ccccc} & & S & \longrightarrow & T \\ & & \downarrow & & \downarrow \\ \mathrm{Pic}^d_{C/R}(R) & \xleftarrow{\mu} & C^{(d)}(R) & \xrightarrow{\phi^{(d)}} & D^{(d)}(R) \\ \downarrow{\scriptstyle \mathrm{red}_k} & & \downarrow{\scriptstyle \mathrm{red}_k} & & \downarrow{\scriptstyle \mathrm{red}_k} \\ \mathrm{Pic}^d_{C/R}(k) & \xleftarrow{\mu} & C^{(d)}(k) & \xrightarrow{\phi^{(d)}} & D^{(d)}(k) \end{array}$$

Proof. Condition (3) ensures that

$$\mathrm{red}_k(\phi^{(d)}(C^{(d)}(R))) = \phi^{(d)}(\mathrm{red}_k(C^{(d)}(R))) \subseteq \mathrm{red}_k(T),$$

and the first two conditions together with Lemma 3.1 ensure that every point in $\mathrm{red}_k(T)$ has exactly one point in $D^{(d)}(R)$ reducing to it. So we can conclude that $\phi^{(d)}(C^{(d)}(R)) = T$ hence the theorem follows from the assumption $S = {\phi^{(d)}}^{-1}(T)$. □

Remark. Theorems 3.2 and 3.3 are still true if one lets t depend on s. Theoretically this is not a huge gain since one can always take $t : J \to A$ to be the universal map of Abelian schemes such that (1) holds. However, if one wants to restrict the choice of t to $t \in \mathrm{End}_R J$, then the elements such that (1) holds form a two sided ideal $I \subseteq \mathrm{End}_R J$. If this ideal is not principal then it might pay to use a t that depends on s.

If condition (3) of Theorem 3.2 holds, then taking $T = \phi^{(d)}(S)$ ensures that (3) of Theorem 3.3 holds. However, even in the case that (3) of Theorem 3.2 fails to hold for $S = C^{(d)}(R)$, it might still be possible to find an $\phi : C \to D$ and a $T \subseteq D^{(d)}(R)$ such that (3) of Theorem 3.3 holds. The only case where we will make use of this is for showing $73 \notin S(6)$. There we found a $\mathbb{Q}$ rational point $x^{(6)} \in (X_1(73)/\langle 10 \rangle)^{(6)}(\mathbb{Q})$ that was the only $\mathbb{Q}$-rational point in its residue class mod 2. We could show that none of the points $X_1(73)^{(6)}(\overline{\mathbb{Q}})$ mapping to $x^{(6)}$ were defined over $\mathbb{Q}$, hence we could show that the 4 points in $X_1(73)^{(6)}(\mathbb{F}_2)$ mapping to $x^{(6)}_{\mathbb{F}_2}$ had no $\mathbb{Q}$-rational points above them.

If the curve C is a smooth curve over some global field and one has generators for a finite index subgroup of the Mordell-Weil group of (a quotient of) J, then instead of using Theorem 3.2 or Theorem 3.3 for a single prime, one could even use the Mordell-Weil sieve as described in [Siksek, 2009, §5] to combine the information about the rational points of $C^{(d)}$ obtained by Lemma 3.1 for several primes. This however, was not necessary for our purposes.

In the setting where we want to apply Lemma 3.1, the ring R will be $\mathbb{Z}_{(\ell)}$. In this case $J^1(R)$ is a finite index subgroup of $J(R)$ and hence we need $t(J(R))$ to be finite in order for condition (1) to be satisfied. Conversely if $t(J(R))$ is finite, then there are some quite mild conditions on t, A and R that imply that condition(1) is satisfied.

Proposition 3.4. *Suppose that $R = \mathbb{Z}_{(\ell)}$ and $t(J(R))$ is finite and either*

(1) $\ell > 2$,
(2) $\ell = 2$ *and* $A(R)[2]$ *injects into* $A(\mathbb{F}_2)$, *or*
(3) $\ell = 2$ *and* $t = t_2 \circ t_1$ *where* $t_1 : J \to A', t_2 : A' \to A$ *are maps of Abelian schemes such that* $t_1(J(R))$ *is finite and* t_2 *kills all the elements in* $A'(R)[2]$ *that reduce to* 0 *mod* 2.

then condition (1) *of Lemma 3.1 is satisfied.*

Proof. If either $\ell > 2$, or $\ell = 2$ and $A(R)[2]$ injects into $A(k)$, then $t(J(R)) \to A(k)$ is injective, hence $t(J^1(R)) = \{0\}$ which deals with the first two cases. Alternatively one could see them as special cases of the third one with $t_2 = 1$. In the third case we know that $t_1(J^1(R))$ is finite and contained in the kernel of reduction. But a $\mathbb{Z}_{(2)}$ valued torsion point that specializes to the identity mod 2 on a group scheme must be a two torsion point [Parent, 2000, Lem 1.7]. This means that $t_1(J^1(R)) \subset A'(R)[2]$ and hence $t_2 \circ t_1(J^1(R)) = \{0\}$ by the definition of t_2. □

A more general statement of the above proposition over arbitrary discrete valuation rings of unequal characteristics also easily obtained by using [Parent, 2000, Prop 2.3] in the proof instead of Lemma 1.7 of loc. cit.. Bu

In the case that the map t of Lemma 3.1 is the identity map, condition (2) of that Lemma can be nicely restated in terms of $C^{(d)}_{2,k}$ where $C^{(d)}_{2,k} \subseteq C^{(d)}_k$ is defined as the closed sub-variety corresponding to the divisors D over $\bar{k}$ of degree d such that $H^0(C_{\bar{k}}, \mathcal{O}_{C_{\bar{k}}}(D))$ is a $\bar{k}$ vector space whose dimension is at least 2.

Proposition 3.5. *Let $y \in C^{(d)}_k(\bar{k})$ be a point then the map $f_{d,y} : C^{(d)}_{\bar{k}} \to J_{\bar{k}}$ is a formal immersion at y if and only if $y \notin C^{(d)}_{2,k}(\bar{k})$. In particular if $C(k) \neq \emptyset$, then $f_{d,y}$ is a formal immersion at all points in $C^{(d)}_k(k)$ if and only if $k(C_k)$ contains no non-constant functions of degree $\leq d$.*

Proof. Since the map $\mathcal{L} \mapsto \mathcal{L}(-y)$ induces an isomorphism $\mathrm{Pic}^d C_k \to J$, we see that $f_{d,y}$ is a formal immersion at y if and only if the canonical map $C^{(d)}_k \to \mathrm{Pic}^d_{C_k/k}$ is. The map $C^{(d)}_k \setminus C^{(d)}_{2,k} \to \mathrm{Pic}^d_{C_k/k}$ is an isomorphism onto its image, which proves the "if"-part. For the "only if"-part one just notices that if $y \in C^{(d)}_{2,k}$, then the connected component of y of the fiber of $f_{d,y}$ above $0 = f_{d,y}(y)$ contains a $\mathbb{P}^1$. The tangent directions inside this $\mathbb{P}^1$ at y are all send to 0 by $f_{d,y}$ hence it is not a formal immersion. □

Let C be as in the above proposition, let $x \in C_k$ be a closed point, $k(x)$ be its residue field and $q \in \widehat{O_{C_k,x}}$ be a uniformizer. The completed local ring $\widehat{\mathcal{O}_{C_k,x}}$ is isomorphic to $k(x)[[q]]$, and if we have a global 1-form $\omega \in \Omega^1_{C_k/k}(C_k)$, then we can

write its pullback to $\widehat{\mathcal{O}_{C_k,x}}$ as $f\mathrm{d}q$ with f in $\widehat{\mathcal{O}_{C_k,x}}$, hence we can write:

$$\omega_{\mathcal{O}_{C_k,x}} = \sum_{n=1}^{\infty} a_n q^{n-1}\mathrm{d}q, \quad a_n \in k(x). \tag{3}$$

The right hand side of the above formula is called the q-expansion of ω.

The map $f_{1,x} : C_{k(x)} \to J_{k(x)}$ induces an isomorphism $f_{1,x}^* : H^0(J_{k(x)}, \Omega^1) \to H^0(C_{k(x)}, \Omega^1)$ and evaluation in zero gives an isomorphism $H^0(J_{k(x)}, \Omega^1) \to \mathrm{Cot}_0 J_{k(x)}$. If $\omega' \in \mathrm{Cot}_0 J_{k(x)}$ corresponds to $\omega \in H^0(C_{k(x)}, \Omega^1)$ under these isomorphisms then we also say that $\sum_{n=1}^{\infty} a_n q^{n-1}\mathrm{d}q$ is the q-expansion of ω'.

The following complete local rings are equal

$$\widehat{\mathcal{O}_{C^{(d)}_{k(x)},dx}} = k(x)[[q_1,\ldots,q_d]]^{S_d} = k(x)[[\sigma_1,\ldots,\sigma_d]] \tag{4}$$

where q_i is the pullback of q along the i'th projection map $\pi_i : C^d_{k(x)} \to C_{k(x)}$ and $\sigma_1 := q_1 + \cdots + q_d$ up to $\sigma_d := q_1 q_2 \cdots q_d$ are the elementary symmetric polynomials in q_1 up to q_d. Let $\overline{\mathrm{d}\sigma_i}$ denote the image of $\mathrm{d}\sigma_i$ in $\mathrm{Cot}_{dx} C^{(d)}_{k(x)}$, then $\overline{\mathrm{d}\sigma_1}$ up to $\overline{\mathrm{d}\sigma_d}$ form a basis of $\mathrm{Cot}_{dx} C^{(d)}_{k(x)}$. The following Lemma is due to Kamienny and can be found implicitly for example in the proof of Proposition 3.1 of Kamienny [1992a].

Lemma 3.6. *Let d be an integer, C, J and $f_{d,dx} : C^{(d)}_{k(x)} \to J_{k(x)}$ be as in the setup of Lemma 3.1 for $x \in C_k$ a closed point. Let q be a uniformizer at x, q_i, σ_i as above and $\omega \in \mathrm{Cot}_0 J_{k(x)}$ an element with q-expansion $\sum_{n=1}^{\infty} a_n q^{n-1}\mathrm{d}q$. Then*

$$\sum_{n=1}^{d} (-1)^{n-1} a_n \overline{\mathrm{d}\sigma_n} = f_{d,dx}^* \omega \in \mathrm{Cot}_{dx} C^{(d)}_{k(x)}$$

Proof. Let $p : C^d_{k(x)} \to C^{(d)}_{k(x)}$ denote the quotient map then $f_{d,dx} \circ p = \sum_{i=1}^{d} f_{1,x} \circ \pi_i$ where $\pi_i : C^d_{k(x)} \to C_{k(x)}$ denotes the i'th projection map. In particular,

$$(f_{d,dx} \circ p)^*(\omega) = \sum_{n=1}^{\infty} a_n \left(\sum_{i=1}^{d} q_i^{n-1} \mathrm{d}q_i \right).$$

For a ring B consider the map of $B[[\sigma_1,\ldots,\sigma_d]]$-modules

$$D_B : \bigoplus_{j=1}^{d} B[[\sigma_1,\ldots,\sigma_d]]\mathrm{d}\sigma_j \to \bigoplus_{i=1}^{d} B[[q_1,\ldots,q_d]]\mathrm{d}q_i$$

given by $\mathrm{d}\sigma_j \mapsto \sum_{i=1}^{d} \frac{\partial \sigma_j}{\partial q_i}\mathrm{d}q_i$. If we define $s_j := \sum_{i=1}^{d} q_i^j$ for all integers j and $\sigma_j = 0$ for all $j > d$, then Newton's identities give

$$s_n + \sum_{j=1}^{n-1} (-1)^j \sigma_j s_{n-j} = (-1)^{n-1} n \sigma_n.$$

Applying d to this expression shows that

$$(-1)^{n-1}\mathrm{d}\sigma_n - \sum_{i=1}^{d} q_i^{n-1}\mathrm{d}q_i = \frac{1}{n}\mathrm{d}\left(\sum_{j=1}^{n-1}(-1)^j\sigma_j s_{n-j}\right)$$

for $B = \mathbb{Q}$. The right hand side is actually contained in $\bigoplus_{j=1}^{n-1} I\mathrm{d}\sigma_j$ where $I \subset \mathbb{Z}[[\sigma_1, \ldots, \sigma_d]]$ is the ideal generated σ_1 up to σ_d. The proposition follows by base changing $D_{\mathbb{Z}}$ to D_k and quotient out by $\bigoplus_{j=1}^{d} I\mathrm{d}\sigma_j$. □

In the proposition below and its proof we identify $C^{(d)}(k)$ with the set of k rational effective divisors of degree d on C.

Proposition 3.7. *Let $y \in C^{(d)}(k)$ be a point and write $y = \sum_{j=1}^{m} n_j y_j$ with $y_j \in C^{(d)}(\bar{k})$ distinct and $m, n_1, \ldots, n_m \in \mathbb{N}_{>0}$. Let q_j be a uniformizer at y_j, e be a positive integer and $\omega_1, \cdots, \omega_e \in t^*(\mathrm{Cot}_0 A_{\bar{k}}) \subseteq \mathrm{Cot}_0 J_{\bar{k}}$. For $1 \leq i \leq e$ and $1 \leq j \leq m$ let $a(\omega_i, q_j, n_j) := (a_1(\omega_i), \ldots, a_{n_j}(\omega_i))$ be the row vector of the first n_j coefficients of ω_i's q_j-expansion.*

Then $t \circ f_{d,y} : C_k^{(d)} \to A_k$ is a formal immersion at y if the matrix

$$A := \begin{bmatrix} a(\omega_1, q_1, n_1) & a(\omega_1, q_2, n_2) & \cdots & a(\omega_1, q_1, n_m) \\ a(\omega_2, q_1, n_1) & a(\omega_2, q_2, n_2) & \cdots & a(\omega_2, q_1, n_m) \\ \vdots & \vdots & \ddots & \vdots \\ a(\omega_e, q_1, n_1) & a(\omega_e, q_2, n_2) & \cdots & a(\omega_e, q_1, n_m) \end{bmatrix} \tag{5}$$

has rank d. If $\omega_1, \cdots, \omega_e$ generate $t^*(\mathrm{Cot}_0 A_{\bar{k}})$, then the previous statement even becomes an equivalence.

Proof. The natural map $\prod_{j=1}^{m} C_{\bar{k}}^{(n_j)} \to C_{\bar{k}}^{(d)}$ is étale at $(n_1 y_1, n_2 y_2, \ldots, n_m y_m)$, hence we get an isomorphism of cotangent spaces

$$\mathrm{Cot}_y C_{\bar{k}}^{(d)} \cong \bigoplus_{j=1}^{m} \mathrm{Cot}_{d_j y_j} C_{\bar{k}}^{(d_j)}.$$

For j from 1 up to m and $1 \leq i \leq n_j$ let $\sigma_{j,i}$ be the symmetric functions associated to q_j as in (4). The elements $(-1)^{i-1}\overline{\mathrm{d}\sigma_{j,i}}$ with $1 \leq j \leq m$ and $1 \leq i \leq n_j$ form a basis of $\mathrm{Cot}_y C_{\bar{k}}^{(d)}$ under this isomorphism. The corollary follows since if $1 \leq h \leq e$ is an integer then the h'th row of A is just $f_{d,y}^*(\omega_h)$ with respect to this basis. □

If one takes $R = \mathbb{Z}_\ell$ with $\ell > \max_i(n_i)$ then the matrix A in Theorem 1 of Siksek [2009] is obtained by dividing the columns of the matrix A above by certain column dependent integers $\leq \max_i(n_i)$. Actually, there is a huge overlap between Theorem 1 of Siksek [2009] and the result one gets when combining Lemma 3.1 and Proposition 3.7. Our version has the advantage that one doesn't have the conditions $\ell > \max_i(n_i)$. The reason is that the formal immersion criterion, and more generally the formal group over R approach, do not introduce denominators in the matrix A,

while the p-adic logarithm in Siksek's Chabauty approach does introduce them, since it is only defined over K and not over R. Theorem 1 of Siksek [2009] has the advantage that one has more freedom in the choice of the one-forms ω_i. For example, our version is useless if J is simple and has rank $r > 1$, while Siksek's version is still applicable in cases where $r + d \leq g$ where g is the genus of C, although this problem can be mitigated by replacing the map $t : J \to A$ by a map of formal groups in Lemma 3.1. The reason for not using the results of Siksek [2009] is that we really want to take $\ell = 2$, since in general the number of points on $C^{(d)}(\mathbb{F}_\ell)$ is the smallest for $\ell = 2$, so that we need to check the formal immersion condition (2) of Lemma 3.1 for fewer points.

The entire strategy in this section depends on the existence of a map $t : J \to A$ of Abelian varieties whose image contains only finitely many rational points as in Proposition 3.4. The main goal of the following section is to explicitly describe a quotient of J that has only finitely many rational points in the case that C is a modular curve.

4. The winding quotient

In this section we will let N be an integer and $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ a subgroup. The curve X_H over $\mathbb{Z}[1/N]$ is defined to be the quotient curve $X_1(N)/H$ where $(\mathbb{Z}/N\mathbb{Z})^*$ acts as the diamond operators. Taking $H = 1$ gives $X_1(N)$ and $H = (\mathbb{Z}/N\mathbb{Z})^*$ gives $X_0(N)$.

Integration gives a map

$$H_1(X_H(\mathbb{C}), \mathit{cusps}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{C}}(H^0(X_H(\mathbb{C}), \Omega^1), \mathbb{C}) \cong H_1(X_H(\mathbb{C}), \mathbb{R}).$$

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

Definition 4.1. The element $\mathbf{e} := \omega \mapsto \int_{\{0,\infty\}} \omega \in H_1(X_H(\mathbb{C}), \mathbb{Q})$ is called the winding element and the corresponding ideal $\mathcal{A}_{\mathbf{e}} := \mathrm{Ann}(\mathbf{e}) \subseteq \mathbb{T}$, consisting of the elements annihilating $\mathbf{e}$, is called the winding ideal. The quotient $J_H^{\mathbf{e}} := J_H/\mathcal{A}_{\mathbf{e}}J_H$ is called the winding quotient.

One can also define $X_{\mu,H}$ to be the quotient of $X_\mu(N)$ by H. The winding element and the winding quotient can be defined in the same way, and the latter will be denoted by $J_{\mu,H}^{\mathbf{e}}$. The isomorphism

$$W_N \colon X_\mu(N) \to X_1(N) \tag{6}$$

sending $(E, f : \mu_N \to E[N])$ to $(E/\operatorname{im}(f), f^\vee : \mathbb{Z}/N\mathbb{Z} \to E[N]/\operatorname{im}(f))$ is defined over $\mathbb{Z}[1/N]$. It interchanges the cusps 0 and ∞ and commutes with taking the quotient by H. This isomorphism sends the winding ideal of $X_{\mu,H}$ to the winding ideal of X_H and hence we get an isomorphism $J_{\mu,H}^{\mathbf{e}} \cong J_H^{\mathbf{e}}$.

The essential property of the winding quotient is that its group of rational points is finite.

Theorem 4.2. *The rank of $J_H^{\mathbf{e}}(\mathbb{Q})$ and $J_{\mu,H}^{\mathbf{e}}(\mathbb{Q})$ are 0 .*

Merel was in [Merel, 1996, §1] the first one to introduce the winding quotient for $J_0(p)$ with p prime, where he also proves that its rank is finite 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. Parent in [Parent, 1999, §3.8] generalized Merels statement it to composite numbers N. The result of Kolyvagin and Logachev was generalized by Kato [Kato, 2004, Cor. 14.3] to abelian varieties that are a quotient of $J_1(N)_{\mathbb{Q}}$. In both Parent [2000] and Parent [2003] it is mentioned that the theorem follows from using Kato's generalization. Here is a short sketch how to deduce the finiteness of the winding quotient form the work of Kato, where we closely follow the arguments of [Parent, 1999, §3.8].

Proof. Because $J_H^{\mathbf{e}}$ is a quotient of $J_1^{\mathbf{e}}(N)$ and $J_H^{\mathbf{e}} \cong J_{\mu,H}^{\mathbf{e}}$, it suffices to show the theorem for $J_1^{\mathbf{e}}(N)$.

The Hecke algebra $\mathbb{T}_{\mathbb{Q}}$ viewed as subalgebra 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 $\mathbb{Q}$-linear combinations of the Galois conjugates of $B_d(g)$ with $g \in f_i$ and $d \mid N/M_i$ and $B_d\colon X_1(N) \to X_1(M_)$ the degeneracy maps [Parent, 1999, Thm. 3.5]. Now let M be an integer that divides N and d an integer dividing N/M. The degeneracy map $B_d\colon X_1(N) \to X_1(M)$ gives rise to $B_d^*\colon J_1(M)_{\mathbb{Q}} \to J_1(N)_{\mathbb{Q}}$ and we can define

$$J_1(N)_{\mathbb{Q}}^{new} := J_1(N)_{\mathbb{Q}} / \sum_{M|N, M\neq N, d|N/M} \operatorname{im} B_d^*.$$

And we can use the maps $B_{d,*}\colon J_1(N)_{\mathbb{Q}} \to J_1(M)_{\mathbb{Q}}$ to define a map of abelian varieties

$$\Phi\colon J_1(N)_{\mathbb{Q}} \to \bigoplus_{M|N} \bigoplus_{d|N/M} J_1(M)_{\mathbb{Q}}^{new}.$$

Now the identification

$$S_2(\Gamma_1(N))_{\mathbb{C}} \cong H^0(X_1(N)_{\mathbb{C}}, \Omega^1) \cong H^0(J_1(N)_{\mathbb{C}}, \Omega^1) \cong \operatorname{Cot}_0(J_1(N)_{\mathbb{C}}$$

together with the isomorphism $\oplus_{M|N} \oplus_{d|N/M} S^2(\Gamma_1(M))_{\mathbb{C}}^{new} \to S^2(\Gamma_1(M))_{\mathbb{C}}^{new}$ shows 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 $S_2(\Gamma_1(M))$ 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 $\oplus_{j\neq i} R_{f_j}$, with this definition 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 $\langle \mathbf{e}, f_i\rangle$ is non-zero, then $\mathcal{A}_{\mathbf{e},\mathbb{Q}} \cap R_{f_i} = 0$ and conversely that if $\langle \mathbf{e}, f_i\rangle = 0$, then $\mathcal{A}_{\mathbf{e},\mathbb{Q}} \cap R_{f_i} = R_{f_i}$. Now since $L(f_i, 1) = 2\pi\langle \mathbf{e}, f_i\rangle$ we can write

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

Combining this with the previous discussion we get an isogeny

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

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

5. The conditions of 3.3 for $X_\mu(N) \to X_{\mu,H}$.

Let p be a prime. In order to determine $X_1(p)^{(d)}(\mathbb{Q})$, or equivalently $X_\mu(p)^{(d)}(\mathbb{Q})$ by using the isomorphism W_p defined in (6), we will apply Theorem 3.3 to the quotient map $f : X_\mu(p) \to X_{\mu,H}$ where $H \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ is some subgroup such that we manage to verify all conditions. Much of the strategy also works if one drops the assumption that p is a prime.

5.1. **Condition 1: Using the winding quotient.** Let N be an integer, $\ell \nmid N$ a prime and $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ a subgroup. Then we can use Theorem 4.2 to construct a $t : J_{\mu,H} \to A$ for some Abelian variety A such that (1) of 3.3 holds, i.e. such that $t(J^1_{\mu,H}(\mathbb{Z}_{(\ell)})) = 0$ where $J^1_{\mu,H}(\mathbb{Z}_{(\ell)})$ is the kernel of reduction. The combination of this Theorem and this Proposition gives.

Proposition 5.1. *Let $\ell > 2$ be a prime coprime to N then condition* (1) *of 3.3 is satisfied with $R = \mathbb{Z}_{(\ell)}$ for the quotient map $t : J_{\mu,H} \to J^{\mathbf{e}}_{\mu,H}$.*

This proposition will not be used in this text, but it is stated since it allows for comparison with other approaches of determining or bounding $S(d)$.

The proposition above is used for $J_0(p)$ with p prime and an ℓ that depends on p in the argument of Merel [1996], and is used for $J_0(p^n)$ for $\ell = 3$ or 5 in the argument of Parent [1999]. It was used by Oesterlé with $\ell = 3$ to prove his exponential bound $(3^{d/2} + 1)^2$, although it is only implicitly used in the Appendix since the part of Oesterlé's argument that uses it is replaced by a citation to Parent [1999]. The need for $\ell > 2$ is also the reason for the occurrence of 3 and not 2 as the base for the exponent in Oesterlé's bound.

The set $X_\mu(N)^{(d)}(\mathbb{F}_\ell)$ has fewer elements for elements for smaller ℓ so one would like to use $\ell = 2$ if $\ell \nmid N$ in view of applying Lemma 3.1. However, there are two difficulties that arise when doing so. The first one is that it is not necessarily true that the $J_{\mu,H}(\mathbb{Q})_{tors}$ injects into $J_{\mu,H}(\mathbb{F}_2)$. The second difficulty arises when

determining which elements in $\mathrm{Cot}_0\left(J_{\mu,H}\right)_{\mathbb{F}_l}$ come from $\mathrm{Cot}_0\left(J^{\mathbf{e}}_{\mu,H}\right)_{\mathbb{F}_l}$ as needed for Proposition 3.7. This is because the exact sequence that relates $\mathrm{Cot}_0\left(J_{\mu,H}\right)_{\mathbb{F}_l}$ to $\mathrm{Cot}_0\left(J^{\mathbf{e}}_{\mu,H}\right)_{\mathbb{F}_l}$ for $\ell > 2$ is not necessarily exact for $\ell = 2$. In Parent [2000] there is already a way of dealing with these difficulties when using $X_\mu(N)$. His solution is to take $t_1 : J_\mu(N) \to J_\mu(N)$ to be a Hecke operator that factors via $J^{\mathbf{e}}_\mu$ and $t_2 : J_\mu(N) \to J_\mu(N)$ such that it kills all the two torsion in $J^1_\mu(N)(\mathbb{Z}_{(2)})$ and apply Proposition 3.4.

The operator t_2 as needed for Proposition 3.4 can be obtained using the following proposition.

Proposition 5.2. *Let $q \nmid N$ be a prime, then $(T_q - \langle q\rangle - q)(Q) = 0$[2] for all $Q \in J_{\mu,H}(\mathbb{Q})_{tors}$ of order coprime to q.*

Proof. Let $Q \in J_{\mu,H}(\mathbb{Q})$ 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

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

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 $(T_q - \langle q\rangle - q)(Q) = 0$. □

What we need now is to find a way to find a Hecke operator t_1 as in Proposition 3.4. Now suppose if $t_1 \in \mathbb{T}$ is such that $t_1\mathcal{A}_e = 0$ then t_1 is a Hecke operator such that $t_1 \colon J_{\mu,H} \to J_{\mu,H}$ factors via $J^{\mathbf{e}}_{\mu,H}$. Lemma 1.9 of Parent [1999] already gives a way of finding such Hecke operators for J_μ as soon as we have found an element t that generates the Hecke algebra $\mathbb{T}_1(N)_{\mathbb{Q}}$. If N is a prime then the Hecke algebra $\mathbb{T}_1(N)_{\mathbb{Q}}$ 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. However if N is composite this is not necessarily true. And even in the prime case testing whether t is a generator is a computationally expensive task if t is represented by a huge matrix, so we don't want to try many different t's. Therefore we generalize his Lemma slightly so that we don't need t to be a generator.

[2]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 $X_1(N)$ while in his article he is working with $X_\mu(N)$, although he denotes our $X_\mu(N)$ by $X_1(N)$. For more details on the Eichler-Shimura relations on $X_\mu(N)$ and $X_1(N)$ see [Diamond and Im, 1995, p. 87]

Proposition 5.3. *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* $\operatorname{End} S_2(\Gamma_H)_{\mathbb{Q}}$. *Define*

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

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

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

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

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 $\mathcal{A}_{e,\mathbb{Q}} = \oplus_{i:L(f_i,1)=0} R_{f_i}$. 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 $\mathcal{A}_{e,\mathbb{Q}} := \left\{t' \in \mathbb{T}_{\mathbb{Q}} \mid t'|_{\mathcal{E}_e^{\perp}} = 0\right\}$ so in particular $t_1 \mathcal{A}_{e,\mathbb{Q}} = 0$ 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 $t_1|_{\mathcal{E}_{f_i}} = t_1|_{\ker P_{j_i}(t)} = 0$ □

If N is composite then one can get away with a smaller set than I in the previous proposition, because then not all the terms with $e_i > 1$ are needed. On can see which ones are not needed by studying the action of t on the space of new forms or $\Gamma_1(M)\Gamma_H$ for all $M \mid N$. But this is not necessary for our application.

5.2. **Condition 2: Kamienny's criterion.** Let N be an integer and $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ a subgroup, denote by $S_\infty \subseteq X_{\mu,H}(\mathbb{Q})$ the set of cusps that map to the cusp ∞ under the map $X_{\mu,H} \to X_0(N)$. On has that there are exactly $\phi(N)/\#\{\pm H\}$ elements in S_∞, where ϕ is Euler's totient function. Actually $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm H\}$ acts transitively and freely on them. Define

$$S_\infty^{(d)} := \pi(S_\infty^d) \subseteq X_{\mu,H}^{(d)}(\mathbb{Q}), \tag{7}$$

where $\pi : X_{\mu,H}^d \to X_{\mu,H}^{(d)}$ is the quotient map. Then we want to be able to check whether condition (2) of Theorem 3.3 holds for $S = S_\infty^{(d)}$. In order to do this we make the following definition.

Definition 5.4. 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 $c_0, \ldots, c_i$ pairwise distinct cusps in $X_{\mu,H}$ that lie above $\infty \in X_0(N)$, then we call $n_0 c_0 + \ldots + n_i c_i$ an **ordered sum ∞ cusps (of degree d)**.

It is clear that every element of $S_\infty^{(d)}$ can be written as an ordered sum of cusps in a unique way.

Remark. If $X_{\mu,H} = X_0(p)$ there is only one ordered sum of ∞ cusps of degree d, namely $d\infty$. So in this case condition (2) is the easiest to verify.

The proposition we will use to verify (2) of Theorem 3.3 is the following variant of Kamienny's Criterion which is a slight generalization of the variant [Parent, 2000, Prop. 2.8].

Proposition 5.5 (Kamienny's Criterion)**.** *Let $\ell \nmid N$ be a prime, $c = n_1c_1 + \ldots + n_mc_m$ be an ordered sum of ∞ cusps of $X_{\mu,H}$ of degree d. Let $\langle d_1\rangle, \ldots, \langle d_m\rangle \in (\mathbb{Z}/N\mathbb{Z})^*/\{\pm H\}$ be the diamond operators such that $\infty = \langle d_j\rangle c_j$, where this time ∞ is the cusp of $X_{\mu,H}$ corresponding to $\infty \in \mathbb{P}^1(\mathbb{Q})$. Let $f_{d,c}\colon X_{\mu,H}^{(d)} \to J_{\mu,H}$ as in Eq. (2), let $t \in \mathbb{T}_{\Gamma_H}$ and view t as a map $J_{\mu,H} \to J_{\mu,H}$ then $t \circ f_{d,c}$: is a formal immersion at $c_{\mathbb{F}_\ell}$ if and only if the d Hecke operators*

$$(T_i\langle d_j\rangle t)_{\substack{j\in 1,\ldots,m\\ i\in 1,\ldots,n_i}} \tag{8}$$

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

Specializing to the case $X_{\mu,H} = X_0(N)$ where $S_\infty^{(d)} = \{d\infty\}$ the condition in Eq. (8) above becomes: The map $t \circ f_{d,d\infty}$ is a formal immersion at $d\infty_{\mathbb{F}_\ell}$ if and only if the d Hecke operators

$$T_1t, T_2t, \ldots, T_dt \tag{9}$$

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

Proof of Proposition 5.5. We have $k(t \circ f_{d,c}(c_{\mathbb{F}_\ell})) = k(0_{\mathbb{F}_\ell}) = \mathbb{F}_l = k(c_{\mathbb{F}_\ell})$ so we only need to check that the linear independence criterion is equivalent to

$$(t \circ f_{d,c})^*\colon \operatorname{Cot}_{0_{\mathbb{F}_\ell}} J_{\mu,H} \to \operatorname{Cot}_{c_{\mathbb{F}_\ell}} X_{\mu,H}^{(d)}$$

being surjective.

Let $E_q/\mathbb{Z}[1/N][[q]]$ be the Tate curve. It has a canonical $\mu_{N,\mathbb{Z}[1/N][[q]]}$ embedding α coming from the unifomization map. The pair (E_q, α) gives a formal coordinate at the cusp ∞ of $X_\mu(N)_{\mathbb{Z}[1/N]}$ and since $X_\mu(N) \to X_{\mu,H}$ is unramified at ∞ it also gives a formal coordinate on $X_{\mu,H}$ at ∞. An element $\omega \in H^0(X_{\mu,H,\mathbb{Z}[1/N]}, \Omega^1)$ with q-expansion $\sum_{i=1}^\infty a_iq^{i-1}\mathrm{d}q$ is sent to the cusp form $f_\omega := \sum_{i=1}^\infty a_iq^i$ under the isomorphism $H^0(X_{\mu,H,\mathbb{Z}[1/N]}, \Omega^1) \cong S_2(\Gamma_H, \mathbb{Z}[1/N])$. Let $q_j = \langle d_j\rangle^*q$, then q_j is a formal coordinate at c_j. And the q_j expansion of ω at c_j is $\langle d_j\rangle f\mathrm{d}q_j/q_j$. This shows that the $a(\omega, q_j, n_j)$ defined as in Proposition 3.7 is given by

$$a(\omega, q_j, n_j) = a_1(\langle d_j\rangle f_\omega), a_2(\langle d_j\rangle f_\omega), \ldots, a_{n_j}(\langle d_j\rangle f_\omega).$$

The q expansion of $t^*\omega$ is tf_ω, now let $\omega_1, \cdots, \omega_g$ be generators of $H^0(X_{\mu,H,\mathbb{Z}[1/N]}, \Omega^1)$, then $t^*\omega_1, \cdots, t^*\omega_g$ generate $t^*H^0(X_{\mu,H,\mathbb{Z}[1/N]}, \Omega^1)$. In particular, using Proposition 3.7 we see that $t^*f_{d,c}$ is a formal immersion at $c_{\mathbb{F}_\ell}$ if and only if the matrix

$$A := \begin{bmatrix} a(t^*\omega_1, q_1, n_1) & a(t^*\omega_1, q_2, n_2) & \cdots & a(t^*\omega_1, q_1, n_m) \\ a(t^*\omega_2, q_1, n_1) & a(t^*\omega_2, q_2, n_2) & \cdots & a(t^*\omega_2, q_1, n_m) \\ \vdots & \vdots & \ddots & \vdots \\ a(t^*\omega_g, q_1, n_1) & a(t^*\omega_g, q_2, n_2) & \cdots & a(t^*\omega_g, q_1, n_m) \end{bmatrix} \tag{10}$$

has rank d over $\mathbb{F}_\ell$.

Now by formula (5.13) of Diamond and Shurman [2005] we have for an integer $1 \leq n \leq n_j$ that $a(t^*\omega_i, q_j, n_j)_n = a_n(\langle d_j\rangle t f_{\omega_i}) = a_1(T_n\langle d_j\rangle t f_{\omega_i})$. Using the isomorphism $\mathbb{T}_{\Gamma_H}/\ell\mathbb{T}_{\Gamma_H} \to Hom(S_2(\Gamma_H, \mathbb{F}_\ell), \mathbb{F}_\ell)$ [Diamond and Im, 1995, Prop. 12.4.13] [3] given by $T \mapsto (f \mapsto a_1(Tf))$ we see that for all $1 \leq i \leq g$ and $n \leq n_j$ we can replace the column of A that contains the elements $a(t^*\omega_i, q_j, n_j)_n$ by $T_n\langle d_j\rangle t$. □

5.2.1. *Making the testing of Kamienny's criterion for $X_{\mu,H}$ faster.* As we have already seen Kamienny's criterion for $X_\mu(N)$ requires the testing of a lot of linear independence relations while Kamienny's criterion for $X_0(N)$ requires testing only 1 linear independence relation. To be more specific about what we mean by a lot, suppose that d is the degree and $p = N$ the the prime for which we want to check the Kamienny's criterion of $X_\mu(p)$ and we only consider the ordered sums of ∞ cusps $n_1c_1, \ldots, n_ic_i$ where the multiplicities $n_1, \ldots, n_i$ are all equal to 1 (hence $i = d$) 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 $X_0(p)$ instead of $X_\mu(p)$ whenever possible. While doing the explicit computations, it turned out that the $X_0(p)$ version of the criterion sometimes fails for primes which are too big to make it practical to just try the $X_\mu(p)$ criterion for all possible ordered cusp sums. For example, we were unable to find t_1 and t_2 such that the $X_0(p)$ version of the criterion was satisfied for $d = 7$ and $p = 193$. In this case the $X_\mu(p)$ 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 $n_1c_1 + \cdots + n_ic_i$ where the multiplicities $n_1, \ldots, n_i$ are all equal to 1 and hence $d = i$. Checking Kamienny's criterion for all these sums of cusps comes down to checking whether

$$\langle d_1\rangle t, \ldots, \langle d_i\rangle t$$

are linearly independent for each set of pairwise distinct diamond operators $\langle d_1\rangle, \ldots, \langle d_i\rangle$ 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 $\langle 1\rangle t, \ldots, \langle (p-1)/2\rangle t$ 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

[3] There they show it only for $\Gamma_H = \Gamma_0(N)$ or $\Gamma_H = \Gamma_1(N)$, however the statement for Γ_H follows from the statement for $\Gamma_1(N)$, because $S_2(\Gamma_H, \mathbb{Z}) = S_2(\Gamma_1(N), \mathbb{Z})^{\Gamma_H/\Gamma_1(N)}$ and $\mathbb{T}_{\Gamma_H} = \mathbb{T}_{\Gamma_1(N)}|_{S_2(\Gamma_H,\mathbb{Z})}$.

coefficients of all linear dependencies. The following lemma generalizes this example to the case where the $n_1, \ldots, n_i$ are not necessarily equal to 1. This trick makes it more feasible to check the $X_\mu(N)$ version of the criterion on the computer.

Lemma 5.6. *Let $\ell \nmid N$ be a prime, d be an integer and $t \in \mathbb{T}_{\Gamma_H}$ and let $D \subset \mathbb{Z}$ be a set of representatives of $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm H\}$ such that $1 \in D$. Define for all integers r with $\lfloor \frac{d}{2} \rfloor \leq r \leq d$ the following set*

$$D_r := \{(1,i) \mid d - r < i \leq r\} \cup \{(k,i) \mid 1 \leq i \leq d-r, k \in D\}.$$

Suppose that for all r with $\lfloor \frac{d}{2} \rfloor \leq r \leq d$ there is no $\mathbb{F}_\ell$ linear dependence among d of the elements $(T_i\langle k\rangle t)_{(k,i)\in D_r}$ in $\mathbb{T}_{\Gamma_H}/\ell\mathbb{T}_{\Gamma_H}$. Then $t \circ f_{d,c} \colon X^{(d)}_{\mu,H} \to J_{\mu,H}$ is a formal immersion at $c_{\mathbb{F}_\ell}$ for all ordered sums of ∞ cusps $c := n_1c_1 + \cdots + n_mc_m$ of degree d.

Proof. Suppose for contradiction that there is an ordered sum of ∞ cusps $c := n_1c_1 + \cdots + n_mc_m$ of degree d such that $t \circ f_{d,c}$ is not a formal immersion at $c_{\mathbb{F}_\ell}$. Write $c_1 = \langle d_j\rangle c_j$ with $d_j \in D$ for $1 \leq j \leq m$ then by 5.5 we see that the d vectors

$$(T_i\langle k\rangle t)_{((k,i)\in S)}, \quad S := \{(d_j,i) \mid 1 \leq j \leq m,\ 1 \leq i \leq n_j\}$$

are $\mathbb{F}_l$ linearly dependent in $\mathbb{T}_{\Gamma_H} \otimes \mathbb{F}_l$. We know that

$$\min(n_1, d-n_1) \geq n_2 \geq n_3 \geq \ldots \geq n_m.$$

So if $n_1 \geq \lfloor \frac{d}{2} \rfloor$ then $S \subseteq D_{n_1}$ and if $n_1 \leq \lfloor \frac{d}{2} \rfloor$ then $S \subseteq D_{d-n_1}$ so both cases lead to a contradiction. □

5.2.2. *Testing the criterion.* Using a computer program written in Sage we first tested the criterion for $X_0(p)$. 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 5.7. *If $p = 131, 139, 149, 151, 167, 173, 179, 181, 191$ or p is a prime with $193 < p \leq 2281$ then there are $t_1, t_2 \in \mathbb{T}_{\Gamma_0(p)}$ as in Proposition 3.4 with $C = X_0(p)$ and $J = A = J_0(p)$ such that $T_1t_1t_2T, \ldots, T_7t_1t_2$ are $\mathbb{F}_2$ linearly independent in $\mathbb{T}_{\Gamma_0(p)} \otimes \mathbb{F}_2$.*

Proof. The computer tested the criterion for all $17 \leq p \leq 2281$ using different choices of t_1 and t_2. The t_1 that were tried are $t_1 = t_1(t)$ as in Proposition 5.3, using $t = T_2, \ldots, T_{60}$, and the t_2 that were tried are $t_2 = T_q - q - 1$ for all primes $2 < q < 20$ with $q \neq p$. For all primes mentioned above the computer found at least one pair t_1, t_2 such that the linear independence holds. The total time used was about 2 hours[4] when checking the criterion for about 8 primes in parallel so it could be used to check the criterion for bigger d and p. □

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

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

Proposition 5.8. *For all pairs (p,d) with p a prime $p \leq 193$ and $3 \leq d \leq 7$ not satisfying any of the following conditions:*

- *$d = 3$ and $p \in \mathrm{Primes}(17)$*
- *($d = 4$ or $d = 5$) and $p \in \mathrm{Primes}(19) \cup \{29\}$*
- *($d = 6$ or $d = 7$) and $p \in \mathrm{Primes}(37)$*

there are $t_1, t_2 \in \mathbb{T}_{\Gamma_1(p)}$ as in Proposition 3.4 with $C = X_\mu(p)$ and $J = A = J_\mu(p)$ such that for $t = t_1 t_2$ the D_r as in lemma 5.6 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 the t_1, t_2 that were tried are $t_1 = t_1(t)$ for $t = T_2, \ldots, T_{20}$ and $t_2 = T_q - q - \langle q \rangle$ for the primes $2 < q < 20$ only trying new choices of t_1 and t_2 if no successful pair combination of t_1 and t_2 had been found yet. The most time was spent on the case $p = 193$ which took about 14 hours.[4]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. □

5.3. **Condition 3: Study of $X_1(p)^{(d)}(\mathbb{F}_2)$.** For a prime $p > 7$ we know from Mazur [1977] that $Y_1(p)(\mathbb{Q}) = \emptyset$ and hence that $X_1(p)(\mathbb{Q})$ consists of $(p-1)/2$ cusps that map to the cusp 0 on $X_0(p)$. Let $S_0 \subseteq X_1(p)(\mathbb{Q})$ be the set of these $(p-1)/2$ cusps mapping 0 on $X_0(p)$, and define

$$S_0^{(d)} := \pi(S_0^d) \subseteq X_1(p)^{(d)}(\mathbb{Q}) \tag{11}$$

where $\pi : X_1(p)^d = X_1(p)^{(d)}$ is the quotient map, then $S_0^{(d)} = W_p^{(d)}(S_\infty^{(d)})$. We would like to verify condition (3) of Theorem 3.2 with $S = S_\infty^{(d)}$ and $C = X_\mu(p)$ when taking $R = \mathbb{Z}_{(\ell)}$, or condition (3) of *Theorem* 3.3 with $C = X_\mu(p)$, $D = X_0(p)$, $S = S_\infty^{(d)}$ and $T = \{d\infty\}$. However since the moduli interpretation of $X_1(p)$ is easier than that of $X_\mu(p)$, we instead apply $W_p^{(d)}$ so that we verify it for $S = S_0^{(d)}$ and $C = X_1(p)$ instead. One situation in which condition (3) of *Theorem* 3.3 is trivially satisfied is if $S = S_0^{(d)}$, $X_1(p)^{(d)}(\mathbb{F}_\ell) = \mathrm{red}_{\mathbb{F}_\ell}(S)$ and $T = f^{(d)}(S)$. For this it is useful to know $X_1(p)^{(d)}(\mathbb{F}_\ell)$. Let $y \in X_1(p)^{(d)}(\mathbb{F}_\ell)$, then y can be written as $\sum_{i=1}^m e_i y_i^{(f_i)}$ with $m, e_i, f_i \in \mathbb{N}_{\geq 0}$ and $y_i \in X_1(p)(\mathbb{F}_{\ell^{f_i}})$ such that each of the y_i does not come from a subfield of $\mathbb{F}_{\ell^{f_i}}$ and such that all the $y_i^{(f_j)}$ are distinct.

Theorem 5.9. *[Waterhouse, 1969, Thm 4.1] Let p, ℓ be distinct primes and d be an integer then*

$$Y_1(p)(\mathbb{F}_{\ell^d}) = \emptyset$$

if and only if the following 5 statements are true

1. *p does not divide any integer n such that both $|n - \ell^d - 1| < 2\ell^{d/2}$ and $\gcd(n-1, \ell) = 1$.*
2. *If d is even then $p \nmid \ell^d + 1 \pm 2\ell^{d/2}$.*

(3) *If d is even and $l \not\equiv 1 \mod 3$ then $p \nmid \ell^d + 1 \pm \ell^{d/2}$.*
(4) *If d is odd and $\ell = 2$ or 3 then $p \nmid \ell^d + 1 \pm \ell^{(d+1)/2}$.*
(5) *If d is odd or $l \not\equiv 1 \mod 4$ then $p \nmid \ell^d + 1$.*

and if (1) is false then all points in $Y_1(p)(\mathbb{F}_{\ell^d})$ are supersingular.

The theorem as stated above only follows from [Waterhouse, 1969, Thm 4.1] for $p > 4$ since for those primes the moduli problem for $Y_1(p)$ is representable over $\mathbb{Z}[1/p]$, but one easily verifies that $Y_1(p)(\mathbb{F}_{\ell^d}) \neq \emptyset$ and that statement 1 is false for $p = 2$ or 3.

If we again assume that $p > 4$ then $X_1(p)(\overline{\mathbb{Q}})$ has aside from the $(p-1)/2$ cusps defined over $\mathbb{Q}$, also $(p-1)/2$ cusps defined over the real subfield of $\mathbb{Q}(\zeta_p)$. The reduction of these $(p-1)/2$ non-rational cusps mod ℓ are definable over $\mathbb{F}_{\ell^d}$ if and only if $p \mid \ell^d - 1$ or $p \mid \ell^d + 1$. In particular the above theorem implies that $X_1(p)(\mathbb{F}_{\ell^{d'}}) = X_1(p)(\mathbb{F}_\ell) = \mathrm{red}_k X_1(p)(\mathbb{Q})$ holds for all $d' \leq d$ if $p > (\ell^{d/2} + 1)^2$. Specializing to the case $\ell = 2$ and $3 \leq d \leq 7$ one can with a small computation for the primes $p < (\ell^{d/2} + 1)^2$ show the following:

Proposition 5.10. *Let $3 \leq d \leq 7$ be an integer and p be a prime such that*

$$\begin{aligned} p \geq 11 \text{ and } p \neq 13, &\quad \text{if } d = 3, \\ p \geq 19, &\quad \text{if } d = 4, \\ p \geq 23 \text{ and } p \neq 31, 41, &\quad \text{if } d = 5, \\ p \geq 23 \text{ and } p \neq 29, 31, 37, 41, 73, &\quad \text{if } d = 6, \text{ and} \\ p = 47, 53 \text{ or } (p \geq 79 \text{ and } p \neq 113, 127), &\quad \text{if } d = 7. \end{aligned}$$

then

$$X_1(p)(\mathbb{F}_{2^{d'}}) = X_1(p)(\mathbb{F}_2) = \mathrm{red}_{\mathbb{F}_2}(X_1(p)(\mathbb{Q})) = \mathrm{red}_{\mathbb{F}_2}(S_0)$$

for all $d' \leq d$.

Corollary 5.11. *If one takes p, d as in the above proposition and one lets $S_0^{(d)}$ as in Eq. (11), then*

$$X_1(p)^{(d)}(\mathbb{F}_2) = \mathrm{red}_{\mathbb{F}_2}(S_0^{(d)})$$

and hence condition (3) of Theorem 3.2 holds for $C = X_1(p), S = S_0^{(d)}$ and $R = \mathbb{Z}_{(2)}$. Additionally condition (3) of Theorem 3.3 holds for $C = X_1(p), D = X_0(p), S = S_0^{(d)}, T = \{d0\}$ and $R = \mathbb{Z}_{(2)}$. By applying the Atkin-Lehner operator $W_p : X_1(p) \to X_\mu(p)$ condition (3) of Theorems 3.2 and 3.3 hold for $C = X_\mu(p)$,$D = X_0(p)$,$S = S_\infty^{(d)}, T = \{d\infty\}$ and $R = \mathbb{Z}_{(2)}$, where $S_\infty^{(d)}$ is as in Eq. (7).

6. Proof of Theorem 1.1

Proposition 6.1. *Let $d \leq 7$ be an integer. If $S(d) \subseteq$ Primes(2281), then $S(d) \subseteq$ Primes(193).*

Proof. It suffices to show that if $d \leq 7$ and $193 < p \leq 2281$ is a prime, then $p \notin S(d)$. This is done by applyingTheorem 3.3 with $C = X_\mu(p), D = X_0(p), S = S_\infty^{(d)}, T = \{d\infty\}$ and $R = \mathbb{Z}_{(2)}$. By Propositions 3.4, 5.5 and 5.7 we see that there exists a t such that conditions (1) and (2) are satisfied. By Corollary 5.11 we see that condition (3) is satisfied so we can indeed apply Theorem 3.3. It follows that $S_\infty^{(d)} = X_\mu(p)^{(d)}(\mathbb{Q})$, showing that the only points in $X_\mu(p)$ defined over a number field of degree $\leq d$ are cusps and hence $p \notin S(d)$. □

Proposition 6.2. *If* $S(d) \subseteq \text{Primes}(193)$ *for all* $d \leq 7$ *then*

$$\begin{aligned}
S(3) &= \text{Primes}\,(17),\\
S(4) &= \text{Primes}\,(17) \cup \{29\}\,,\\
S(5) &= \text{Primes}\,(19) \cup \{29, 31, 41\}\,,\\
S(6) &= \text{Primes}\,(19) \cup \{29, 31, 37, 41, 73\} \qquad \textit{and}\\
S(7) &\subseteq \text{Primes}\,(43) \cup \{59, 61, 67, 71, 73, 113, 127\}\,.
\end{aligned}$$

Proof. This is proven almost the same as Proposition 6.1, with the difference that this time one has to use Theorem 3.2 instead of Theorem 3.3, with C and S still $X_\mu(p)$ and $S_\infty^{(d)}$. Also Propositions 5.5 and 5.7 have to be replaced by Lemma 5.6 and Proposition 5.8. □

So in order to prove Theorem 1.1 it remains to deal with the primes $17, 29, 31, 41$ and 73.

6.1. **Proof of Theorem 1.1 for** $p = 17, 29, 31$ **or** 41**.** We quote [Conrad et al., 2003, Prop. 6.2.1.] in an equivalent formulation using that $J_1(p) \cong J_\mu(p)$ and adding some more information from Section 6.2 in loc.cit.

Proposition 6.3. *The primes* p *such that* $J_\mu(p)$ *has rank zero are the primes* $p \leq 31$ *and* 41*,* 47*,* 59*, and* 71*.*

For all of these, except possibly $p = 29$*, the Mordell-Weil group is generated by differences of rational cusps, and for all except* $p = 17$*,* 29*,* 31 *and* 41*, the order of* $J_1(p)(\mathbb{Q})$ *is odd.*

We can add to this the following new result.

Theorem 6.4. *The group* $J_1(29)(\mathbb{Q})$ *is generated by differences of rational cusps.*

Proof. Instead of proving this statement for $J_1(29)$ we will prove it for $J_\mu(29)$. This suffices because $X_1(N)$ and $X_\mu(N)$ are isomorphic over $\mathbb{Q}$ by an isomorphism that sends cusps to cusps. This allows us to use the description for the action of Galois on the cusps of $X_\mu(N)$ described in Stevens [1982]. It is already known that $J_\mu(29)(\mathbb{Q})[p^\infty]$ is generated by differences of rational cusps for all $p \neq 2$ prime (see the discussion after Conjecuture 6.2.2 of Conrad et al. [2003]). So it suffices to prove that $J_\mu(29)(\mathbb{Q})[2^\infty]$ is generated by the rational cusps.

Let $q \neq 2, 29$ be a prime then Proposition 5.2 implies that

$$J_\mu(29)(\mathbb{Q})[2^\infty] \subseteq J_\mu(29)(\overline{\mathbb{Q}})[2^\infty, T_q - \langle q\rangle - q].$$

Let $\tau : J_\mu(29)(\overline{\mathbb{Q}}) \to J_\mu(29)(\overline{\mathbb{Q}})$ be complex conjugation, then also

$$J_\mu(29)(\mathbb{Q})[2^\infty] \subseteq J_\mu(29)(\overline{\mathbb{Q}})[2^\infty, \tau - 1].$$

Using the isomorphism $J_\mu(29)(\overline{\mathbb{Q}})[2^\infty] \cong \varinjlim 2^{-i} H_1(X_\mu(29), \mathbb{Z})/H_1(X_\mu(29), \mathbb{Z})$ it is possible to compute the kernels of $\tau - 1$ and $T_q - \langle q\rangle - q$ seen as maps on $J_\mu(29)(\overline{\mathbb{Q}})[2^\infty]$ purely in terms of modular symbols. Let

$$M := J_\mu(29)(\overline{\mathbb{Q}})[2^\infty, T_5 - \langle 5\rangle - 5, \tau - 1]$$

then a Sage computation shows that $M \cong (\mathbb{Z}/4\mathbb{Z})^6$. Let $C \subseteq J_\mu(29)(\mathbb{Q}(\zeta_{29}))$ be the subgroup generated by all cusps: using a Sage computation we showed $M = C[2^\infty]$. Using the explicit description of the action of $G := \mathrm{Gal}(\mathbb{Q}(\zeta_{29})/\mathbb{Q})$ on the cusps in Stevens [1982] we verified that $C[2^\infty]^G = J_\mu(29)(\mathbb{Q})[2^\infty]$ is indeed generated by the differences of rational cusps. □

This shows that for all primes p such that $J_1(p)(\mathbb{Q})$ is finite, the latter group is generated by differences of rational cusps. Now if $J_1(p)(\mathbb{Q})$ is finite and $J_1(p)(\mathbb{Q})[2] \hookrightarrow J_1(p)(\mathbb{F}_2)$ then condition (1) of Theorem 3.2 is satisfied for $t = \mathrm{Id}_{J_1(p)}$. For the primes $p = 3$, 5, 7, 11, 13, 19, 23, 47, 59 and 71, $J_1(p)(\mathbb{Q})[2] \hookrightarrow J_1(p)(\mathbb{F}_2)$ is trivially satisfied, since the group has odd order. Ironically the primes of Proposition 6.3 missing from this sequence are exactly the primes we are interested in.

Proposition 6.5. *For $p = 17, 29, 31$ or 41 one has $J_1(p)(\mathbb{Q})[2] \hookrightarrow J_1(p)(\mathbb{F}_2)$, and hence condition (1) of Theorem 3.2 is satisfied for $t = \mathrm{Id}_{J_1(p)}$.*

Proof. We only have to consider $p = 17$, 29, 31 and 41. We know that $J_1(p)(\mathbb{Q})$ is generated by differences of rational cusps, see Proposition 6.3 and Theorem 6.4. It is also known what the order of this group is, see [Conrad et al., 2003, § 6.2.3 and Table 1]. We now use Magma Bosma et al. [1997] to compute a model of $X_1(p)$ over $\mathbb{F}_2$ and check that the subgroup of its Picard group generated by differences of its $\mathbb{F}_2$-points (which are the images of the cusps under reduction mod 2) has the correct order. In fact, it suffices to check that the 2-primary part of the group has the correct order. For $p = 17$, we do this directly. For the other three primes, we use an intermediate curve X_H such that the predicted order of the 2-primary part of $J_H(\mathbb{Q})$ equals that of $J_1(p)(\mathbb{Q})$, since the computation using $X_1(p)$ directly would be too involved. We check that the subgroup of $J_H(\mathbb{F}_2)$ generated by differences of the images of cusps has 2-primary part of the correct size. For $p = 29$, we use X_H corresponding to $d = 7$ in the notation of Conrad et al. [2003], for $p = 31$, we use the curve corresponding to $d = 3$, and for $p = 41$ we use the curve corresponding to $d = 4$. In each case, the computation gives the desired result. (It is also possible and not taking too much time to do the computation directly on $X_1(p)$ over $\mathbb{F}_2$ for $p = 29$ and $p = 31$.) □

Lemma 6.6. *Condition* (3) *of Theorem 3.2 is satisfied for* $C = X_1(29)$ *and* $C = X_1(31)$, $S = S_0^{(d)}$, $R = \mathbb{Z}_{(2)}$ *and* $d \leq 7$. *Here* $S_0^{(d)}$ *is as in Eq.* (11).

Proof. For $d < 5$, this is covered by Proposition 5.10. For $d = 5, 6, 7$, we check it by a Magma calculation. In this calculation we computed the images in $\mathrm{Pic}_{C_{\mathbb{F}_2}/\mathbb{F}_2}(\mathbb{F}_2)$ of all points $s \in C^{(d)}(\mathbb{F}_2)$ not coming from a point in $S_0^{(d)}$. We verified that these images are not in the subgroup of $\mathrm{Pic}_{C_{\mathbb{F}_2}/\mathbb{F}_2}(\mathbb{F}_2)$ generated by the points coming from $\mathbb{Q}$-rational cusps, and we know that the $\mathbb{Q}$ rational cups generate $\mathrm{Pic}_{C_{\mathbb{Q}}/\mathbb{Q}}(\mathbb{Q})$ for these two curves by Proposition 6.3 and Theorem 6.4. □

The above proof involves computing $\mathrm{Pic}_{C_{\mathbb{F}_2}/\mathbb{F}_2}(\mathbb{F}_2)$ in Magma. For $C = X_1(41)$ this would probably take too long to be practical. Therefore we deal with $C = X_1(41)$ in a slightly different way:

Lemma 6.7. *Condition* (3) *of Theorem 3.2 is satisfied for* $C = X_1(41)$, $S = S_0^{(d)}$, $R = \mathbb{Z}_{(2)}$ *and* $d \leq 7$.

Proof. There is no elliptic curve E over $\mathbb{F}_{2^e}$ with $41 \mid \#E(\mathbb{F}_{2^e})$ if $e = 1, 2, 3, 4, 6$ or 7. There is exactly one elliptic curve E over $\mathbb{F}_{2^5}$ with $\#E(\mathbb{F}_{2^5}) = 41$; this is the curve $y^2 + y = x^3 + x + 1$ already defined over $\mathbb{F}_2$. Its automorphism group over $\mathbb{F}_{2^5}$ is cyclic of order 4; we therefore obtain only $10 = (41 - 1)/4$ distinct $\mathbb{F}_{2^5}$-points on $X_1(41)$ that are not cusps. Let X_H be the intermediate curve corresponding to $d = 4$ in Conrad et al. [2003]. Then $X_1(41) \to X_H$ is an étale cover of degree 5, and the ten $\mathbb{F}_{2^5}$-points on $X_1(41)$ map to two $\mathbb{F}_2$-points on X_H. In fact, $X_H(\mathbb{F}_2)$ consists of six points; four of them are cusps, and the other two are the ones just mentioned. It can be checked that these two points do not map into the subgroup of $\mathrm{Pic}_{X_{H,\mathbb{F}_2}/\mathbb{F}_2}(\mathbb{F}_2)$ generated by the four cusps, which implies condition (3). □

Proposition 6.8. *The following exclusions hold:*

$$\begin{aligned} 17 &\notin S(3), \\ 29 &\notin S(4), \\ 29, 31, 41 &\notin S(5), \\ 29, 31, 41 &\notin S(6) \quad \textit{and} \\ 29, 31, 41 &\notin S(7). \end{aligned}$$

The proof of $17 \notin S(3)$ is similar to that in Parent [2003] although we manage to avoid the careful analysis of the formal group of $J_1(p)_{\mathbb{Z}_2}$ since we have proven that $J_1(p)(\mathbb{Q})[2] \hookrightarrow J_1(p)(\mathbb{F}_2)[2]$ in Proposition 6.5.

Proof. This is again done by applying Theorem 3.2 over $R = \mathbb{Z}_{(2)}$, this time with $C = X_1(p)$ and $S = S_0^{(d)}$ for the p, d for which we want to show $p \notin S(d)$. We check that Theorem 3.2 can indeed be applied by verifying that its conditions (1),(2) and (3) are satisfied using $t = \mathrm{Id} : J_1(p) \to J_1(p)$.

(1) This follows from Proposition 6.5.
(2) For $(p, d) = (17, 3)$ this is in [Parent, 2000, §4.3].
    For $p = 29$ resp. 31 it is known that the $\mathbb{F}_2$ gonality of $X_1(p)$ is 11 resp. 12 [Derickx and van Hoeij, 2014, Tbl. 1, Rmk. 1]. So condition (2) is satisfied by Proposition 3.5.
    For $p = 41$ this follows from Proposition 5.8 together with Lemma 5.6 using the isomorphism $W_p : X_\mu(p) \to X_1(p)$.
(3) For $p = 17$ this is Corollary 5.11, for $p = 29, 31, 41$ it follows from Lemmas 6.6 and 6.7.

□

This leaves us with only one case which we also found the hardest to prove.

6.2. **Proof of Theorem 1.1 for $p = 73$.** First we start by analysing the points in $X_1(73)(\mathbb{F}_2^d)$ for $d \leq 6$. The first thing to notice is that for $d \leq 6$ the only points in $X_1(73)(\mathbb{F}_{2^d}) \setminus Y_1(73)(\mathbb{F}_{2^d})$ are the points mapping to the cusp 0 on $X_0(73)$, because $2^d \not\equiv \pm 1 \mod 73$ for $d \leq 6$. Using the isomorphism $W_p : X_1(p) \to X_\mu(p)$ and applying Lemma 5.6 and Proposition 5.8 shows that the conditions of Lemma 3.1 are satisfied for all cuspidal points of $X_1(73)^{(6)}(\mathbb{F}_2)$. As a result we only need to study the residue classes in $X_1(73)^{(6)}(\mathbb{F}_2)$ that do not consist entirely of cusps. After a detailed study of these residue classes the proof will be finished by Proposition 6.9.

We continue by analysing the points of $X_1(73)^{(6)}(\mathbb{F}_2)$ that do not consist completely of cusps. For this we first describe the Tate normal form see Knapp [1992] of a point $(E, P) \in Y_1(N)(K)$ for K a field and $N \geq 4$ an integer coprime to the characteristic to K. For every pair (E, P) where E is an elliptic curve over K and P a point of order exactly N there are unique $b, c \in K$ such that $(E, P) \cong (E_{b,c}, (0, 0))$ where $E_{b,c}$ is the elliptic curve given by the Weierstrass equation

$$y^2 + (1 - c)xy - by = x^3 - bx^2. \tag{12}$$

By Theorem 5.9 one sees that there are no points in $Y_1(73)(\mathbb{F}_{2^d})$ for $d \leq 5$ and that all points in $Y_1(73)(\mathbb{F}_{2^6})$ are supersingular. To explicitly find the Tate normal form of all points in $Y_1(73)(\mathbb{F}_{2^6})$ note that $E_{b,c}$ has discriminant $\Delta_{b,c} := b^3(c^4+c^3+c^2+b+c)$ and j-invariant $\frac{(c+1)^{12}}{\Delta_{b,c}}$ in characteristic 2. The curve $E_{b,c}$ is supersingular if and only if $j = 0$, which is equivalent to $c = 1$. By computing the 73 division polynomial for $E_{b,1}$ one sees that the solutions of

$$(b^6 + b + 1)(b^6 + b^3 + 1)(b^6 + b^5 + b^2 + b + 1)(b^6 + b^5 + b^4 + b + 1) \tag{13}$$

are exactly the values of $b \in \mathbb{F}_{2^6}$ such that $(0, 0)$ is of order 73. This calculation shows that $X_1(73)^{(6)}(\mathbb{F}_2)$ has exactly 4 points that do not consist entirely of cusps, namely the points corresponding to the 4 factors of (13). Explicitly calculating the action of $(\mathbb{Z}/73\mathbb{Z})^*/\{\pm 1\}$ on these 4 points one can show that the diamond operator $\langle 10 \rangle$ of order 4 acts transitively on them. Let $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ be the subgroup

generated by 10, then 4 points in $Y_1(73)^{(6)}(\mathbb{F}_2)$ map to a single point on $Y_H^{(6)}(\mathbb{F}_2)$ by the discussion above.

If E is an elliptic curve with $73 = 2^6+1+8$ points over $\mathbb{F}_{2^6}$ then the characteristic polynomial of frobenius is

$$x^2 - 8x - 2^6 = (x - 8\zeta_3)(x + 8\zeta_3 + 8).$$

Let E_{ζ_3} be an elliptic curve $\mathbb{Q}(\zeta_3)$ that has complex multiplication by $\mathbb{Q}(\zeta_3)$, then E_{ζ_3} has two isogenies of degree 73 over $\mathbb{Q}(\zeta_3)$ namely $8\zeta_3-1$ and $-8\zeta_3-9$. The map $X_1(73) \to X_0(73)$ is of degree $36 = (73-1)/2$, and since the automorphism ζ_3 of order 3 preserves the kernels of the isogenies $8\zeta_3-1$ and $-8\zeta_3-9$ we see that the ramification index of $\pi : X_1(73) \to X_0(73)$ at the points corresponding to the isogenies $8\zeta_3 - 1$ and $-8\zeta_3 - 9$ is 3. Showing that $S := \pi^{-1}(\{(E, 8\zeta_3 - 1), (E, -8\zeta_3 - 9)\}) \subseteq X_1(73)(\overline{\mathbb{Q}})$ is a set of size 24. The action of Galois on S is transitive because there are no CM elliptic curves with a 73 torsion point over number fields of degree < 24 [Clark et al., 2013, Table 1]. If one fixes a prime ℓ above 2 in $\overline{\mathbb{Q}}$, then reduction modulo ℓ gives a bijection between S and $Y_1(73)(\mathbb{F}_{2^6})$. The existence of this bijection can be shown either by explicit computation in Sage or by pure thought by showing that for $(E, P) \in Y_1(73)^{(6)}(\mathbb{F}_2)$ the canonical lift (or Deuring lift) (E_0, ϕ_0) of $(E, \mathrm{Frob}_{\mathbb{F}_{2^6}}/8)$ to $\bar{\mathbb{Q}}$ is either (E, ζ_3) or its Galois conjugate $(E, -\zeta_3 - 1)$.

The above discussion shows that if one takes $x_1, \ldots, x_6 \in X_H(\bar{\mathbb{Q}})$ to be the 6 points corresponding to the 6 orbits of $\langle 10 \rangle$ acting on S, that then

$$x^{(6)} : x_1 + \cdots + x_6 \in X_H^{(6)}(\mathbb{Q}) \tag{14}$$

is a point that reduces to the unique point in the image of $Y_1(73)^{(6)}(\mathbb{F}_2) \to Y_H^{(6)}(\mathbb{F}_2)$.

Since $x^{(6)}$ corresponds to a CM curve and CM curves over number fields of degree < 24 have no 73 torsion as mentioned before, and we know that a point in $y \in X_H^{(6)}(\mathbb{Q})$ coming from $X_1(73)^{(6)}(\mathbb{Q})$ has to specialize to $x_{\mathbb{F}_2}^{(6)}$ we can prove that $73 \notin S(6)$ by showing:

Proposition 6.9. *Let $H \subseteq (\mathbb{Z}/73\mathbb{Z})^*/\{\pm 1\}$ the subgroup generated by 10. Then the point $x^{(6)}$ defined above is the unique point in $X_H^{(6)}(\mathbb{Q})$ reducing to $x_{\mathbb{F}_2}^{(6)}$ modulo 2.*

Proof. We do this by proving instead that $W_p^{(6)}(x^{(d)}) \in X_{\mu,H}^{(6)}(\mathbb{Q})$ is the unique point reducing to $W_p^{(6)}(x_{\mathbb{F}_2}^{(d)})$. This allows us to work with a model where the cusp at infinity is rational. We are going to prove that the matrix A of Proposition 3.7 at $W_p^{(6)}(x_{\mathbb{F}_2}^{(d)})$ has rank 6 using an explicit model of $X_{\mu,H,\mathbb{F}_2}$, we know that its genus is 43. Using Sage to compute an explicit basis of $H^0(X_{\mu,H,\mathbb{F}_2}, \Omega^1) = S_2(\Gamma_H, \mathbb{F}_2)$ shows that q^{47} is the largest leading term among all modular forms. So giving the coefficients of a modular form up to and including q^{47} is enough to determine it uniquely. The subspace $H^0(X_{\mu,H,\mathbb{F}_2}, \Omega^1(-41\infty)) \subseteq H^0(X_{\mu,H,\mathbb{F}_2}, \Omega^1)$ is 3 dimensional

and has as basis

$$\begin{aligned}\omega_1 &:= (q^{42}+q^{47}+q^{49}+O(q^{50}))\frac{\mathrm{d}q}{q}\\ \omega_2 &:= (q^{43}+q^{49}+O(q^{50}))\frac{\mathrm{d}q}{q}\\ \omega_3 &:= (q^{47}+q^{48}+O(q^{50}))\frac{\mathrm{d}q}{q}.\end{aligned}$$

Let $\mathcal{L} \subseteq \Omega^1_{X_{\mu,H,\mathbb{F}_2}}$ be the line bundle generated by $\omega_1, \omega_2, \omega_3$ then $\mathcal{L}$ has degree at most $2 \cdot 43 - 2 - 41 = 43$. Viewing $\omega_1, \omega_2, \omega_3$ as sections of $\mathcal{L}$ gives us a map $\phi : X_{\mu,H,\mathbb{F}_2} \to \mathbb{P}^2_{\mathbb{F}_2}$ given by $\phi(P) = (\omega_1(P) : \omega_2(P) : \omega_3(P))$. Its image is given by a homogeneous polynomial of degree at most 43. Indeed, using the computer to compare the q-expansions of products of ω_1, ω_2 and ω_3 we found a homogeneous polynomial $f_H \in \mathbb{F}_2[x_0, x_1, x_2]$ of degree 41 describing the image of ϕ, since this is only 2 smaller then expected we know that $\Omega^1_{X_{\mu,H,\mathbb{F}_2}}/\mathcal{L}$ is an effective divisor $\mathbb{F}_2$ of degree 2, in particular there are no points with residue field $\mathbb{F}_{2^6}$ in its support, meaning that at least one of $\omega_1, \omega_2, \omega_3$ is a generator of $\Omega^1_{X_{\mu,H,\mathbb{F}_2}}$ at the points we are interested in. The polynomial f_H takes about two pages in LaTeX so we did not include it here, but we could use Sage to compute with it. Let C_H be the curve with equation f_H, using Sage we computed its geometric genus. Its genus turned out to be 43, so we know it has to be birational to $X_{\mu,H,\mathbb{F}_2}$.

The next step is to find the points in $X_{\mu,H}(\mathbb{F}_{2^6})$ that are supersingular, for this we use the Hasse invariant A_2, it is a modular form of weight 1 over $\mathbb{F}_2$ whose zero's are exactly the supersingular curves and its q expansions is $1 \in \mathbb{F}_2[q]$. Using Magma we listed all points with residue field $\mathbb{F}_{2^6}$ on the desingularisation of $\operatorname{im}\phi \subset \mathbb{P}^2_{\mathbb{F}_2}$ none of these points had 0 as their 3-th coordinate. So we know that $g := A_2^2/\omega_3$ is a function on $X_{\mu,H,\mathbb{F}_2}$ which has a zero at all the supersingular points in $X_{\mu,H}(\mathbb{F}_{2^6})$, comparing q-expansions we found two homogeneous polynomials $g^{num}, g^{den} \in \mathbb{F}_2[x_0, x_1, x_2]$ of degree 40 such that

$$A_2^2 g^{den}(\omega_1, \omega_2, \omega_3) = \omega_3 g^{num}(\omega_1, \omega_2, \omega_3),$$

so that $g = g^{num}/g^{den}$. Choose a $c \in \mathbb{F}_{2^6}$ such that $c^6 + c^5 + 1 = 0$. By looking at the zero's of g we found that, up to relabeling, the points

$$x_i := (0 : c^{2^{i-1}} : 1) \in (\operatorname{im}\phi)(\mathbb{F}_{2^6}) \subset \mathbb{P}^2(\mathbb{F}_{2^6}), \quad 1 \leq i \leq 6$$

correspond to the points $x_1, \ldots, x_6$ of Eq. (14). Define $T = (T_3 - \langle 3\rangle - 3)t_1(T_5)$ where t_1 is as in Proposition 5.3. Then T is as in Proposition 3.4. The matrix of T when seen as acting on $S_2(\Gamma_H, \mathbb{F}_2)$ was seen to be of rank 39 showing that the dimension of $T^*(\operatorname{Cot}_0 J_{\mu,H,\mathbb{F}_2})$ is 39, providing good hope that we can find ω_i such that the matrix A of Proposition 3.7 has rank 6.

Define

$$\begin{aligned}
\omega'_1 &:= (q^{40} + q^{41} + q^{46} + O(q^{48}))\tfrac{\mathrm{d}q}{q}\\
\omega'_2 &:= (q^{37} + q^{43} + O(q^{48}))\tfrac{\mathrm{d}q}{q}\\
\omega'_3 &:= (q^{36} + q^{38} + q^{39} + q^{41} + q^{46} + q^{47} + O(q^{48}))\tfrac{\mathrm{d}q}{q}\\
\omega'_4 &:= (q^{34} + q^{39} + q^{43} + q^{44} + q^{45} + O(q^{48}))\tfrac{\mathrm{d}q}{q}\\
\omega'_5 &:= (q^{33} + q^{39} + q^{45} + O(q^{48}))\tfrac{\mathrm{d}q}{q}\\
\omega'_6 &:= (q^{32} + q^{41} + q^{44} + q^{46} + q^{47} + O(q^{48}))\tfrac{\mathrm{d}q}{q}
\end{aligned}$$

Let q_j be a uniformizer at x_j such that and write $\omega_3 = f_j \mathrm{d}q_j$ and $\omega'_i = f_{i,j}\mathrm{d}q_j$. Then the coefficient $a(\omega'_i, q_j, 1)$ of the matrix A is just $f_{i,j}(0)$. If we view $g_i := \omega'_i/\omega_3$ as a function on $X_{\mu,H,\mathbb{F}_2}$ then because as we saw earlier that $f_j(0) \neq 0$ we see that g_i does not have a pole at x_j and $g_i(x_j) = f_{i,j}(0)/f_j(0)$. The rank does not change if we scale the q_j'th row by $f_j(0)$ so the rank of the matrix A is the same as that of $(g_i(x_j))_{i,j=1}^6$. Comparing q-expansions like we did to write $g = g^{num}/g^{den}$ we again managed to find the function g_i explicitly on our model, allowing us to compute

$$(g_i(x_j))_{i,j=1}^6 := \begin{pmatrix}
c^{46} & c^{29} & c^{58} & c^{53} & c^{43} & c^{23}\\
c^{14} & c^{28} & c^{56} & c^{49} & c^{35} & c^{7}\\
c^{8} & c^{16} & c^{32} & c & c^{2} & c^{4}\\
c^{35} & c^{7} & c^{14} & c^{28} & c^{56} & c^{49}\\
c & c^{2} & c^{4} & c^{8} & c^{16} & c^{32}\\
c^{5} & c^{10} & c^{20} & c^{40} & c^{17} & c^{34}
\end{pmatrix}.$$

The fact that each column is the square of the previous column is explained by

$$g_i(x_j)^2 = \mathrm{Frob}_2(g_i(x_j)) = g_i(\mathrm{Frob}_2(x_j)) = g_i(x_j).$$

The determinant of the above matrix is 1 showing that the map

$$T \circ f_{6,x^{(6)}_{\mathbb{F}_2}} : X^{(6)}_{\mu,H,\mathbb{F}_2} \to J_{\mu,H,\mathbb{F}_2}$$

is a formal immersion at $x^{(6)}_{\mathbb{F}_2}$. So we can apply Lemma 3.1 to get the proposition. □

References

Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990. ISBN 3-540-50587-3. doi: 10.1007/978-3-642-51438-8. URL `http://dx.doi.org/10.1007/978-3-642-51438-8`.

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).

Pete L. Clark, Brian Cook, and James Stankewicz. Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice). *Int. J. Number Theory*, 9(2):447–479, 2013. ISSN 1793-0421. doi: 10.1142/S1793042112501436. URL http://dx.doi.org/10.1142/S1793042112501436.

Brian Conrad, Bas Edixhoven, and William Stein. $J_1(p)$ has connected fibers. *Doc. Math.*, 8:331–408, 2003. ISSN 1431-0635.

Maarten Derickx and Mark van Hoeij. Gonality of the modular curve $X_1(N)$. *J. Algebra*, 417:52–71, 2014. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2014.06.026. URL http://dx.doi.org/10.1016/j.jalgebra.2014.06.026.

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.

Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. ISBN 0-387-23229-X.

Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(273): 579–591, 2011a. ISSN 0025-5718. doi: 10.1090/S0025-5718-10-02369-0. URL http://dx.doi.org/10.1090/S0025-5718-10-02369-0.

Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Families of elliptic curves over quartic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(276): 2395–2410, 2011b. ISSN 0025-5718. doi: 10.1090/S0025-5718-2011-02493-2. URL http://dx.doi.org/10.1090/S0025-5718-2011-02493-2.

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.

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.

Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992. ISBN 0-691-08559-5.

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.

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.

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.

The Developers of Sage. *SageMath, the Sage Mathematics Software System (Version 6.4)*, 2014. http://www.sagemath.org.

Samir Siksek. Chabauty for symmetric powers of curves. *Algebra Number Theory*, 3(2):209–236, 2009. ISSN 1937-0652. doi: 10.2140/ant.2009.3.209. URL http://dx.doi.org/10.2140/ant.2009.3.209.

Glenn Stevens. *Arithmetic on modular curves*, volume 20 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1982. ISBN 3-7643-3088-0.

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

Mathematisch Instituut, Universiteit Leiden, P.O. Box 9512, 2300 RA Leiden, The Netherlands
E-mail address: maarten@mderickx.nl

University of Southern California, 3620 South Vermont Ave., KAP 108, Los Angeles, California 90089-2532, USA
E-mail address: kamienny@usc.edu

University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195-4350, USA.
E-mail address: wstein@gmail.com

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.
E-mail address: Michael.Stoll@uni-bayreuth.de

APPENDIX A: OESTERLÉ'S BOUND

A.1. **Introduction.** The goal of this appendix is to publish a proof of the following well known theorem.

Theorem A.1 (Oesterlé, 1994, unpublished)**.** *Let $K/\mathbb{Q}$ be a number field of degree d, E/K an elliptic curve and $P \in E(K)$ a point of prime order p then*

$$p \leq (3^{d/2}+1)^2.$$

Loïc Merel already proved this theorem in 1994 with a bound of d^{3d^2}, published in [Merel, 1996]. Shortly after Merel, Joseph Oesterlé proved the theorem above for $(d,p) \neq (3,43)$ and in fact Oesterlé's improvement is already announced in Merel's article. The case case $(d,p) = (3,43)$) was later dealt with in [Parent, 2000]. This appendix closely follows Oesterlé's notes which he made available to the first author, although this appendix contains some minor simplifications using literature which didn't exist in 1994. The better bound of Oesterlé is an essential starting point in order to make the explicit computations in the article to which this Appendix is attached possible. Conversely, because of Theorem 1.1 of the main text and the results that $p \leq 7$ if $d = 1$ of [Mazur, 1977] and $p \leq 13$ if $d = 2$ of [Kamienny, 1992b] it suffices to prove the following weaker theorem:

Theorem A.2. *Let $K/\mathbb{Q}$ be a number field of degree d, E/K an elliptic curve and $P \in E(K)$ a point of prime order p then:*

(1) $p \leq (3^{d/2}+1)^2$ *if* $d \geq 6$.
(2) $p < 410$ *if* $d = 3, 4$ *or* 5.

Actually, in his notes Oesterlé first establishes Theorem A.2, and then later goes on to prove Theorem A.1 for $(d,p) \neq (3,43)$ using a comparable but slightly different strategy. The section of his notes where Oesterlé proves Theorem A.1 for $d = 3, 4, 5$, $p < 410$ and $(d,p) \neq (3,43)$ contains no surprising new techniques. This section is omitted since it is covered by the computations in the main text.

Several of Oesterlé's ideas can already be found in the literature, since Pierre Parent generalized several of his ideas to points on elliptic curves whose order is a prime power in [Parent, 1999]. In fact, Theorem A.2 for $d > 25$ is an easy corollary of the following theorem, as will be shown in section A.2.

Theorem A.3. *[Parent, 1999, Thm. 1.6] Let E be an elliptic curve over a number field K of degree d over $\mathbb{Q}$ possessing a K-rational point P of prime power order p^n. Let l be prime different from 2^* and p. Suppose that for every prime ideal ℓ of O_K*

*Parent only mentions the condition $l \neq p$ in his Theorem and not $l \neq 2$. However he mentions it at the beginning of §1.3 and this condition is necessary for his proof of this Theorem to work.

dividing l one has that E has split multiplicative reduction and that P has order p^n in the component group of the Néron model of E, then

$$p^n < 65(2d)^6 \quad \text{if } p > 2 \qquad \text{and} \qquad p^n < 129(3d)^6 \quad \text{if } p = 2.$$

But not all ideas of Oesterlé were generalized by Parent. The main ingredients that are not yet in the literature are the intersection formulas in sections A.5.3 and A.5.4.

Note that from the work of Parent it is also possible to deduce a version of A.2 with the weaker bound $p < 65(2d)^6$ for $d \leq 25$. However the results of the main text would have been very difficult to obtain starting from this weaker bound (although maybe not impossible), since it would require significantly more computer computations as the following table indicates.

d	4	5	6	7	25
$\lfloor (3^{d/2}+1)^2 \rfloor$	100	275	784	2281	847×10^9
$65(2d)^6$	17,039,360	65,000,000	194,088,960	489,419,840	$1,015 \times 10^9$

Acknowledgements. I would like to thank Tessa Schild for her proofreading, Loïc Merel for his help explaining Oesterlé's notes and Bas Edixhoven for his useful discussions and his detailed reading of this text. But most of all I would like to thank Joseph Oesterlé for his help in understanding his proof and giving me his notes. I also want to thank him for allowing me to use it to write this appendix. The two sections A.5.3 and A.5.4 and section A.6 are a translation into English of Oesterlé's notes, where I added some details making claims easier to verify for the reader and replaced certain arguments by references. The rest of this article is a summary of needed background theory and results already present in the literature, much of which was also already in Oesterlé's notes.

A.2. **Proof of Theorem A.2 for $d > 25$.** To be able to use [Parent, 1999, Thm. 1.6] we first have to check whether its conditions are satisfied. This means we first need to prove the following proposition which is similar to Proposition 1.4 of [Parent, 1999].

Proposition A.4. *Let $K/\mathbb{Q}$ be a number field of degree d, E/K an elliptic curve with Néron model $\tilde{E}$ and $P \in E(K)$ a point of prime order p. If $p > (3^{d/2}+1)^2$ then $\tilde{E}$ has split multiplicative reduction at all primes ℓ of $\mathcal{O}_K$ dividing 3 and $\tilde{P}_{\mathcal{O}_K/\ell}$ does not lie in the identity component of $\tilde{E}_{\mathcal{O}_K/\ell}$.*

Remark. The map $X_0(p) \to X_0(1)$ is unramified at the cusp ∞ and ramified of order p at the cusp 0 see [Mazur, 1977, p. 64], so one sees that because $\tilde{P}_{\mathcal{O}_K/\ell}$ lies in a component that is not the identity implies that the pair $(\tilde{E}_{\mathcal{O}_K/\ell}, \langle \tilde{P}_{\mathcal{O}_K/\ell} \rangle)$ has to be the cusp 0 of $X_0(p)$ [Deligne and Rapoport, 1975, VII, §2]. This however is inconsistent with the modular interpretation of the cusps on page 159 of [Mazur, 1977]. The description of the cusps in [Deligne and Rapoport, 1975, VII, §2] shows

that moduli interpretation of the unramified cusp of $X_0(p)$ should be a Néron 1-gon and that of the ramified cusp a Néron p-gon. Luckily this mistake does not affect the main results of [Mazur, 1977] since one can apply the Atkin-Lehner operator W_p to swap the cusps 0 and ∞. This mistake also propagated to works that cite Mazur his article, among for example [Kamienny, 1992a,b, Kamienny and Mazur, 1995], the first author has notified Kamienny and Mazur of this mistake and an erratum is being written.

Proof. Let ℓ be a prime ideal of $\mathcal{O}_K$ dividing 3 and k be its residue field. We want to rule out all types of reduction except split multiplicative where $\tilde{P}_k$ does not lie in the identity component.

The first thing to notice is that $p > (3^{1/2}+1)^2 > 3 = \operatorname{char} k$. This means that the map $\tilde{E}[p](\mathcal{O}_K) \to \tilde{E}[p](k)$ is injective and in particular that $\tilde{P}_k \in \tilde{E}[p](k)$ has order p.

- $\tilde{E}$ does not have good reduction at ℓ, because if it has good reduction, then $\tilde{E}_k$ is an elliptic curve and hence the Hasse bound gives
$$\#\tilde{E}(k) \leq (\sqrt{\#k}+1)^2 \leq (3^{d/2}+1)^2$$
which clearly contradicts that $\tilde{E}(k)$ has a point of order $p > (3^{d/2}+1)^2$.
- $\tilde{E}$ does not have additive reduction at ℓ. This is because additive reduction means that we have an exact sequence:
$$\mathbb{G}_a(k) \to \tilde{E}(k) \to \phi(k)$$
where ϕ is the component group of $\tilde{E}_k$. This means that either $\tilde{P}_k$ lies in the image of $\mathbb{G}_a(k)$, in which case $p = 3$ or $p \mid \#\phi(k) \leq 4$, with both possibilities leading to a contradiction with $p > (3^{1/2}+1)^2 > 7$.
- $\tilde{E}$ does not have non-split multiplicative reduction at ℓ. This is because this would mean that we have an exact sequence
$$\tilde{\mathbb{G}}_{m,k}(k) \to \tilde{E}(k) \to \phi(k)$$
$\tilde{\mathbb{G}}_{m,k}$ is the quadratic twist of the multiplicative group over k. In this case either
$$p|\#\tilde{\mathbb{G}}_m(k) = \#k + 1 < (3^{d/2}+1)^2 \text{ or } p|\#\phi(k) \leq 2,$$
with both possibilities leading to a contradiction with $p > (3^{d/2}+1)^2$.
- If $\tilde{E}$ has split multiplicative reduction, then $\tilde{P}_k$ cannot lie in the identity component of $\tilde{E}_k$. This is because the identity component is isomorphic to $\mathbb{G}_m$ and $\#\mathbb{G}_m(k) = \#k - 1 < (3^{d/2}+1)^2 < p$.

□

Now Theorem A.2 easily follows from Theorem A.3 using the following inequality:

$$\text{If } d \geq 26 \text{ then } (3^{d/2}+1)^2 > 65(2d)^6. \tag{A.1}$$

Indeed, suppose that K is a number field of degree $d \geq 26$ over $\mathbb{Q}$, E/K an elliptic curve and $P \in E(K)$ of prime order p. Then Proposition A.4 says that either $p < (3^{d/2}+1)^2$, in which case we are done, or the hypotheses of Theorem A.3 are satisfied. In the latter case one gets

$$(3^{d/2}+1)^2 > 65(2d)^6 > p$$

and Theorem A.2 follows.

A.3. **The Winding Quotient.** This section only contains a short summary about the winding quotient $J_0^{\mathbf{e}}(\mathbb{Q})$. For more details and the fact that $J_0^{\mathbf{e}}(\mathbb{Q})$ is finite, see either [Merel, 1996, §1] or [Parent, 1999, §3.8] or §4 of the main text. Note that the finiteness of $J_0^{\mathbf{e}}(\mathbb{Q})$ is proved by using the analytic rank 0 implies algebraic rank 0 case of the BSD conjecture as proven in [Kolyvagin and Logachëv, 1989] completed by [Bump et al., 1990] or [Murty and Murty, 1991].

If $a, b \in \mathbb{Q} \cup \{\infty\}$, then we define $\{a, b\} \in H_1(X_0(p)(\mathbb{C}), cusps, \mathbb{Z})$ to be the element given by a path from a to b in $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. The element $\{a, b\}$ is called a modular symbol. If $k \in \mathbb{Z}_{(p)}$ is a fraction whose denominator is not divisible by p, then define

$$\lambda(k) := \{0, 1/k\}. \tag{A.2}$$

The element $\lambda(k)$ only depends on $k \mod p$, hence one can also see λ as a map

$$\lambda : \mathbb{Z}/p\mathbb{Z} \to H_1(X_0(p)(\mathbb{C}), cusps, \mathbb{Z}).$$

The $\lambda(k)$ where k ranges over $\mathbb{Z}/p\mathbb{Z}$ are known to generate $H_1(X_0(p)(\mathbb{C}), cusps, \mathbb{Z})$ and if $k \not\equiv 0 \mod p$ then $\lambda(k) \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, and hence the element $\lambda(0) = \{0, \infty\}$ generates the rank 1 $\mathbb{Z}$-module $H_1(X_0(p)(\mathbb{C}), cusps, \mathbb{Z})/H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$.

We have an isomorphism $H_1(X_0(p)(\mathbb{C}), \mathbb{R}) \cong H^1(X_0(p)(\mathbb{C}), \Omega^1)^\vee$, of real vector spaces, given by integration. So the map

$$\begin{aligned} \mathbf{e} : H^1(X_0(p)(\mathbb{C}), \Omega^1) &\to \mathbb{C} \\ \omega &\mapsto -\int_{\{0,\infty\}} \omega \end{aligned} \tag{A.3}$$

defines an element $\mathbf{e} \in H_1(X_0(p)(\mathbb{C}), \mathbb{R})$ under this isomorphism, which is called the winding element. Actually $(p-1)\mathbf{e} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ showing that $\mathbf{e} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$. Let $\mathbb{T}$ be the sub algebra of $\operatorname{End} H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ generated by the Hecke operators and the Atkin-Lehner involution, then $\mathbb{T}$ also acts faithfully on $J_0(p)$, the Jacobian of $X_0(p)$ over $\mathbb{Z}[1/p]$. Let $\mathcal{J}_{\mathbf{e}} \subseteq \mathbb{T}$ be the annihilator of $\mathbf{e}$, then

$$J_0^{\mathbf{e}} := J_0(p)/\mathcal{J}_{\mathbf{e}} J_0(p)$$

is called the winding quotient.

Let $X_0(p)^{(d)}$ be the d-th symmetric power of the modular curve $X_0(p)$, then one has a natural map $X_0(p)^{(d)} \to J_0(p)$ by sending a divisor D of degree d to the linear

equivalence class of $D - d\infty$. Composing with the quotient map $J_0(p) \to J_0^{\mathbf{e}}$ gives us the map

$$f_d : X_0(p)^{(d)} \to J_0^{\mathbf{e}}. \tag{A.4}$$

Now if $x \in X_0(p)(K)$ is a point where K is a number field of degree d and $\sigma_1, \ldots, \sigma_d : K \to \bar{\mathbb{Q}}$ are the different embeddings, then define

$$x^{(d)} := \sigma_1(x) + \cdots + \sigma_d(x) \in X_0(p)^{(d)}(\mathbb{Q}).$$

We will also write $x^{(d)}$ for $\sum_{i=1}^{d} x$ if $x \in X_0(p)(\mathbb{Q})$.

A.4. **Kamienny's Criterion.** The discussion that follows is based on section 4.12 of [Parent, 1999], who himself says that he is following Oesterlé's unpublished exposition. The main reason for following Parent, is because this allows certain proofs to be skipped and instead just cite Parent. This section is called Kamienny's criterion because the main ideas originate from [Kamienny, 1992a, §3] , although many of Kamienny's arguments have been sharpened to get the needed statement of this section. The following proposition is a slight variation of [Parent, 1999][Thm. 4.15], although his Theorem is much shorter. The reason the statement of Theorem 4.15 of Parent is so much shorter is because Parent did not include his running hypotheses in his Theorem.

Proposition A.5. *Let d be an integer and p be a prime such that $p > (3^{d/2} + 1)^2$. If there exists a number field $K/\mathbb{Q}$ of degree d, an elliptic curve E/K and a point $P \in E(K)$ of prime order p, then the map $f_d : X_0(p)^{(d)} \to J_0^e$ of equation A.4 above is not a formal immersion at $\infty_{\mathbb{F}_3}^{(d)}$.*

Proof. Let $K/\mathbb{Q}$ be a number field of degree d, E/K an elliptic curve and $0 \neq P \in E(K)[p]$. Consider j resp. $j' \in X_0(p)(K)$ to be the points corresponding to $(E, \langle P \rangle)$ resp. $(E/\langle P \rangle, E[p]/\langle P \rangle)$. By proposition A.4 one sees that $j_{\mathbb{F}_3}^{(d)} = 0_{\mathbb{F}_3}^{(d)}$ and hence $j_{\mathbb{F}_3}^{\prime(d)} = \infty_{\mathbb{F}_3}^{(d)}$. Now because $J_0^e(\mathbb{Q})$ is torsion and $f_d(j^{\prime(d)})_{\mathbb{F}_3} = f_d(\infty^{(d)})_{\mathbb{F}_3} = 0$ we get $f_d(j^{\prime(d)}) = f_d(\infty^{(d)}) = 0$. But $j^{\prime(d)} \neq \infty^{(d)}$, hence we can apply [Parent, 1999][Lemma 4.13] to get the proposition. □

The above proposition reduces the proof of Theorem A.2 to checking whether f_d is a formal immersion.

Theorem A.6. *[Parent, 1999][Thm 4.18] Let $l > 2$ be a prime, then the following two statements are equivalent:*

1. *f_d is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$.*
2. *$T_1\mathbf{e}, \ldots, T_d\mathbf{e}$ are linearly independent in $\mathbb{T}\mathbf{e}/l\mathbb{T}\mathbf{e}$.*

A.5. **Intersection numbers of modular symbols.** Since we can view $X_0(p)(\mathbb{C})$ as a smooth oriented real manifold we get an intersection pairing on homology. The intersection pairing $\bullet : H_1(X_0(p)(\mathbb{C}), \mathbb{Z}) \times H_1(X_0(p)(\mathbb{C}), \mathbb{Z}) \to \mathbb{Z}$ also gives a pairing $\bullet : H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l) \times H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l) \to \mathbb{F}_l$. It would be convenient to be able to use these pairings to check the linear independence of $T_1\mathbf{e}, \ldots, T_d\mathbf{e}$ in $\mathbb{T}\mathbf{e}/l\mathbb{T}\mathbf{e}$. However while $\mathbb{T}\mathbf{e} \subset H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$, it is not true that $\mathbb{T}\mathbf{e} \subset H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, so checking the linear independence cannot be checked directly with the intersection pairing. The solution, which will be worked out in more detail later, is to chose a Hecke operator I in such a way that $I\mathbf{e} \subseteq H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ and use this to write down a linear map

$$I : \mathbb{T}\mathbf{e} \to H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l)$$

after which we can use the intersection pairing to check linear independence.

A.5.1. *Action of the Hecke operators on homology.* For $r > 0$ an integer and define $\sigma_1(r) := \sum_{d|r, d>0} d$. Using this definition one can compute $(T_r - \sigma_1(r))\,\mathbf{e}$ as follows.

Lemma A.7. *[Merel, 1996, Lemma 2] If p is a prime and $r < p$ a positive integer, then the following equality holds in $H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$*

$$(T_r - \sigma_1(r))\,\mathbf{e} = - \sum_{\substack{a > b \geq 0 \\ d > c > 0 \\ ad - bc = r}} \lambda(c/d).$$

Where one should note that our element $\lambda(k)$ is denoted by $\xi(k)$ in [Merel, 1996].

Remark. Note that since $p > r = ad - bc \geq ad - (a-1)(d-1) \geq d > c > 0$, we see that none of the c and d in the sum are divisible by p. This means that the right hand side actually is an element of $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$. Since $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ is torsion free, the equality actually holds in $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, and in particular $(T_r - \sigma_1(r))\,\mathbf{e} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$. This is also something that could have been seen directly by noting that the boundary of $(T_r - \sigma_1(r))\,\{0, \infty\}$ is zero.

A.5.2. *The intersection number $\lambda(k) \bullet \lambda(k')$.* For p a prime and $1 \leq k < p$ an integer let k^* be the integer such that $1 \leq k^* < p$ and $kk^* \equiv -1 \mod p$ and let C_k denote the oriented straight line segment in $\mathbb{C}$ from $e^{2\pi ik/p}$ to $e^{2\pi ik^*/p}$. Recall that if $k \in \mathbb{Z}/p\mathbb{Z}^*$ then $\lambda(k)$ was defined as $\{0, 1/k\} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$. The intersection number of $\lambda(k)$ and $\lambda(k')$ can be computed as follows.

Lemma A.8. *[Merel, 1996, Lemma 4.] Let k, k' be two integers such that $1 \leq k < p$ and $1 \leq k' < p$. If $k' \neq k$ and $k' \neq k^*$ then $\lambda(k) \bullet \lambda(k')$ equals the intersection number $C_{k'} \bullet C_k$ and $\lambda(k) \bullet \lambda(k') = 0$ otherwise.*

Where in [Merel, 1996] the element k^* is denoted by k_*. The fact that $\lambda(k) \bullet \lambda(k') = 0$ if $k' = k$ or $k' = k^*$ is not mentioned by Merel. But this follows easily from the fact that $\bullet$ is an alternating bilinear form and $\lambda(k) = -\lambda(k^*)$.

The reason that the order of intersection is swapped is because Merel first proves $\lambda(k) \bullet \lambda(k') = C'_k \bullet C'_{k'}$ where C'_k denotes the oriented straight line segment in $\mathbb{C}$ from $e^{-2\pi i k/p}$ to $e^{-2\pi i k^*/p}$, and then concludes by $C'_k \bullet C'_{k'} = C_{k'} \bullet C_k$ because both complex conjugation and reversing the order of intersection changes sign. The lemma above is independent of the choice of orientation on $\mathbb{C}$ as long as one takes the orientation on $X_0(p)(\mathbb{C})$ to be the one compatible with the map $\mathbb{H} \to X_0(p)(\mathbb{C})$. From now on we will take the orientation on $\mathbb{C}$ such that $[-1,1] \bullet [-i,i] = 1$ where $[a,b]$ denotes the oriented straight line segment from a to b.

Definition A.9. Let $H : \mathbb{R} \to \mathbb{R}$ be the function given by

$$H(x) = \begin{cases} 1 \text{ if } x > 0 \\ \frac{1}{2} \text{ if } x = 0 \\ 0 \text{ if } x < 0 \end{cases}$$

With this definition the above lemma translates to

$$\lambda(k) \bullet \lambda(k') = -H(k'-k) + H(k'-k^*) + H(k'^*-k) - H(k'^*-k^*).$$

This equality can be verified by first checking that the both sides only depend on the cyclic ordering, with possible equalities, of k, k^*, k', k'^* in $\mathbb{Z}/p\mathbb{Z}$. And then verifying it holds for the possible cyclic orderings.

A.5.3. *The intersection number $I_r\mathbf{e} \bullet \lambda(k)$.* Let p be a prime and let $1 \leq r < p$ be an integer. Define

$$I_r := T_r - \sigma_1(r),$$

then $I_r\mathbf{e} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$.

Proposition A.10. *Let p be a prime number and let r, k be integers such that $1 \leq k < p$ and $1 \leq r < p$, then one has*

$$I_r\mathbf{e} \bullet \lambda(k) = \sum_{s|r} \left(\left\lfloor \frac{sk}{p} \right\rfloor - \left\lfloor \frac{sk^*}{p} \right\rfloor \right) + v_r(k) - v_r(k^*)$$

where for $i \in \mathbb{Z}$ one defines $v_r(i)$ to be the following quantity

$$v_r(i) = \#\left\{a', b', c', d' \in \mathbb{N}_{\geq 1} \mid a'd' + b'c' = r, d'i \equiv c' \mod p\right\}$$

Proof. Define the map $x \mapsto k_x$ from $\mathbb{P}^1(\mathbb{Q})$ to the set $\{1, \ldots, p\}$ by sending a simple fraction x where p does not divide the denominator to the unique element congruent to it modulo p, and one defines $k_x = p$ for $x = \infty$ and the fractions where p divides the denominator. Combining Lemmas A.7 and A.8 one gets

$$I_r\mathbf{e} \bullet \lambda(k) = \sum_{\substack{a > b \geq 0 \\ d > c > 0 \\ ad - bc = r}} \left(H(k - k_{c/d}) - H(k - k_{-d/c}) - H(k^* - k_{c/d}) + H(k^* - k_{-d/c}) \right)$$

The equality stays true if we also include the terms with $c = 0$ in the sum, since those terms are all 0. Now let B_r be the set of all matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ of determinant r with $a > b \geq 0$,$d > c \geq 0$ and let B'_r (resp. B''_r) be the set of matrices in B_r with $b \neq 0$ (resp. $c \neq 0$). Now we have a bijection between B'_r and B''_r by sending the matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to $\left[\begin{smallmatrix} b & -a+mb \\ d & -c+md \end{smallmatrix}\right]$ where m is the unique integer such that $0 \leq -a + mb < b$ (its inverse is obtained by sending $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to $\left[\begin{smallmatrix} -b+na & a \\ -d+na & c \end{smallmatrix}\right]$ where n is the unique integer such that $0 \leq -d + na < c$). This shows

$$I_r \mathbf{e} \bullet \lambda(k) = S_1 - S_2 + S_3, \text{ where}$$

$$S_1 = \sum_{B_r \setminus B'_r} \big(H(k - k_{c/d}) - H(k^* - k_{c/d}\big)$$

$$S_2 = \sum_{B_r \setminus B''_r} \big(H(k - k_{-d/c}) - H(k^* - k_{-d/c})\big)$$

$$S_3 = \sum_{B'_r} \big(H(k - k_{c/d}) - H(k - k_{(c-md)/d}) - H(k^* - k_{c/d}) + H(k^* - k_{(c-md)/d})\big)$$

Let's start by calculating S_2. The matrices in $B_r \setminus B'_r$ are the matrices of the form $\left[\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right]$ with $ad = r$ and $0 \leq c < d$. For $s \mid r$ let $S_1(s)$ be the contribution to S_1 of coming from the matrices such that $d = s$. The contribution to $S_1(s)$ of the matrix with $c = 0$ is 0. For $1 \leq c < d$ the number $k_{c/d}$ is equal to $\frac{up+c}{d}$, where u is the element $1 \leq u < d$ congruent to $-c/p \mod d$, and $k_{c/d}$ is the smallest integer $\geq \frac{up}{d}$. The map which associates u to c is a permutation of $\{1, \ldots, d-1\}$. So the number of $c \in \{1, \ldots, d-1\}$ such that $k_{c/d} \leq k$ is equal to the number of $u \in \{1, \ldots, d-1\}$ such that $\frac{up}{d} \leq k$. An analogues argument with k replaced by k^* gives that

$$S_1 = \sum_{s|r} \left(\left\lfloor \frac{sk}{p} \right\rfloor - \left\lfloor \frac{sk^*}{p} \right\rfloor \right) - \frac{1}{2} S'_1 + \frac{1}{2} S''_1,$$

where S'_1 (resp. S''_1) is the number of pairs of integers (c, d) such that $d \mid r$, $1 \leq c < d$ and $k_{c/d} = k$ (resp. $k_{c/d} = k^*$).

The matrices in $B_r \setminus B''_r$ all have $c = 0$, hence $k_{-d/c} = p$ and $H(k - k_{-d/c}) = H(k^* - k_{-d/c}) = 0$ implying

$$S_2 = 0.$$

What remains is to determine S_3. Let $x = c/d$ be a rational number occurring in S_3, then one has that $p > r \geq d > 0$ hence $p \nmid d$. In particular if $k_x \neq 1$, then $k_{x-1} = k_x - 1$ and hence $H(k - k_x) - H(k - k_{x-1})$ equals $-\frac{1}{2}$ if $k = k_x$ or $k = k_{x-1}$ and equals 0 otherwise. If $k_x = 1$ then $k_{x-1} = p$ and $H(k - k_x) - H(k - k_{x-1})$ equals $1/2$ if $k = 1$ and 1 if $1 < k < p$. In particular, whether $k_x = 1$ or $k_x \neq 1$, the following always holds

$$H(k - k_x) - H(k - k_{x-1}) - H(k^* - k_x) + H(k^* - k_{x-1}) =$$

$$\frac{1}{2}\left(\#(\{k^*\}\cap\{k_x,k_{x-1}\})-\#(\{k\}\cap\{k_x,k_{x-1}\})\right).$$

By induction on m, one sees that for all $m\geq 1$,

$$H(k-k_x)-H(k-k_{x-m})-H(k^*-k_x)+H(k^*-k_{x-m})$$

equals the number of integers $i\in\{0,\dots,m\}$ such that $k^*=k_{x-i}$ minus the number of integers such that $k=k_{x-i}$, taking into account that one counts $i=0$ and $i=m$ only for half an integer.

Now to evaluate S_3, let us first define U (resp. U', resp. U'') as the set of pairs $(\left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right],i)$ with $\left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right]\in B'_r$ and $1\leq i<m$ (resp. $i=0$, resp. $i=m$) where m is the unique integer such that $0\leq -a+mb<b$. Let $u(k)$ (resp. $u'(k)$, resp. $u''(k)$) be the number of these pairs such that $k=k_{(c-id)/d}$. This means that

$$S_3=u(k^*)+\frac{1}{2}u'(k^*)+\frac{1}{2}u''(k^*)-u(k)-\frac{1}{2}u'(k)-\frac{1}{2}u''(k).$$

The map $(\left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right],i)\mapsto\left[\begin{smallmatrix}b&-a+ib\\d&-c+id\end{smallmatrix}\right]$ is a bijection between U and the set of matrices of the form $\left[\begin{smallmatrix}a'&-b'\\c'&d'\end{smallmatrix}\right]$ with a',b',c',d' integers ≥ 1 with $a'd'+b'c'=r$ (its inverse is given by sending $\left[\begin{smallmatrix}a'&-b'\\c'&d'\end{smallmatrix}\right]$ to $\left(\left[\begin{smallmatrix}b'+ja'&a'\\-d'+jc'&c'\end{smallmatrix}\right],j\right)$ where j is the unique integer such that $0\leq -d'+jc'<c'$). Under this bijection, $k=k_{(c-id)/d}$ if and only if $k\equiv -d'/c' \mod p$ or equivalently if $k^*\equiv c'/d' \mod p$. This shows that $u(k)=v_r(k^*)$ and $u(k^*)=v_r(k)$.

The integer $u'(k)$ equals the number of quadruples of integers (a,b,c,d) such that $a>b>0$, $d>c\geq 0$, $ad-bc=r$ and $k\equiv c/d \mod p$. The bijection between B'_r and B''_r, one can show that $u''(k)$ is equal to the number of quadruples (a,b,c,d) such that $a>b\geq 0$, $d>c>0$, $ad-bc=r$ and $k\equiv -d/c \mod p$. From this it follows that $u''(k)=u'(k^*)+S''_1$ and $u''(k^*)=u'(k)+S'_1$ and hence

$$S_3=v_r(k)-v_r(k^*)+\frac{1}{2}S'_1-\frac{1}{2}S''_1.$$

Putting the formulas for S_1,S_2 and S_3 together finally finishes the proof. □

If one defines $v'_r(i)$ by the following

$$v'_r(i):=\#\left\{a',b',c',d'\in\mathbb{N}_{\geq 1}\mid \gcd(c',d')=1,\, a'd'+b'c'=r,\, d'i\equiv c' \mod p\right\},$$

then for $r<p$ one has $v_r(k)=\sum_{s|r}v'_s(k)$. If one also defines the Hecke operators I'_r for $1\leq r<p$ to be such that

$$I_r=\sum_{s|r}I'_s, \tag{A.5}$$

then an equivalent form of the above proposition is obtained by using he Möbius inversion formula to remove the sum over the divisors of r.

Proposition A.11. *Let p be a prime number and let $1 \leq k, k^* < p$ be integers such that and $kk^* \equiv -1 \mod p$. If r is an integer such that $1 \leq r < p$ then*

$$I'_r\mathbf{e} \bullet \lambda(k) = \left\lfloor \frac{rk}{p} \right\rfloor - \left\lfloor \frac{rk^*}{p} \right\rfloor + v'_r(k) - v'_r(k^*)$$

where for $i \in \mathbb{Z}$ one defines $v'_r(i)$ to be the following quantity

$$v'_r(i) = \#\left\{a', b', c', d' \in \mathbb{N}_{\geq 1} \mid \gcd(c', d') = 1,\ a'd' + b'c' = r,\ d'i \equiv c' \mod p\right\}$$

A.5.4. *The intersection number $I'_r\mathbf{e} \bullet \left\{0, \frac{a}{c}\right\}$.*

Proposition A.12. *Let p be a prime and r, c, d be integers such that $1 \leq r$, $1 \leq d < c < \frac{p}{r}$ and c and d are coprime. Define a, b to be the integers such that $ad - bc = 1$, $0 \leq a < c$ and $0 \leq b < d$. Define $1 \leq k < p$ and $1 \leq k^* < p$ to be the integers that are equal to c/d and $-d/c$ modulo p and finally let u, u^* be such that $dk = up + c$ and $ck^* = u^*p - d$. Then $0 \leq u < d$, $0 \leq u^* < c$ and*

$$I'_r\mathbf{e} \bullet \lambda(k) = \left\lfloor \frac{ru}{d} \right\rfloor - \left\lfloor \frac{rb}{d} \right\rfloor + \left\lfloor \frac{ra}{c} \right\rfloor - \left\lfloor \frac{ru^*}{c} \right\rfloor$$

Proof. Because $\frac{rk}{p} = \frac{ru}{d} + \frac{rc}{pd}$ and $0 \leq \frac{rc}{pd} < \frac{1}{d}$ one has

$$\left\lfloor \frac{rk}{p} \right\rfloor = \left\lfloor \frac{ru}{d} \right\rfloor.$$

And because $\frac{rk^*}{p} = \frac{ru^*}{c} - \frac{rd}{pc}$ and $0 < \frac{rd}{pc} < \frac{1}{c}$ one has

$$\left\lfloor \frac{rk^*}{p} \right\rfloor = \left\lfloor \frac{ru^* - 1}{c} \right\rfloor.$$

Now let a', b', c', d' be a quadruple as in the definition of $v'_r(k)$, because $d'k \equiv c' \mod p$ one has $c'd \equiv cd' \mod p$. Because $1 \leq cd' < cr < p$ and $1 \leq c'd < rd < p$, one even has $c'd = cd'$ and because $\gcd(c', d') = \gcd(c, d) = 1$, it follows that $c = c'$ and $d = d'$. Since $rad - rbc = r = a'd + b'c$ there exists an integer t such that $tc = ra - a'$ and $td = rb + b'$. The fact that $a', b' \geq 1$ translate into $\left\lfloor \frac{rb}{d} \right\rfloor < t \leq \left\lfloor \frac{ra-1}{c} \right\rfloor$ and since $\frac{rb}{d} < \frac{ra}{c}$ one has $\left\lfloor \frac{rb}{d} \right\rfloor \leq \left\lfloor \frac{ra-1}{c} \right\rfloor$.

This shows that under the assumptions on r, k and p, that $v'_r(k)$ is equal to the number of integers t satisfying $\left\lfloor \frac{rb}{d} \right\rfloor < t \leq \left\lfloor \frac{ra-1}{c} \right\rfloor$, or in formulas:

$$v'_r(k) = \left\lfloor \frac{ra - 1}{c} \right\rfloor - \left\lfloor \frac{rb}{d} \right\rfloor.$$

Now let a', b', c', d' be a quadruple as in the definition of $v'_r(k^*)$. Since $d'k^* \equiv c' \mod p$, we get $cc' + dd' \equiv 0 \mod p$. Now $a'd' + b'c' = r$ implies $c' + d' \leq r$ and hence $1 \leq cc' + dd' < c(c' + d') \leq cr < p$ which is incompatible with $cc' + dd' \equiv 0 \mod p$ so,

$$v'_r(k^*) = 0.$$

Putting the above equalities together one gets

$$I'_r\mathbf{e}\bullet\lambda(k) = \left\lfloor\frac{rk}{p}\right\rfloor - \left\lfloor\frac{rk^*}{p}\right\rfloor + v'_r(k) - v'_r(k^*) = \left\lfloor\frac{ru}{d}\right\rfloor - \left\lfloor\frac{rb}{d}\right\rfloor + \left\lfloor\frac{ra-1}{c}\right\rfloor - \left\lfloor\frac{ru^*-1}{c}\right\rfloor.$$

What remains to be shown is

$$\left\lfloor\frac{ra}{c}\right\rfloor - \left\lfloor\frac{ra-1}{c}\right\rfloor = \left\lfloor\frac{ru^*}{c}\right\rfloor - \left\lfloor\frac{ru^*-1}{c}\right\rfloor$$

But this is indeed the case. Since c is coprime with both u^* and a, one sees that the left and right hand side are 1 if c divides r and 0 otherwise. □

Taking $1 < k < p/r$ an integer and $d = 1$ and $c = k$ in the above proposition gives $a = 1$ which proves:

Corollary A.13. *Let p be prime and $k \geq 2$, $r \geq 1$ be integers such that $kr < p$, and let $1 \leq u^* < k$ be the inverse of p modulo k then*

$$I'_r\mathbf{e}\bullet\lambda(k) = \left\lfloor\frac{r}{k}\right\rfloor - \left\lfloor\frac{ru^*}{k}\right\rfloor.$$

Proposition A.14. *Let $c \geq 2, r \geq 1$ be integers such that $cr < p$ and $1 \leq a < c$ an integer coprime to c. Let $1 \leq u^* < c$ be such that $apu^* \equiv 1 \mod c$ then*

$$I'_r\mathbf{e}\bullet\left\{0, \frac{a}{c}\right\} = \left\lfloor\frac{ra}{c}\right\rfloor - \left\lfloor\frac{ru^*}{c}\right\rfloor.$$

Proof. We do this by induction on c. If $c = 2$ then $a = 1$ and it follows from the above corollary.

For larger c, let b, d such that $ad - bc = 1$ with $1 \leq d < c$. Because $a < c$ it follows that $b < d$. The case $d = 1$ implies $b = 0$ and hence $a = 1$ which is dealt with by the above corollary, so we can assume $d \geq 2$.

Let $1 \leq k < p$ be such that $k \equiv c/d \mod p$, then

$$\begin{bmatrix} a - bk & b \\ c - dk & d \end{bmatrix}\left\{0, \frac{1}{k}\right\} = \left\{\frac{b}{d}, \frac{a}{c}\right\}.$$

Since $k \equiv c/d \mod p$ the above matrix is in $\Gamma_0(p)$ and hence $\lambda(k) = \left\{\frac{b}{d}, \frac{a}{c}\right\}$. Since $ad \equiv 1 \mod c$ we see that the u^* of this proposition agrees with that of Proposition A.12. If we take u to be such that $pu = dk - c$, and using $bc \equiv -1 \mod d$ we get that $1 \leq u < d$ and $bpu \equiv 1 \mod d$. So using the induction hypothesis we have $I'_r\mathbf{e}\bullet\left\{0, \frac{b}{d}\right\} = \left\lfloor\frac{rb}{d}\right\rfloor - \left\lfloor\frac{ru}{d}\right\rfloor$. Writing $\left\{0, \frac{a}{c}\right\} = \left\{0, \frac{b}{d}\right\} + \left\{\frac{b}{d}, \frac{a}{c}\right\} = \left\{0, \frac{b}{d}\right\} + \lambda(k)$ finally gives

$$I'_r\mathbf{e}\bullet\left\{0, \frac{a}{c}\right\} = \left\lfloor\frac{rb}{d}\right\rfloor - \left\lfloor\frac{ru}{d}\right\rfloor + \left\lfloor\frac{ru}{d}\right\rfloor - \left\lfloor\frac{rb}{d}\right\rfloor + \left\lfloor\frac{ra}{c}\right\rfloor - \left\lfloor\frac{ru^*}{c}\right\rfloor = \left\lfloor\frac{ra}{c}\right\rfloor - \left\lfloor\frac{ru^*}{c}\right\rfloor$$

□

A.6. **Putting it all together.** With all these intersection formulas now at our disposal it is time to return to the question of when the morphism

$$f_d : X_0(p) \to J_0^e$$

of (A.4) is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ using Theorem A.6.

Let T'_r be the Hecke operators such that $T_r = \sum_{s|r} T'_s$ then one easily sees that for $r < p$ one has $\sum_{s|r} I'_s = T_r - \sigma_1(r) = \sum_{s|r}(T'_s - s)$ and hence $I'_s = T'_s - s$. Define $L_r := T'_{2r} - 2T'_r$ then $L_r = I'_{2r} - 2I'_r$. Using $T_{2r} = T_2T_r$ if r is odd and $T_{2r} = T_2T_r - 2T_{r/2}$ if r is even, one can deduce that for $1 \leq r < p$:

$$\sum_{s|r} I_2T'_s = (T_2 - 3)T_r = \sum_{s|r} L_s - \sum_{s|r,\, s \text{ even}} L_{s/2},$$

from which it follows that

$$I_2T'_r = \begin{cases} L_r & \text{if } r \text{ is odd} \\ L_r - L_{r/2} & \text{if } r \text{ is even} \end{cases}$$

Since $I_2\mathbf{e} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ we have that I_2 induces a linear map $I_2 : \mathbb{T}\mathbf{e}/l\mathbb{T}\mathbf{e} \to H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l)$, and we get the following addition to A.6.

Theorem A.15. *If $l > 2, p$ are distinct is primes and $d > 0$ an integer with $2d < p$ then $f_d : X_0(p)^{(d)} \to J_0^e$ is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ if either*

1. *$L_1\mathbf{e}, L_2\mathbf{e} \ldots, L_d\mathbf{e}$ are linearly independent in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l)$,*
2. *$I'_2\mathbf{e}, I'_3\mathbf{e}, \ldots, I'_{2d}\mathbf{e}$ are linearly independent in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l)$, or*
3. *$I_2\mathbf{e}, I_3\mathbf{e}, \ldots, I_{2d}\mathbf{e}$ are linearly independent in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l)$.*

In the above theorem the statements 2 and 3 are equivalent and they both imply the first. In Oesterlé's notes there is a part where he proved that the linear independence condition 2 of the above theorem always holds if $d > 2$ and $p/\log^4 p \geq (2d)^6$, giving a proof of Theorem A.2 for $d > 36$. We skip this part of the argument since a variation of this argument is already in [Parent, 1999, §5]. For the smaller d Oesterlé verified the linear independence 1 using the following proposition.

Proposition A.16. *Let $d \geq 1$ be an integer, $M \geq 3$ an odd integer and $l \geq 3$ a prime. Let $\varepsilon : (\mathbb{Z}/M\mathbb{Z})^* \to 0, 1$ be the map such that $\varepsilon(n) = 0$ if n is represented by an integer between 0 and $M/2$ and 1 otherwise. Let $u \in (\mathbb{Z}/M\mathbb{Z})^*$ and define the matrix $R_{d,u}$ to be the matrix with rows indexed by $\{1, \ldots, d\}$ and columns indexed by $(\mathbb{Z}/M\mathbb{Z})^*$ and whose (r, a) entry is $\varepsilon(ra) - \varepsilon(ru/a)$.*

If the matrix $R_{d,u}$ has rank d modulo l, then $L_1\mathbf{e}, \ldots, L_d\mathbf{e}$ are linearly independent in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_l)$ for all primes p such that $p > 2dM$, and $pu \equiv 1 \mod M$.

Proof. The congruence $pu \equiv 1 \mod M$ implies that $ap(u/a) \equiv 1 \mod M$ and hence $u^* \equiv u/a \mod M$ where u^* is as in Proposition A.14 with $c = M$. Now because $L_r = I'_{2r} - 2I'_r$ and $\varepsilon(n) = \left\lfloor \frac{2n}{M} \right\rfloor - 2\left\lfloor \frac{n}{M} \right\rfloor$, it follows from A.14 that for all primes p such that $p > 2dM$ and $pu \equiv 1 \mod M$ that $L_r\mathbf{e} \bullet \{0, a/M\} = \varepsilon(ra) - \varepsilon(ru/a)$. Hence the linear independence holds if $R_{d,u}$ has rank d modulo l. □

A.6.1. *Proof of Theorem A.2 for* $3 \leq d \leq 25$. The following table lists for all integers $3 \leq d \leq 26$ an integer M_d such that reduction of the matrix $R_{d,u}$ modulo 3 of the above proposition has rank d for all $u \in \mathbb{Z}/M\mathbb{Z}^*$.

d	3	4	5	6	7	8	9	10	11	12	13	14
M_d	29	37	41	43	47	47	53	53	53	61	73	73

d	15	16	17	18	19	20	21	22	23	24	25	26
M_d	79	79	89	89	89	101	101	109	109	109	127	127

These values of M_d have been found using a computer and the code can be found at `https://sage.math.leidenuniv.nl/home/pub/51`. Since the M_d in the table satisfy $2dM_d < (3^{d/2}+1)^2$ if $d > 6$ and $2dM_d \leq 410$ for $d = 3, 4, 5$ it follows from Proposition A.16 that $L_1\mathbf{e}, \ldots, L_d\mathbf{e}$ are linearly independent in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_3)$ for all $p > \max((3^{d/2}+1)^2, 410)$. Hence from Theorem A.15 it follows that $f_d : X_0(p)^{(d)} \to J_0^{\varepsilon}$ is a formal immersion at $\infty_{\mathbb{F}_3}^{(d)}$ for all $p > \max((3^{d/2}+1)^2, 410)$, so that Theorem A.2 follows from Proposition A.5.

References

Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for L-functions of modular forms and their derivatives. *Invent. Math.*, 102(3): 543–618, 1990. ISSN 0020-9910. doi: 10.1007/BF01233440. URL `http://dx.doi.org/10.1007/BF01233440`.

P. Deligne and M. Rapoport. Correction to: "Les schémas de modules de courbes elliptiques" (*modular functions of one variable, ii* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316, Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973). In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages p. 149. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

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).

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.

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.

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.

M. Ram Murty and V. Kumar Murty. Mean values of derivatives of modular L-series. *Ann. of Math. (2)*, 133(3):447–475, 1991. ISSN 0003-486X. doi: 10.2307/2944316. URL http://dx.doi.org/10.2307/2944316.

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.

CHAPTER 4

Rational families of 17-torsion points of elliptic curves over number fields

RATIONAL FAMILIES OF 17-TORSION POINTS OF ELLIPTIC CURVES OVER NUMBER FIELDS

MAARTEN DERICKX, SHELDON KAMIENNY, AND BARRY MAZUR

This article will appear in a Memorial volume for Fumiyuki Momose. He was a generous warm human being, with immense energy and generosity of spirit, and an extremely gifted mathematician. One of his abiding interests was rational torsion on elliptic curves over number fields, as in [32], [24]. *This article is written in his memory.*

Contents

1. Introduction

Rational torsion points on elliptic curves present challenges that one can come back to again and again since the topic simply continues to be a source of extremely interesting diophantine issues. If E is an elliptic curve over a number field k, its Mordell–Weil group, $E(k)$, is finitely generated. Moreover, any finite subgroup of $E(k)$ is of the form $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ where N, m are positive integers with m dividing N. Ogg's Conjecture, proved thirty-five years ago, might be phrased as saying that there is no rational torsion on elliptic curves over $\mathbf{Q}$ except as directly forced by the underlying algebraic geometry. More specifically: any example of an elliptic curve over $\mathbf{Q}$ with its Mordell–Weil group containing a subgroup isomorphic to $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ is a member of a rationally parametrized family, in the sense that the modular curve $X(N, m)$ classifying such examples is isomorphic to $\mathbf{P}^1$.

In a paper published over two decades ago, written jointly with M. Kenku, Momose inaugurated an analogous investigation of certain types of subgroups of torsion points on elliptic curves rational over quadratic fields [24]. Kenku and Momose proved the following theorem:

Theorem 1. *(Kenku, Momose) For integers N that factor as a product of powers of prime numbers < 17, and for integers m dividing N the following statements are equivalent.*

(1) *There exists a quadratic field k and an elliptic curve E defined over k such that $E(k)$ contains a subgroup isomorphic to $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.*
(2) *The modular curve that classifies such torsion, $X(N, m)$, is rational or hyperelliptic.*

Following on this work, one of the authors of the present paper established general classification results for torsion in the Mordell–Weil group of elliptic curves over quadratic fields ([21], [23]; for a slightly different problem regarding torsion in elliptic curves and quadratic fields, see [26]).

Nowadays, one considers even more general questions from theoretical and computational perspectives.

- We might fix N and m and ask for a structural and numerical understanding of the collection of elliptic curves defined over fields of some fixed degree d over $\mathbf{Q}$—or over a fixed base number field k—for which its Mordell–Weil group over those fields contains a subgroup isomorphic to $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.
- Or more specifically, we might ask to classify rationally parametrized families of elliptic curves defined over number fields K_t of degree d over k and which possess N-torsion points rational over K_t[1]. In particular, we might study functions of degree d on $X_1(N)$ defined over $\mathbf{Q}$.

[1]The word "rational," then, is used in two senses: the parameter t ranges through the k-rational points of a rational curve (over k).

This paper will focus on the latter type of problem[2] as related to a diophantine analysis of appropriate Brill–Noether varieties attached to the modular curves $X_1(N)$.

A substantial amount of computation has been done. Intriguing examples have been discovered ([7], [14], [36], [15], [16]). In work in progress the authors of this paper will be treating a number of explicit examples related to modular Brill–Noether curves. The present expository article, focusing on 17-torsion—dedicated to the memory of Fumiyuki Momose—is a report on a piece of that work in progress.

We are thankful to Ken Ribet for very helpful comments regarding an early draft of this paper.

2. Rational N-torsion over fields of degree d

Fix two positive integers (N, d) and darken the point (N, d) in the plane if there exists a *non-CM elliptic curve*[3] defined over a number field of degree $\leq d$ having an N-torsion point rational over that field; call such points (N, d) simply: **data points**. One would like to know anything that stands out in this data set: its structure and its statistics.

There are two standard ways to look for uniformity phenomena:

- *Focusing, for example, on prime torsion, fix d and let $P(d)$ be the largest prime p such that (p, d) is in the data set.*

  Specific *exact values* of $P(d)$ are known only for small d. By [28] $P(1) = 7$. Kamienny proved that $P(2) = 13$; Parent, building on work of Kamienny, showed $P(3) = 13$. Recently, Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll [8] showed that $P(4) = 17$, $P(5) = 19$ and $P(6) = 37$.

  For general values of d we have the (trivially obtained) lower bound

  $$d^{1/2} \ll P(d)$$

  and the deep upper bounds given by Merel's Theorem tellling us that $P(d) < \infty$. More specifically, Merel [31] (and Oesterlé, Parent [34]) proved, for general d that

  $$P(d) \leq (1 + 3^{d/2})^2,$$

  so we have:

  $$d^{1/2} \ll P(d) \ll 3^d.$$

  We don't even seem yet able to come up with much more precise conjectures for the qualitative behavior and/or the volatility of $P(d)$. Is $P(d)$ bounded

[2] and even more specifically when the base field is $\mathbf{Q}$ and $N = 17$

[3] We're thankful to Andrew Sutherland who suggested that one might keep separate the study of examples of CM elliptic curves possessing rational points of order N over fields of low degree d, since they represent a very orderly collection of known examples where for each such CM-elliptic curve, d admits a linear upper bound in N—and this would simply muddle the essential data set.

by a constant times d^A for any $A > 1/2$? Or for *some* finite value of A? Or does it grow more rapidly than that?

Consider the 'minimalist' attitude that any *interesting* diophantine phenomenon occurs no more often than would be predicted by general structural constraints. This viewpoint seems to lead to firmly believed conjectures, for example, for statistics regarding ranks of Mordell–Weil groups. This general viewpoint might also suggest the guess that $P(d) \ll d^A$ for any $A > 1/2$. But we don't seem to have enough experience yet to give any firm conjectures[4].

- *Fix N and let $D(N)$ be the smallest integer d such that (N, d) is in the data set.*

In contrast to our knowledge of the asymptotics of $P(d)$, with $D(N)$ we are in slightly better shape. There is a clear *cut-off* for $D(N)$: namely, $D(N) \leq \gamma_{\mathbf{Q}}(N)$ where $\gamma_{\mathbf{Q}}(N)$ is the $\mathbf{Q}$-*gonality* of the modular curve $X_1(N)$. The basic $\mathbf{Q}$-parametrization $X_1(N) \to X(1) \simeq \mathbf{P}^1$ already gives us $\gamma_{\mathbf{Q}}(N) \leq \Phi(N)\Psi(N)/2$—where $\Phi(N)$ is the Euler phi function and

$$\Psi(N) = \Psi(\prod p_i^{e_i}) = \prod (p_i + 1) p_i^{e_i - 1}.$$

In particular, we have $\gamma_{\mathbf{Q}}(N) \ll N^2$. For a discussion of the concept of gonality, see [1], [7].

If $d = \gamma_{\mathbf{Q}}(N)$, or more generally if there exists an $f : X_1(N) \to \mathbf{P}^1$ of degree d, then not only are there elliptic curves over fields of degree d with rational N-torsion over those fields, but there are infinitely many of them parametrized by a subset of $\mathbf{P}^1(\mathbf{Q})$. See Abramovich's basic paper [1] where he proves the inequality

$$\frac{21}{200}(g-1) \leq \gamma_{\mathbf{C}}(N) \leq (g+3)/2,$$

where $\gamma_{\mathbf{C}}(N)$ is the $\mathbf{C}$-*gonality*, and $g \approx N^2$ is the *genus*, of $X_1(N)$. For more elementary reasons

$$\gamma_{\mathbf{C}}(N) \leq \gamma_{\mathbf{Q}}(N) \leq g + 1.$$

For the $\mathbf{Q}$-gonalities of the modular curves $X_1(N)$ with $N \leq 40$ see [7]. In particular

$N = p$	13	17	19	23	29	31	37
$\gamma_{\mathbf{Q}}(N)$	2	4	5	7	11	12	18

We will be considering data points (N, d) only for degrees $d \leq \gamma_{\mathbf{C}}(N)$. We will call an elliptic curve defined over a field of degree d possessing an N-torsion point

[4] Some conjectures in the literature give upper bounds for primes of torsion in elliptic curves of degree d, but since these published conjectures also include CM elliptic curves which our "$P(d)$" doesn't register, those conjectures necessarily must allow for an essentially linear lower bound. Specifically, see [6] and [27].

rational over that field **sporadic** if $d = \gamma_{\mathbf{C}}(N)$ and it is *not* a member of a $\mathbf{Q}$-rationally parametrized rational family of such elliptic curves defined over fields of degree d possessing N-torsion points rational over those fields. We call it **very sporadic** if $d < \gamma_{\mathbf{C}}(N)$.

Very sporadic data points exist. Here is a list of some known examples:

d	N	$\gamma_{\mathbf{C}}(N)$	*Reference*
3	21	4	[33]
9, 10	29	11	[14]
9, 10, 11	31	12	[7]

A result of Pete L. Clark, Brian Cook and James Stankewicz (which builds on the work of Dan Abramovich) [6] implies that for a prime $p \geq 5$ there are at most finitely many points on $X_1(p)$ with degree $< \frac{7}{3200}(p^2 - 1)$. Related to this, see [12].

3. Brill–Noether Varieties

Let X be a smooth projective curve over a characteristic zero field k. Let $\bar{k}/k$ be an algebraic closure, and $\bar{X} := X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\bar{k})$. For integers $d \geq 1$, $r \geq 0$, let

$$W^r_d(X) \subset \mathrm{Pic}^d(X)$$

denote the closed subvariety of $\mathrm{Pic}^d(X)$ (defined over k) classifying divisor classes of effective divisors D of degree d that are members of linear systems (of effective divisors of degree d) of dimension $\geq r$, or equivalently such that $h^0(X, \mathcal{O}(D)) \geq r+1$; see [4], [5], [9].

The collection of Brill–Noether varieties $\{W^r_d(X) \mid d \geq 0, r \geq 0\}$ connect in the following ways:

(1) For $r \geq 1$ we have natural inclusions $W^r_d(X) \hookrightarrow W^{r-1}_d(X) \subset \mathrm{Pic}^d(X)$.

(2) Let α be a k-rational point of X, and let

$$f_\alpha : \mathrm{Pic}^d(X) \to \mathrm{Pic}^{d-1}(X)$$

be the morphism that sends the class of a divisor D to the class of $D - [\alpha]$. For $r \geq 1$ we have a commutative diagram of k-rational maps,

$$\begin{array}{ccc} W^r_d(X) & \xrightarrow{\subset} & \mathrm{Pic}^d(X) \\ \downarrow{\scriptstyle f_\alpha} & & \downarrow{\scriptstyle f_\alpha} \\ W^{r-1}_{d-1} & \xrightarrow{\subset} & \mathrm{Pic}^{d-1}(X). \end{array}$$

Statement (2) above follows from considering the global sections of the exact sequence

$$0 \to \mathcal{O}_X(D - \alpha) \to \mathcal{O}_X(D) \to \mathcal{O}_\alpha \to 0.$$

(3) We have the natural surjection

$$\eta_d : \mathrm{Sym}^d(X) \twoheadrightarrow W_d^0(X) \subset \mathrm{Pic}^d(X). \tag{1}$$

which is an isomorphism when restricted to

$$\mathrm{Sym}^{d,\#}(X) := \eta_d^{-1}\big(W_d^0(X) - W_d^1(X)\big) \subset \mathrm{Sym}^d(X),$$

i.e., to the inverse image of the complement of $W_d^1(X)$:

$$\begin{array}{ccccc} \mathrm{Sym}^{d,\#}(X) & \xrightarrow{\subset} & \mathrm{Sym}^d(X) & & \\ \downarrow \cong & & \downarrow & & \\ W_d^0(X) - W_d^1(X) & \xrightarrow{\subset} & W_d^0(X) & \xrightarrow{\subset} & \mathrm{Pic}^d(X). \end{array}$$

In paticular $\mathrm{Sym}^d(X)$ is a desingularization of $W_d^0(X)$. In certain cases of interest (e.g., as in our analysis of $X = X_1(17)$ below) $\mathrm{Sym}^d(X)$ is a small resolution of the singularities of $W_d^0(X)$.

By Theorem (1.1) in Chapter V of [4] if the genus $g > 1$ of X is in the range

$$d - 1 \leq g \leq 2(d-1),$$

the Brill–Noether variety $W_d^1(X)$ is of dimension greater than or equal to $2(d-1)-g$. So, if it satisfies these conditions it can be a curve only if $2d \leq g + 3$ and a surface only if $2d \leq g + 4$.

We will be specifically interested in the cases $r = 0, 1$:

$$W_d^1(X) \subset W_d^0(X) \subset \mathrm{Pic}^d(X),$$

noting that a choice of k-rational point α of X will give us a (k-rational) closed immersion

$$W_d^1(X) \quad \overset{f_\alpha}{\hookrightarrow} \quad W_{d-1}^0(X) \subset \mathrm{Pic}^{d-1}(X).$$

Note: If X is a curve over k a number field, for any d, one has—applying a more general theorem of Faltings [11]—that the set of k-rational points of $W_d^1(X)$ decomposes into a *finite* union,

$$W_d^1(X)(k) \quad = \quad \bigsqcup_j \mathcal{A}_j, \tag{2}$$

where, for each j, the Zariski closure of $\mathcal{A}_j$ is a translate of an abelian subvariety of $Pic^0(X)$. For a study of upper bounds for the dimension of such abelian subvarieties that may arise for given values of d, gonality, and genus, see [2].

3.1. **The canonical involution v.** An important case for us is when $d = g-1 \geq 0$ where g is the genus of X. In this situation we have the natural involution

$$\mathrm{Pic}^{g-1}(X) \quad \overset{v}{\cong} \quad \mathrm{Pic}^{g-1}(X)$$

defined by sending any linear equivalence class of divisors $[D]$ of degree $g-1$ to the linear equivalence class of $[K-D]$ where K is the canonical divisor of X. The involution v is 'functorially defined' and is defined over any field k over which the curve itself is defined, and commutes with any automorphism of X.

Consider the fixed locus $\mathrm{Th}(X) \subset \mathrm{Pic}^{g-1}(X)$ of the involution v. The 2^{2g} geometric points of $\mathrm{Th}(X)$ are classically referred to as theta-characteristics of X; they correspond to 'square roots' of the canonical line bundle. The finite subscheme $\mathrm{Th}(X) \subset \mathrm{Pic}^{g-1}(X)$ is a torsor over $\mathrm{Pic}^0(X)[2]$. Note that the Riemann-Roch Theorem guarantees that

$$h^0(X, \mathcal{O}(D)) = h^0(X, \mathcal{O}(K-D)), \tag{3}$$

so v induces an involution of $W^r_{g-1}(X)$ for any $r \geq 0$. Consider the theta divisor

$$\Theta := W^0_d(X) = W^0_{g-1}(X) \subset \mathrm{Pic}^{g-1}(X),$$

noting that choosing any theta-characteristic $\partial \in \mathrm{Th}(X) \subset \mathrm{Pic}^{g-1}(X)$ gives the commutative diagram

$$\begin{array}{ccccc}
\Theta & \xrightarrow{v} & \Theta & \xrightarrow{\subset} & \mathrm{Pic}^{g-1}(X) \\
\downarrow{\scriptstyle -\partial} & & \downarrow{\scriptstyle -\partial} & & \downarrow{\scriptstyle -\partial} \\
\Theta - \partial & \xrightarrow{-1} & \Theta - \partial & \xrightarrow{\subset} & \mathrm{Pic}^0(X),
\end{array}$$

the theta divisors, $\{\Theta - \partial \quad \subset \quad \mathrm{Pic}^0(X)\}$ for the theta-characteristics ∂ ranging through $\mathrm{Th}(X)(\bar{k})$ being—each of them—symmetric under multiplication by -1 in $\mathrm{Pic}^0(X)$ and the set of them being a torsor under the group $\mathrm{Pic}^0(X)[2]((\bar{k}))$.

Note, as well, that $W^1_{g-1}(X) \subset \Theta$ is stable under the involution v as can be seen from (3).

3.2. **Basic Brill–Noether varieties.** For X a curve defined over k, denote by $\gamma = \gamma_{\bar{k}}$, its $\bar{k}$-gonality. Call $WX := W^1_\gamma(X)$ the **Basic Brill–Noether variety** attached to X. Given a k-rational point α of X, we obtain an immersion

$$WX = W^1_\gamma(X) \quad \overset{f_\alpha}{\hookrightarrow} \quad W^0_{\gamma-1}(X) = \mathrm{Sym}^{\gamma-1}(X) \subset \mathrm{Pic}^{\gamma-1}(X).$$

3.3. **The Basic Brill–Noether variety attached to $X_1(N)$.** Consider the basic Brill–Noether variety $WX_1(N) := W(X_1(N))$. Thanks to the functorial nature of Brill–Noether varieties, the automorphism group of $X_1(N)$ viewed as finite group scheme over $\mathbf{Q}$ acts naturally on $WX_1(N)$. Thus we have the group Δ of diamond

operators acting $\mathbf{Q}$-rationally on $WX_1(N)$, and the w-operators acting $\mathbf{Q}(\mu_N)^+$-rationally. When N is a prime number all these operators fit into a dihedral group that act $\mathbf{Q}(\mu_N)^+$-rationally on $WX_1(N)$.

3.4. **Basic Brill–Noether curves attached to algebraic curves of genus** 5 **and gonality** 4. *Assume from now on that X is a curve defined over $\mathbf{Q}$ of genus* 5 *and has $\mathbf{Q}$-gonality equal to $\mathbf{C}$-gonality $\gamma = 4$.*[5]

In this case the Basic Brill–Noether variety, $W := WX$, is a curve defined over $\mathbf{Q}$ (possibly reducible). We'll refer to it as the the Basic Brill–Noether curve attached to X. An application of Clifford's Theorem[6] guarantees that $h^0(X, \mathcal{O}_X(D)) \leq 2$ for any effective divisor D of degree 4, so $W_4^2(X)$ is empty. That is, the complete linear series that corresponds to any point in the Basic Brill–Noether curve attached to X is parametrized by a pencil.

A k-rational point of WX gives us a k-linear parametrization class of maps $X \to \mathbf{P}^1$ of degree $\gamma_{\bar{k}}(X)$, and conversely. So we have

Proposition 1. *Let* $\mathrm{Aut}(X)$ *denote the group of k-rational automorphisms of X. There is a one-to-one correspondence between k-similarity classes*[7] *of maps $X \to \mathbf{P}^1$ (defined over k) of degree $\gamma_{\bar{k}}(X)$ and* $\mathrm{Aut}(X)$*-orbits of k-rational points of the Basic Brill–Noether curve WX:*

$$k\text{-similarity classes} \quad \leftrightarrow \quad WX(k)/\mathrm{Aut}(X).$$

If $d < \gamma_k(X)$ then $W_d^1(X)$ is empty. In the special case where $\gamma_{\bar{k}}(X) = g - 1$ we are in the situation of section 3.1 above, and we have the canonical involution v acting on $W(X)$ compatibly with its action on $\mathrm{Pic}^{g-1}(X)$ giving a commutative diagram:

$$\begin{array}{ccc} W(X) & \xrightarrow{v} & W(X) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^{g-1}(X) & \xrightarrow{v} & \mathrm{Pic}^{g-1}(X) \end{array}$$

which commutes with any automorphism of X.

Consider a canonical embedding (defined over $\mathbf{Q}$)

$$\beta : X \xrightarrow{\cong} \Gamma \subset \mathbf{P}^4.$$

[5] The example we treat, $X_1(17)$, is of this form, as are $X_1(21)$, and $X_1(24)$.

[6] See page 204 of [4] for a discussion that covers the case of interest to us: genus =5, gonality and degree =4.

[7] *k-similarity* is the natural notion of equivalence for k-parametrizations: two parametrizations are **k-similar** if one can be brought to the other by composition with appropriate k-isomorphisms of domain and range.

Since the genus of X is $g = 5$, by a theorem of Max Noether [4] the curve Γ lies on $3 = (g-2)(g-3)/2$ independent quadrics in $\mathbf{P}^4$.

For ease of nomenclature in this discussion (i.e., for the rest of this section) let us strictly reserve the symbols $\mathbf{P}^4$ to mean the projective 4-dimensional space which is the ambient space of the canonical embedding above, and $\mathbf{P}^2$ to mean the projective space generated by the linear space of *those* three independent quadrics just mentioned.

In the case of our interest we will be fixing bases,

$$\omega_0, \omega_1, \omega_2, \omega_3, \omega_4$$

of the 5 dimensional space $S := H^0(X, \Omega^1(X))$ such that the projectivization of $S^\vee$ is the $\mathbf{P}^4$ above. In terms of this basis we will be stipulating three independent quadratic relations

$$\begin{aligned} e_0 &:= e_0(\omega_0, \dots, \omega_4) \\ e_1 &:= e_1(\omega_0, \dots, \omega_4) \\ e_2 &:= e_2(\omega_0, \dots, \omega_4), \end{aligned}$$

generating the kernel of the natural cup product map

$$(*) \qquad \mathrm{Sym}^2(S) \xrightarrow{\kappa} H^0(X, (\Omega^1(X)^{\otimes 2}),$$

and therefore representing a basis of the projective space $\mathbf{P}^2$ above.

Note that $S = H^0(X, \Omega^1(X))$ and $H^0(X, (\Omega^1(X)^{\otimes 2})$ have a natural action of $\mathrm{Aut}(X)$ with respect to which the morphism $(*)$ is equivariant.

In the cases of our particular interest S will be the space of cuspforms of weight two and the cup product above will be given by multiplication to the space of cuspforms of weight four.

3.5. **Loci of singular quadrics.** For the results we are now about to quote, see page 207 of [4].

- Let $\mathcal{V} \subset \mathbf{P}^2$ be the sub-locus of singular quadrics[8] $\mathcal{Q} \subset \mathbf{P}^4$.
- Let $\mathcal{W} \to \mathcal{V}$ be the double cover determined by choosing one of the two systems of planes in these singular quadrics.
- Let

$$\mathcal{G} \overset{\mathrm{proj}}{\to} \mathcal{W}$$

[8] Recall that the 'generic' singular quadric threefold $\mathcal{Q} \subset \mathbf{P}^4$ has a unique singular point ϵ and is the cone 'at ϵ' of a (nonsingular) quadric surface given by the intersection of $\mathcal{Q}$ with any hyperplane not passing through ϵ. That quadric surface has two rulings by lines (possibly not rational over the base field k). Taking the cone through ϵ of each of these rulings gives us two 2-dimensional rulings, now, of the quadric threefold $\mathcal{Q}$ (again possibly not rational over the base field k). That is, $\mathcal{Q}$ is swept out by two pencils of planes (i.e., 2-dimensional projective linear subspaces).

be the $\mathbf{P}^1$-bundle whose points consist of pairs $(\Pi, \mathcal{Q})$ where $\mathcal{Q} \in \mathcal{V}$ and $\Pi \subset \mathcal{Q}$ is a two-plane.

- Let $v : \mathcal{W} \to \mathcal{W}$ be the involution defining the covering $\mathcal{W} \to \mathcal{V}$.
- Consider the commutative diagram

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\alpha} & \mathrm{Sym}^4(X) \\ \Big\downarrow{\scriptstyle \mathrm{proj}} & & \Big\downarrow{\scriptstyle \mathrm{proj}} \\ \mathcal{W} & \xrightarrow{\alpha} & \mathrm{Pic}^4(X) \end{array}$$

where the morphism $\alpha : \mathcal{G} \to \mathrm{Sym}^4(X)$ is characterized on points by the rule that sends $(\Pi, \mathcal{Q})$ of $\mathcal{G}$ to the divisor (of degree four),

$$\alpha(\Pi, \mathcal{Q}) := \Pi \cap \Gamma \subset \Gamma,$$

the latter being construed, via the isomorphism $\beta : X \longrightarrow \Gamma$ of subsection 3.4, as an element of $\mathrm{Sym}^4(X)$. The image of α restricted to a fiber of $\mathcal{G} \overset{\mathrm{proj}}{\to} \mathcal{W}$ runs through a complete linear system of divisors, and therefore determines a well-defined point of $\mathrm{Pic}^4(X)$, providing a characterization (on points) of the morphism $\alpha : \mathcal{W} \to \mathrm{Pic}^4(X)$.

If ever we need to specify the curve X to which these objects are related, we indicate this in the standard manner; e.g., we write $\mathcal{W} = \mathcal{W}X, \quad \mathcal{V} = \mathcal{V}X, \quad \mathcal{G} = \mathcal{G}X$ etc.

3.6. **The canonical representation of the Basic Brill–Noether curve.** Let X be a curve satisfying our running hypotheses in this section, and put $W := WX$, the *Basic Brill–Noether curve* attached to X. Recall the involution $v : W \to W$ constructed in subsection 3.2. Let $\mathcal{W} = \mathcal{W}X$ be as in subsection 3.5 above, recalling the involution $v : \mathcal{W} \to \mathcal{W}$ constructed there.

The discussion of pp. 207-210 of of [4] gives the following identification.

Proposition 2. *The image of the canonical morphism $\alpha : \mathcal{W} \to \mathrm{Pic}^4(X)$ is contained in $W \subset \mathrm{Pic}^4(X)$ and induces an isomorphism, $\alpha : \mathcal{W} \xrightarrow{\cong} W$ commuting with the involutions v on domain and image. That is, letting $V := W/\{v\}$, we have the commutative diagram:*

$$\begin{array}{ccc} \mathcal{W} & \xrightarrow{\cong} & W \\ \Big\downarrow & & \Big\downarrow \\ \mathcal{V} & \xrightarrow{\cong} & V \end{array}$$

3.7. **Elliptic components and new components.** Let X be a ("bi-elliptic") curve defined over $\mathbf{Q}$ satisfying our running hypotheses in this section and let $W := WX$ be—as usual—the Basic Brill–Noether curve attached to X. By an *elliptic*

involution of X let us mean an involution $\iota : X \to X$ such that the quotient of X under its action,

$$\mathrm{proj}_\iota : X \to X/\{\sim \iota\} = \mathcal{E},$$

is a curve of genus one. The involution ι induces an action on W and on the constructions of Subsections 3.5 and 3.6. In particular ι commutes with the double cover mapping:

$$\begin{array}{ccc} W & \xrightarrow{\iota} & W \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v} \\ V & \xrightarrow{\iota} & V \end{array}$$

For any such quotient, and any point $u \in \mathcal{E}$ let $j_u : \mathcal{E} \to \mathcal{E}$ denote the canonical (nontrivial) involution fixing the point u, and let

$$\mathrm{proj}_{j_u} : \mathcal{E} \to \mathcal{E}/\{\sim j_u\} =: \mathbf{P}^1_u$$

denote the projection to the (genus zero) quotient (which we denote $\mathbf{P}^1_u$) under the action of j_u. Denote by t_u the running parameter in the projective line $\mathbf{P}^1_u$. For any pair (u, t_u) with $u \in \mathcal{E}$ and $t_u \in \mathbf{P}^1_u$ let $D_\iota(u, t_u) \subset \mathrm{Symm}^4(X)$ be the effective divisor of degree four on X given by

$$D_\iota(u, t_u) := \mathrm{proj}_\iota^{-1} \circ \mathrm{proj}_{j_u}^{-1}(t_u).$$

For each $u \in \mathcal{E}$, then, we have a linear system of divisors of degree four on X parametrized by the variable t_u, giving us a point on W, which we denote $w_\iota(u)$.

The morphism

$$w_\iota : \mathcal{E} \longrightarrow W$$

factors through the quotient $\mathcal{E}'$ of $\mathcal{E}$ under the natural action of the 2-torsion subgroup of its jacobian, i.e., $\mathrm{Pic}^0\big(\mathcal{E}\big)[2]$. The induced morphism

$$w'_\iota : \mathcal{E}' \hookrightarrow W$$

is a closed immersion, and its image is a (reduced) irreducible component of W defined over the field k. We denote this component $W_\iota \subset W$ and refer to $W_\iota \approx \mathcal{E}'$ as the **k-elliptic component of W associated to ι**. It is fixed by the action of the involution ι on W.

By a **new component** of W we will mean an irreducible component that is not elliptic in the above sense.

4. Fine Siegel units and fine Siegel points

Let $X := X_1(N)$. A **Fine Siegel unit** on X is a rational function f on X defined over $\bar{\mathbf{Q}}$ whose divisor of zeroes and poles consist only of $\mathbf{Q}$-rational cusps. Let $C(N)$ denote the set of $\mathbf{Q}$-rational cusps; so a fine Siegel unit is a unit in the ring of regular functions on $X_1(N) - C(N)$ (over $\bar{\mathbf{Q}}$). Since the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ preserves the divisor of zeroes-and-poles of a fine Siegel unit, an application of Hilbert's Theorem

90 guarantees that we may normalize our fine Siegel units (by multiplication by an appropriate nonzero scalar) so that they are defined over $\mathbf{Q}$. Such a normalized Siegel unit f is well-defined by its divisor of zeroes-and-poles up to a factor in $\mathbf{Q}^*$ and gives us a $\mathbf{Q}$-rational parametrization $f : X \to \mathbf{P}^1$. Let $\mathcal{Z}(N)$ denote the group of fine Siegel units modulo $\mathbf{Q}^*$. By the Manin–Drinfeld Theorem, $\mathcal{Z}(N)$ is a free abelian group of rank $|C(N)| - 1$. The action of the group Δ of diamond operators on $X_1(N)$ induces an action on $\mathcal{Z}(N)$ and there is a natural metric on $\mathcal{Z}(N)$ given by the geometric degree of the function $f : X_1(N) \to \mathbf{P}^1$. This metric satisfies a triangle inequality:

$$\deg(f \cdot g) \leq \deg(f) + \deg(g),$$

and it scales well, i.e.,

$$\deg(f^n) = |n| \cdot \deg(f)$$

for $n \in \mathbf{Z}$, and is preserved by the action of the diamond operators. See [37] for an explicit description of the fine Siegel units in terms of their q-expansions and their expression in relation to specific modular forms.

The following two conditions on $X := X_1(N)$ hold for only a (finite) number of values of N but they do hold for the case $N = 17$.

(1) $X = X_1(N)$ contains no very sporadic points (in the terminology of Section 2) *except for the set of* $\mathbf{Q}$*-rational cusps* $C(N)$.
(2) $\gamma_{\mathbf{C}}(X) < |C(N)|$.

When $N = 17$ these conditions are indeed met[9].

Proposition 3. $X_1(17)$ *has no non-cuspidal very sporadic points.*

Proof: There are no non-cuspidal points on $X_1(17)$ of degree 1 by [28]; none of degree 2 by [19]; and none of degree 3 by [34].

As we shall see (Proposition 6) $X_1(17)$ contains no non-cuspidal sporadic points, as well.

Under hypothesis **(1)** above, every function $\phi : X_1(N) \to \mathbf{P}^1$ of degree $\gamma_{\mathbf{C}}(X)$ and defined over $\mathbf{Q}$ has the property that any of its fibers above points in $\mathbf{P}^1(\mathbf{Q})$ either consists entirely of $\mathbf{Q}$-rational cusps, or contains no $\mathbf{Q}$-rational cusps at all. This is because each fiber is of degree $\gamma_{\mathbf{C}}(X)$ and if it contains a $\mathbf{Q}$-rational cusp, the points of the fiber are all of degree strictly less than $\gamma_{\mathbf{C}}(X)$. That is, these points are all very sporadic, so by **(1)** they are *all* rational cusps. If a fiber of such a ϕ consists entirely of rational cusps, call it a **rational-cuspidal-fiber** of ϕ. By **(2)**, ϕ has at least two rational-cuspidal-fibers. Choosing two rational-cuspidal-fibers of such a $\phi : X \to \mathbf{P}^1$ and composing ϕ with an appropriate linear fractional transformation of $\mathbf{P}^1$ that sends the image of one of those fibers to 0 and the other to ∞ we see that any such ϕ is in the $\mathbf{Q}$-similarity class of a $\mathbf{Q}$-parametrization of $X_1(N)$ by a fine Siegel unit f (of geometric degree equal to the gonality of X).

[9] As has been verified by the first author of this article and Mark van Hoeij, these two conditions are satisfied for $X_1(N)$ for $N = 32$, and for $N < 28$ but not $N = 21$.

There is a natural way of denoting such a fine Siegel unit f up to the equivalence relation defined by deeming two such Siegel units equivalent if one can be obtained from the other by composition by an appropriate $\mathbf{Q}$-automorphism $b : \mathbf{P}^1 \to \mathbf{P}^1$. Namely, one simply lists the rational-cuspidal-fibers of f giving the divisors with support on cusps that constitutes each of those fibers.

Each divisor with support on the cusps is encoded by $|C(N)|$ integers, where the i-th integer is the multiplicity of the i-th cusp. We display this data for a given f as a matrix, with exactly $|C(N)|$ columns, and as many rows as there are rational-cuspidal-fibers for f. We call it the **rational-cuspidal-fiber matrix** for the $\mathbf{Q}$-linear parametrization class of f.

We also organize these cuspidal-fiber matrices in Δ-orbits. Any such Δ-orbit determines a $\mathbf{Q}$-similarity class of $\mathbf{Q}$-parametrizations of $X_1(N)$ of geometric degree equal to the gonality of X.

Under both hypotheses above, any such f has at least two rational-cuspidal-fibers ($|C(N)| > \gamma_{\mathbf{C}}(X)$ implies that there are at least two fibers containing $\mathbf{Q}$-rational cusps). We can compose f with an appropriate $b : \mathbf{P}^1 \to \mathbf{P}^1$ sending one rational-cuspidal-fiber to 0 and another to ∞, so that $b \circ f$ is a fine Siegel unit.

Consequently

Proposition 4. *Under the hypotheses* **(1)** *and* **(2)** *above*

(1) *Any* $\mathbf{Q}$*-parametrization of* $X = X_1(N)$ *of geometric degree* $\gamma_{\mathbf{C}}(X)$ *is represented by at least one fine Siegel unit in* $\mathcal{Z} = \mathcal{Z}(N)$ *of degree* $\gamma_{\mathbf{C}}(X)$.
(2) *There are only finitely many classes of* $\mathbf{Q}$*-parametrizations of* $X_1(N)$ *of degree* $\gamma_{\mathbf{C}}(X)$.

Definition 1. *By a* **fine Siegel point** *on the Basic Brill–Noether variety* $WX_1(N)$ *let us mean a* $\mathbf{Q}$*-rational point on* $WX_1(N)$ *represented by a linear system parametrized by a fine Siegel unit.*

Corollary 2. *Under the hypotheses* **(1)** *and* **(2)** *above, the Basic Brill–Noether variety* $WX_1(N)$ *has only finitely many* $\mathbf{Q}$*-rational points. These are all fine Siegel points and are effectively obtainable.*[10].

The first statement in Corollary 2 follows from Proposition 4 simply by considering the number of pairs of possible cuspidal-fibers. Effectivity follows because there are effective methods to compute Riemann-Roch spaces of divisors on curves (cf. [13]). The computations of cuspidal-fiber matrices can be done for some small values of N (including $N = 17$) by a combination of modular symbol computations implemented by Sage ([3, p. 57]) and brute force computations.

[10]The same proof gives a similar finiteness and effectivity result for the set of $\mathbf{Q}$-rational points of the Basic Brill–Noether variety WX of *any* curve X defined over $\mathbf{Q}$ that has the property that all its very sporadic points are $\mathbf{Q}$- rational and $|X(\mathbf{Q})|$ is strictly greater than $\gamma_{\mathbf{Q}}(X)$.

When $N = 17$ we shall see that all $\mathbf{Q}$-rational points of $WX_1(N)$ are fine Siegel points. It would be interesting to understand, for more general values of N what portion of $WX_1(N)(\mathbf{Q})$ comes from Siegel (or fine) Siegel points.

A computation of Derickx and van Hoeij [7] guarantees that for all $N \leq 40$ there is at least one modular unit of degree equal to the $\mathbf{Q}$-gonality of $X_1(N)$. It follows that if, for these values of N, the $\mathbf{Q}$-gonality were equal to the $\mathbf{C}$-gonality of $X_1(N)$, the corresponding Basic Brill–Noether variety $WX_1(N)$ would contain at least one Siegel point.

5. Families of 17-torsion

The curve $X = X_1(17)$ is of genus 5 with $\mathbf{Q}$-gonality and $\mathbf{C}$-gonality both equal to 4. The basic Brill–Noether variety $WX_1(17)$ is a curve.

The curve $X_1(17)$ has no non-cuspidal very sporadic points (Proposition 3) and no non-cuspidal sporadic points (Proposition 6). Andrew Sutherland has computed elegant equations for these modular curves in [36]. The equation for $X_1(17)$ is particularly crisp[11]:

There is a birational morphism (over $\mathbf{Q}$) of $X_1(17)$ onto the bi-projective curve of bi-degree $(4, 4)$ in $\mathbf{P}^1 \times \mathbf{P}^1$ cut out by the polynomial

$$(*) \quad x^4y - x^3y^3 - x^3y + x^2y^4 + x^2y - x^2 - xy^4 + xy^3 - xy^2 + xy + y^3 - 2y^2 + y = 0,$$

This morphism is an embedding when restricted to the complement of the cusps, $Y_1(17) \subset X_1(17)$ into $\mathbf{P}^1 \times \mathbf{P}^1$. Projection to the first factor is given by the modular unit[12] $x := E_5E_6/E_1E_3$ and the projection to the second factor is given by the modular unit $y := E_6E_7/E_2E_8$. Both x and y are functions of degree 4 and in fact there is another function of degree 4, namely:

$$z = \frac{y(x^2 - yx + y - 1)}{(y-1)^2x}.$$

An example of the type of result that we prove (based, of course, on the results already mentioned) is the following:

Theorem 3. *Any elliptic curve defined over a field of degree ≤ 4 possessing points of order 17 defined over that field can be obtained by applying a diamond operator to a point of $X_1(17)$ for which one of the functions x, y takes on a rational value $\neq 0, 1$ or z takes a value $\neq 0$. Conversely, setting x, y to a rational value $\neq 0, 1$ or z to a value $\neq 0$ defines an elliptic curve over a field of degree four with a rational 17-torsion point.*

[11] As we understand it, this equation was originally written down by Cady and Elkies; see also a closely related description of $X_1(17)$ in [16].

[12] Here we are using the notation of Yang [37], following Kubert-Lang [25].

Moreover, the rational parameters x, y, z give, up to **Q***-similarity*[13] *all* **Q***-rational parametrizations of $X_1(17)$ of degree equal to its gonality (i.e., degree = 4). The Galois group of the finite extension*

$$\mathbf{Q}(x) \subset \mathbf{Q}(X_1(17))$$

is the full symmetric group[14] *S_4 while the finite mappings*

$$y, z : X_1(17) \to \mathbf{P}^1$$

factor through the bi-elliptic representation

$$X_1(17) \longrightarrow X_1(17)/\{\text{action of } \langle 13\rangle\} = X_1(17)/\{\text{action of } \langle 3\rangle^4\}$$

and their Galois group is the dihedral group D_4.

The functions x, y, z of the theorem are in the equivalence classes of **Q**-parametrizations of type $(\mathbf{C}), (\mathbf{A}), (\mathbf{B})$ described in subsection 5.2 below.

The fun here is that there are, in fact, two distinct ways of getting at the diophantine problem involved, as discussed above. They dovetail in a nice way. We can approach the problem either by considering:

- **Q**-rational points on the Basic Brill–Noether modular curve WX,

or

- rational cuspidal divisors and "fine" Siegel units.

5.1. **Via the Basic Brill–Noether modular curve.** We have computed the Basic Brill–Noether modular curve $W := WX_1(17)$ to be a double cover of a plane quintic (reducible) curve

$$(*) \quad V: \quad X \cdot (X^4 - 3X^2Y^2 - 3X^2Z^2 + Y^4 + 2Y^3Z + 3Y^2Z^2 - 2YZ^3 + Z^4) = 0.$$

The involution v of W that is the automorphism of the double cover $W \to V$ (the identity on V) has three descriptions. First, it is given by the diamond operator involution $\langle 13\rangle = \langle 3\rangle^4$. Secondly, it is also the involution induced on W (via the Serre duality theorem) from the transformation of divisors of degree four $D \mapsto K - D$ where K is the canonical divisor (of degree 8) on $X_1(17)$. The third description comes from what one might call the *canonical representation* of $W \to V$ as described in some generality in Subsections 3.5 and 3.6 above.

The group, Δ, of **Q**-automorphisms of X is canonically isomorphic to $(\mathbf{Z}/17\mathbf{Z})^*/\{\pm 1\}$. The operator $\langle 3\rangle \in \Delta$ is a generator.

Let $S_k := S_k(\Gamma_1(17))$ denote the **Q**-vector space of cuspforms of weight k on $\Gamma_1(17)$). Since the genus of $X_1(17)$ is 5 we have $\dim S_2 = 5$. The characteristic

[13] Recall the definition in Proposition 1: two parametrizations are **Q-similar** if one can be brought to the other by composition with appropriate **Q**-isomorphisms of domain and range.

[14] Hilbert's Irreducibility theorem would then guarantee infinitely many specializations $x \mapsto a \in \mathbf{Q}^*$ give a quartic polynomial in $\mathbf{Q}[y]$ with full symmetric Galois group.

polynomial of $\langle 3\rangle$ acting on S_2 is $(x-1)(x^4+1)$, this means that there is a basis $\omega_0,\ldots,\omega_4 \in S_2$ such that with respect to this basis we have:

$$\langle 3\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

One such basis is given by

$$\omega_0 := q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 + O(q^9) \tag{4}$$
$$\omega_1 := q - q^2 - q^3 + q^6 - q^7 + q^8 + O(q^9) \tag{5}$$
$$\omega_2 := q^2 - q^3 - 2q^4 + q^5 + q^6 + q^7 + O(q^9) \tag{6}$$
$$\omega_3 := -q^2 + q^3 + q^4 + q^5 - q^6 - q^7 - q^8 + O(q^9) \tag{7}$$
$$\omega_4 := q^3 - 2q^4 + q^6 - q^7 + 3q^8 + O(q^9) \tag{8}$$

Every nonzero element in $\mathrm{Sym}^2(S_2)$ defines a quadratic form in the ω_i and and hence a quadric in $\mathbf{P}^4$. Now let $Y \subseteq \mathrm{Sym}^2(S_2)$ be the kernel of the natural map:

$$\mathrm{Sym}^2(S_2) \to S_4$$

Then Y will be a 3-dimensional space with basis e_0, e_1, e_2 given by

$$e_0 := \omega_0^2 - \omega_1^2 - \omega_2^2 - \omega_3^2 - \omega_4^2 \tag{9}$$
$$e_1 := 2\omega_1\omega_2 + 2\omega_1\omega_3 - 2\omega_3\omega_4 \tag{10}$$
$$e_2 := 2\omega_2\omega_3 + 2\omega_1\omega_4 + 2\omega_2\omega_4 \tag{11}$$

The matrix of $\langle 3\rangle$ acting on Y with respect to this basis is:

$$\langle 3\rangle = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

Let (a_0, a_1, a_2) be coordinates of Y with respect to the basis e_0, e_1, e_2. Now consider the locus $V \subset \mathbf{P}^2 = \mathbf{P}(Y)$ corresponding to the singular quadrics in $\mathbf{P}^4$. This locus will be given by the single homogenous equation of degree 5, **(*)** above.

Each of these singular quadrics has (generally) two rulings by planes, and each of these planes intersect the canonically embedded curve X in an (effective, of course) divisor of degree 4. Each ruling, then, gives a unique linear system of effective divisors of degree 4 on X. That is, we can identify the Basic Brill–Noether curve W with the locus of rulings on these singular quadrics. The involution v simply switches rulings on the same singular quadric.

The plane quintic V breaks up into the union of a line

$$V_0 : \quad X = 0$$

and a plane quartic

$$V_1: \quad X^4 - 3X^2Y^2 - 3X^2Z^2 + Y^4 + 2Y^3Z + 3Y^2Z^2 - 2YZ^3 + Z^4 = 0$$

and $W = W_0 \cup W_1$ is a union of two irreducible components where W_0 (a double cover of V_0) is an elliptic curve of Cremona type 17a4.

The curve of genus one, W_0 is directly related to the bi-elliptic representation of $X_1(17)$. It has four rational points, two of which yield parameterizations in the $\mathbf{Q}$-similarity class of the function y and the other two yield parameterizations in the class of z.

The more interesting component W_1 is given (birationally) as a double cover of V_1 given by extracting a "square root" of the function

$$(2Y^2Z + 2XY^2 + XZ^2 - X^3)/X^3$$

on V_1.

Much of the internal structure of the Basic Brill–Noether curve W is directly related to the bi-elliptic representation of $X_1(17)$ mentioned above, so let us return to it with a bit more detail. The diamond operators of $X_1(17)$ acting functorially on W preserve the irreducible component W_1 and we have the following curiously similar sequences of double covers:

- Consider the sequence of double covers:[15]

$$\begin{array}{ccccc} X & \longrightarrow & X/(\langle 3\rangle^4) & \longrightarrow & X/(\langle 3\rangle^2) & \longrightarrow & X/(\langle 3\rangle) \\ & & \downarrow \approx & & \downarrow \approx & & \downarrow = \\ & & 17a4 & \longrightarrow & 17a2 & \longrightarrow & X_0(17) \end{array}$$

  We easily compute that $X/(\langle 3\rangle^4), X/(\langle 3\rangle^2)$ and $X/(\langle 3\rangle)$ are curves of genus 1, and the automorphism $\langle 3\rangle$ acts freely on them of order $4, 2$ and 1 respectively. In particular, the action of $\langle 3\rangle$ on $X/(\langle 3\rangle^4)$ can be understood as the action of translation by a ($\mathbf{Q}$-rational) point $\mathcal{P}$ of order 4 in the jacobian, $\mathcal{J} := \mathrm{Pic}^0(X/(\langle 3\rangle^4))$. This pins things down, after consulting Cremona's tables, forcing (the jacobian of) $X/(\langle 3\rangle^4)$ to be $17a4$ (which is the only curve of conductor 17 that has a rational 4-torsion point, the quotient by which is isomorphic to $X_0(17)$) and forcing (the jacobian of) $X/(\langle 3\rangle^2)$ to then be 17a2.

  It is an exercise to see, with no computation at all, that W_0 can be canonically identified as the curve of genus one given as the quotient of the curve $X/(\langle 3\rangle^4)$ by the natural action of the 2-torsion subgroup of its jacobian. It follows then that W_0 is isomorphic to 17a4, and therefore has exactly four

[15] We use Cremona's classification to refer to some of the elliptic curves that occur in these computations.

rational points. These four points break up into two orbits under the action of the 'diamond operators' Δ contributing to two $\mathbf{Q}$-similarity classes represented by the functions "y" and "z" of our theorem.

- The curve W_1 is a curve of genus 7, but is also directly related to 17a4 and neatly mimics the sequence displayed in the previous bullet as follows. Consider the diamond operators acting on W_1 which can be computed to produce the sequence of double covers:

$$\begin{array}{ccccccc} W_1 & \twoheadrightarrow & W_1/(\langle 3\rangle^4) & \twoheadrightarrow & W_1/(\langle 3\rangle^2) & \twoheadrightarrow & W_1/(\langle 3\rangle) & \twoheadrightarrow & X_0(17) \\ & & \downarrow = & & \downarrow \approx & & \downarrow \approx & & \downarrow = \\ & & V_1 & \longrightarrow & 17a4 & \longrightarrow & 17a2 & \longrightarrow & X_0(17) \end{array}$$

The curve V_1 has exactly four $\mathbf{Q}$-rational points: $(1, \pm 1, \pm 1)$ and the eight points in W_1 comprising the inverse image of those four points are all $\mathbf{Q}$-rational, and therefore give the full set of $\mathbf{Q}$-rational points of W_1. These eight point comprise a single Δ-orbit. Therefore they give rise to a unique $\mathbf{Q}$-similarity class of rational parametrizations of $X_1(17)$, for which the function "x" of the theorem is a representative.

5.2. **Via Fine Siegel Units.** As is clear from the account already given, to compute the rational points on the Basic Brill–Noether curve $WX_1(17)$ is not greatly difficult since each of its connected components is a perfectly specified finite cover of an elliptic curve possessing only four rational points. Section 4 above offers an utterly independent way of making this computation: by Proposition 3 the only very sporadic points on $X_1(17)$ are the eight rational cusps, and therefore any $\mathbf{Q}$-rational function ϕ of degree 4 on $X_1(17)$ has the curious property, as discussed in section 4 that

- any of its fibers that contain even a single rational cusp must consist entirely of rational cusps—call such a fiber a **rational cuspidal fiber** and
- there are at least two such rational cuspidal fibers.

It follows that by composing ϕ with an appropriate $\mathbf{Q}$-automorphism of $\mathbf{P}^1$ one gets a fine Siegel unit. It follows that the problem of computing the $\mathbf{Q}$-rational points on $WX_1(17)$ is essentially equivalent to that of computing fine Siegel units of degree four. As mentioned in Section 4, this is a finite computation.

We will be giving the collection of all fine Siegel units f of geometric degree 4—up to composition by appropriate $\mathbf{Q}$-automorphisms $b : \mathbf{P}^1 \to \mathbf{P}^1$. This we do by listing the divisors that describe the cuspidal-fibers for each f and organizing these cuspidal-fiber matrices in Δ-orbits. Each such Δ-orbit describes *one* class of $\mathbf{Q}$-parametrizations of $X_1(17)$ (of geometric degree 4); there are three of them.

Each divisor with support on these rational cusps is encoded by 8 integers, where the i-th integer is the multiplicity of the i-th cusp in the ordering:

$$\{2/17, 3/17, 4/17, 5/17, 6/17, 7/17, 8/17, \infty\}.$$

We display this data for a given f as a matrix, with exactly 8 columns, and as many rows as there are cuspidal-fibers for f. This is the **cuspidal-fiber matrix of** f as discussed in section 4 above.

The first two classes factor through the quotient of $X_1(17)$ under the action of the involution $\langle 13\rangle$. That is, they factor through the double cover

$$X_1(17) \quad \stackrel{\pi}{\longrightarrow} \quad X_1(17)/\langle 13\rangle.$$

The quotient curve $X_1(17)/\langle 13\rangle$ is isomorphic over $\mathbf{Q}$ to the elliptic curve $E := 17A4$ in Cremona's classification. The Mordell–Weil group of 17A4 (over $\mathbf{Q}$), is cyclic of order four. Make one (of the four possible) identifications—rational over $\mathbf{Q}$:

$$X_1(17)/\langle 13\rangle \quad \stackrel{\iota}{\cong} \quad E$$

The determination of the cuspidal-fiber matrix for each of these two classes uses a minimum of computation; i.e., we work essentially by 'pure thought,' given the fact that $E(\mathbf{Q})$ is cyclic of order four. Since there are eight rational cusps on $X_1(17)$ and $\iota \cdot \pi$ is of degree two, these eight rational cusps are unramified for the mapping $\iota \cdot \pi$, and the set of them map surjectively—by a two-to-one mapping—to $E(\mathbf{Q})$. Now E itself has precisely four $\mathbf{Q}$-rational involutions υ_a such that $E/\langle \upsilon_a\rangle \cong \mathbf{P}^1$. These are given by the formulae $x \mapsto a - x$ for $a \in E(\mathbf{Q})$. Note that

- $|E(\mathbf{Q})/\langle \upsilon_a\rangle| = 3$ if a is trivial or of order two, while
- $|E(\mathbf{Q})/\langle \upsilon_a\rangle| = 2$ if a is one of the two generators of $E(\mathbf{Q})$.

Denote

$$f_a : E \to E/\langle \upsilon_a\rangle \approx \mathbf{P}^1$$

the double cover associated to the involution υ_a. Now if t_b is translation by b with b a point of order 4 and if $a' - a$ is in $E(\mathbf{Q})[2] \setminus \{0\}$ then $\upsilon_a = t_b \circ \upsilon_{a'} \circ t_b^{-1}$, implying that f_a and $f_{a'}$ are in the same parameterization class. So we have (at most) two $\mathbf{Q}$-rational classes of parametrizations of E of degree two coming from the four maps f_a.That these are in fact different equivalence classes can be seen from the bullets above. For more specificity, choose an identification ("$\approx$") of $E/\langle \upsilon_a\rangle$ with $\mathbf{P}^1$ so that in the first case above $E(\mathbf{Q})/\langle \upsilon_a\rangle$ is identified with the set $\{0, 1, \infty\}$ (any order will do) and in the second case it is identified with $\{0, \infty\}$. Fixing such an identification, but composing with $\iota \cdot \pi$ for the four possible choices of ι gives two Δ-orbits of fine Siegel units of degree four on $X_1(17)$.

The cuspidal-fiber matrices for the two $\mathbf{Q}$-parametrizations of $X_1(17)$ (of geometric degree 4) that factor through $X_1(17)/\langle 13\rangle$ are immediately computable from this discussion. In particular they each consist of a single Δ-orbit of order two. We'll call them "$\mathbf{Q}$-similarity classes **(A)** and **(B)**."

- **Q-similarity class of parametrizations (A):**

$$M_1 := \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}$$

$$M_2 := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \end{pmatrix}$$

- **Q-similarity class of parametrizations (B):**

$$M_3 := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_4 := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Far less evident is the third (and last) class of $\mathbf{Q}$-parametrization of $X_1(17)$ of degree four. This class ("**(C)**") is given (as shown in the discussion below) by a single Δ-orbit of order eight, described by eight cuspidal-fiber matrices $M_5, M_6, \ldots, M_{12}$ permuted by the action of Δ. These 8 matrices correspond to the 8 rational points of W_1.

- **Q-similarity class of parametrizations (C):**

$$M_5 := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$M_6 := \langle 3 \rangle M_5 \quad \cdots \quad M_{12} := \langle 3 \rangle^7 M_5$$

Depending on how you decide which of the three rational cuspidal fibers will be *zeroes* of your function and which *poles* you get different $\mathbf{Q}$-linear parameterizations of $X_1(17)$ and different fine Siegel units. For example E_1E_3/E_5E_6 has the first row of M_5 as zero-divisor and the second row as polar-divisor, while $E_3E_4E_8/E_2E_6E_7$ has the third row of M_5 as zero-divisor and the second row as polar-divisor.

We can summarize as follows. Let

$$\Gamma \subset X_1(17)(\bar{\mathbf{Q}})$$

denote the set of non-cuspidal algebraic points of $X_1(17)$ defined over number fields of degree four. If $\gamma \in \Gamma$ let $\mathbf{Q}(\gamma)$ denote the number field (of degree four) over which γ is defined. Say that γ is of type **(A)**, **(B)** respectively **(C)** if the projection of γ under one of the $\mathbf{Q}$-parametrization in the equivalence class **(A)**, **(B)** respectively **(C)** is a $\mathbf{Q}$-rational point of $\mathbf{P}^1$. Let $\Gamma_{(\mathbf{A})} \subset \Gamma$ denote the subset of points of type **(A)**; and similarly for $\Gamma_{(\mathbf{B})}$ and $\Gamma_{(\mathbf{C})}$.

Theorem 4. *The set* Γ *(of non-cuspidal algebraic points of* $X_1(17)$ *defined over number fields of degree four) is the disjoint union*

$$\Gamma \quad = \quad \Gamma_{(\mathbf{A})} \bigsqcup \Gamma_{(\mathbf{B})} \bigsqcup \Gamma_{(\mathbf{C})}.$$

Proof. The above discussion gives us the full list of $\mathbf{Q}$-similar classes of $\mathbf{Q}$-parametrized points of degree 4 on $X_1(17)$. The fact that $W_4^2 X_1(17)$ is empty (because $X_1(17)$ has no functions of degree 3) shows that the union above is a *disjoint union*. It remains to show that $X_1(17)$ has no very sporadic, or sporadic points that are not cusps. For this, see section 5.3 below. □

Proposition 5. *Let* x, y, z *be the functions from theorem 3, then the Galois groups of* $\mathbf{Q}(x) \subset \mathbf{Q}(X_1(17))$, $\mathbf{Q}(y) \subset \mathbf{Q}(X_1(17))$ *and* $\mathbf{Q}(z) \subset \mathbf{Q}(X_1(17))$ *are* S_4, D_4 *and* D_4 *respectively.*

Proof. Let K_x denote the Galois closure of $\mathbf{Q}(x) \subset \mathbf{Q}(X_1(17))$, then by looking at matrix M_5 one sees that $[K_x : \mathbf{Q}(X_1(17))]$ has to be divisible by 6, implying that 24 divides $[K_x : \mathbf{Q}(x)]$ hence the Galois group has to be S_4.

For the proof that the other two Galois groups are D_4, one can use the following observation: Suppose that $M \subset L \subset K$ is a tower of field extensions with $[L : M] = [K : L] = 2$ and K/M is not Galois, then K/M has Galois group D_4. One can then apply this observation to $\mathbf{Q}(y) \subset \mathbf{Q}(X_1(17)/\langle 3^4 \rangle) \subset \mathbf{Q}(X_1(17))$ and $\mathbf{Q}(z) \subset \mathbf{Q}(X_1(17)/\langle 3^4 \rangle) \subset \mathbf{Q}(X_1(17))$. Now $\mathbf{Q}(X_1(17))/\mathbf{Q}(y)$ and $\mathbf{Q}(X_1(17))/\mathbf{Q}(z)$ are not Galois follows from the fact that there is no subgroup $H \subset \mathrm{Aut}_{\mathbf{Q}}(X_1(17)) = (\mathbf{Z}/17\mathbf{Z})^*/\pm 1$ of order 4 such that $X_1(17)/H \cong \mathbf{P}^1$.

□

5.3. **Sporadic and very sporadic points on** $X_1(17)$**.** The computations in the previous section show that the number of g_4^1's on $X_1(17)$ that are defined over $\mathbf{Q}$ is exactly 12. This is actually proved twice, once by proving $12 = 4 + 8 = \#W_0(\mathbf{Q}) + \#W_1(\mathbf{Q})$, and once by using proposition 4 and computing that there are exactly 12 cuspidal fiber matrices corresponding to fine Siegel units of degree 4. The main goal of this section is to prove the following theorem:

Theorem 5. *Every point on* $X_1(17)$ *of degree* 4 *over* $\mathbf{Q}$ *is in one of the 12* g_4^1*'s.*

For the proof of this theorem we will use a slight modification of a theorem due to Michael Stoll in [8].

Let $C/\mathbf{Q}$ be a curve with jacobian J, and let $d \geq 1$ be an integer. Let C^d be the dth power, and $C_d := \mathrm{Symm}^d(C)$ the dth symmetric power of C. Let

$$C_d^{\{1\}} := C_d \times_J W_d^1(C).$$

So $C_d^{\{1\}} \subset C_d$ is the closed subvariety parametrizing those divisors D of degree d such that $\dim H^0(O_C(D), C) - 1 = \dim |D| \geq 1$.

Denote by $s : C^d \to C_d$ the natural quotient map.

Theorem 6. *Let ℓ be a prime of good reduction for C. Let $P_0 \in C(\mathbf{Q})$ be chosen as base-point for an embedding $\iota : C \to J$. This also induces morphisms $C^d \to C_d \to J$. If the following assumptions hold:*

1. *$\ell > 2$ or $J(\mathbf{Q})[2]$ injects into $J(\mathbf{F}_\ell)$ (for example, $\#J(\mathbf{Q})$ is odd).*
2. *$J(\mathbf{Q})$ is finite.*
3. *The reduction map $C(\mathbf{Q}) \to C(\mathbf{F}_\ell)$ is surjective.*
4. *The intersection of the image of $C_d(\mathbf{F}_\ell)$ in $J(\mathbf{F}_\ell)$ with the image of $J(\mathbf{Q})$ under reduction mod ℓ is contained in the image of $C^d(\mathbf{F}_\ell)$.*

Then $C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q})$ is contained in the image of $C^d(\mathbf{Q}) \to C_d(\mathbf{Q})$.

Proof. Let ρ_X denote the reduction map $X(\mathbf{Q}) \to X(\mathbf{F}_\ell)$, where X is a smooth projective variety over $\mathbf{Q}$ with good reduction at ℓ.

From assumptions (2) and (1) we can deduce that $\rho_J : J(\mathbf{Q}) \to J(\mathbf{F}_\ell)$ is injective. By the definition of $C_d^{\{1\}}$ it is also clear that $C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q}) \to J(\mathbf{Q})$ is injective.

Finally (3) shows that $\rho_C^d : C^d(\mathbf{Q}) \to C^d(\mathbf{F}_\ell)$ is surjective.

$$\begin{array}{ccccc}
 & & C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q}) & & \\
 & & \downarrow & \searrow^{\iota} & \\
C^d(\mathbf{Q}) & \xrightarrow{s} & C_d(\mathbf{Q}) & \xrightarrow{\iota} & J(\mathbf{Q}) \\
\downarrow{\scriptstyle \rho_{C^d}} & (3) & \downarrow{\scriptstyle \rho_{C_d}} & & \downarrow{\scriptstyle \rho_J} \; (2,1) \\
C^d(\mathbf{F}_\ell) & \xrightarrow{s} & C_d(\mathbf{F}_\ell) & \xrightarrow{\iota} & J(\mathbf{F}_\ell).
\end{array}$$

Now let $P \in C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q}) \to J(\mathbf{Q})$. We want to show that there is a $Q \in C^d(Q)$ such that $s(Q) = P$. Now $\rho_J \circ \iota(P) = \iota \circ \rho_{C_d}(P) \in J(\mathbf{F}_\ell)$ so from assumption (4) it follows that there is a $\overline{Q} \in C^d(\mathbf{F}_\ell)$ such that $\iota \circ s(\overline{Q}) = \rho_J \circ \iota(P)$. Let $Q \in C^d(\mathbf{Q})$ be such that $\rho_{C^d}(Q) = \overline{Q}$ then

$$\rho_J \circ \iota \circ s(Q) = \iota \circ s(\overline{Q}) = \rho_J \circ \iota(P).$$

The injectivity of ρ_J implies $\iota \circ s(Q) = \iota(P)$ and because $P \notin C_d^1(\mathbf{Q})$ we know that $s(Q) = P$. □

Corollary 7. *If the above hypotheses hold for $d = \gamma_{\mathbf{C}}(C)$ then all sporadic points of C are $\mathbf{Q}$-rational.*

Proposition 6. *There are no sporadic non-cuspidal points on $X_1(17)$.*

Proof. We apply Theorem 6 taking $C := X = X_1(17)$. We take $\ell = 3$, so (1) holds. Since $J_1(17)(\mathbf{Q})$ is of finite order[16], condition (2) holds. The Hasse-Weil bound implies that for an elliptic curve E over $\mathbf{F}_3$ we have $\#E(\mathbf{F}_3) \leq 3 + 1 + 2\sqrt{3} < 8$ so

[16] $J_1(17)(\mathbf{Q})$ is of order $584 = 8 \cdot 73$ ([18] for the prime-to-2 part; and for the 2-torsion: [34]). Regarding values of N for which $J_1(N)(\mathbf{Q})$ is finite, consult Prop. 6.2.1 in [10].

this E cannot have an $\mathbf{F}_3$-rational point of order 17 showing that $X = X_1(17)(\mathbf{F}_3)$ consists entirely of cusps, which gives (3). Finally we verified with a computation in magma that assumption (4) is also satisfied.

□

References

[1] D. Abramovich, A linear lower bound on the gonality of modular curves, International Mathematical Research Notices **20** (1996) 1005-1011

[2] D. Abramovich; J. Harris, Abelian varieties and curves in $W_d(C)$, Compositio Mathematica, **78** (1991) 227-238

[3] J. Bosman, Explicit computations with modular Galois representations, PhD Thesis

[4] E. Arbarello; M. Cornalba; P. Griffiths; J. Harris, Geometry of Algebraic Curves I, Springer (1985)

[5] E. Arbarello; M. Cornalba; P. Griffiths, Geometry of Algebraic Curves II (with a contribution of J. Harris), *Grundlehren der Mathematischen Wissenschaften* [Fundamental Principles of Mathematical Sciences] **268**, Springer (2011)

[6] P.L. Clark; B. Cook; J. Stankewicz, Torsion points on elliptic curves with complex multiplication, International Journal of Number Theory **9** 2013 447-479

[7] M. Derickx; M. Hoeij, Gonality of the modular curve $X_1(N)$ (preprint `http://arxiv.org/abs/1307.5719v3`)

[8] M. Derickx; S. Kamienny; W. Stein; M. Stoll, Torsion Points on Elliptic Curves over Fields of Small Degree (preprint)

[9] I.V. Dolgachev *Classical Algebraic Geometry: a modern view*

[10] B. Conrad; B. Eidixhoven, W. Stein, $J_1(p)$ has connected fibers. Documenta Math. **8** (2003) 325-402

[11] G. Faltings, The general case of S. Lang's conjecture, Barsotti Symposium in Algebraic Geometry, Perspectives in Math **15** (1994) 175-182

[12] G. Frey, Curves with infinitely many points of fixed degree, Israel Journal of Mathematics **85** (1994) 79-83

[13] F. Hess, Computing Riemann-Roch spaces in algebraic function fields and related topics, J. Symbolic Computation **11** (2001) 1-21. http://www.staff.uni-oldenburg.de/florian.hess/publications/rr.pdf

[14] M. Hoeij, Low degree places on the modular curve $X_1(N)$ (preprint `http://arxiv.org/abs/1202.4355`)

[15] D. Jeon; C.H. Kim; Y. Lee, Families of elliptic curves over cubic number fields with prescribed torsion subgroups, Math. Comp. **80** (2011) 579-591

[16] D. Jeon; C.H. Kim; Y. Lee, Families of elliptic curves over quartic number fields with prescribed torsion subgroups, Math. Comp. **80** (2011) 2395-2410

[17] S. Kamienny, On $J_1(p)$ and the Conjecture of Birch and Swinnnerton-Dyer, Duke Math J. **49** (1982) 329-340

[18] S. Kamienny, Rational points on modular curves and abelian varieties, J. reine angew. Math. **359** (1985) 174-187

[19] S. Kamienny, Torsion Points on Elliptic Curves over all Quadratic Fields, Duke. Math. Journal 53 (1986), 157-162.

[20] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109** (1992), 221-229

[21] S. Kamienny, Torsion points on elliptic curves over fields of higher degree, Internat. Math. Res. Notices (1992) **6** 129-133

[22] S. Kamienny; B. Mazur, Rational torsion of prime order in elliptic curves over number fields. With an appendix by A. Granville. Columbia University Number Theory Seminar (New York, 1992) Astérisque **228** (1995), 3, 81-100.
[23] S. Kamienny; Najman, Filip, Torsion groups of elliptic curves over quadratic fields. Acta Arith. **152** (2012), 291-305.
[24] Kenku; M. A.; F. Momose, Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. **109** (1988), 125-149
[25] D. Kubert; S. Lang, *Modular Units* Springer (1981)
[26] M. Laska; M. Lorenz, Rational point in elliptic curves over **Q** in elementary abelian 2-extensions of **Q**, J.Reine Angew. Math **355** (1985) 163-172
[27] Lozano-Robledo, On the field of definition of p-torsion on elliptic curves over the rationals, Math. Annalen, **35** (2013) 279-305
[28] B. Mazur, Modular Curves and the Eisenstein Ideal I.H.E.S. Publ. Math **47** (1978) 33-186
[29] B. Mazur, Rational Isogenies of Prime Degree, Inv. Math. **44** (1978), 129-162
[30] B. Mazur; J. Tate, Points of Order 13 on Elliptic Curves, Inv. math. **22** (1973) 41-49
[31] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Inv. Math. **124** (1996) 437-449
[32] F. Momose, p-torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **96** (1984) 139-165
[33] F. Najman, Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$, `arXiv.org>math>arXiv:1211.2188` (version 3) (2013) (Math. Res. Letters; to appear)
[34] P. Parent, No 17-torsion on elliptic curves over cubic number fields, J. Th. Nombres Bordeaux **15**, no. 3 (2003) 831-838
[35] G. Stevens, Arithmetic on modular curves. Progress in Mathematics, **20**, Birkhauser, (1982)
[36] A. Sutherland, `http://math.mit.edu/~drew/X1_altcurves.html`
[37] Y. Yang, Modular unit and cuspidal divisor class groups of $X_1(N)$, arXiv:0712.0629 [math.NT]

Aknowledgements

First of all I would like to thank my first supervisor Bas Edixhoven who was also my thesis supervisor during my masters and helped me get this Ph.D position. I already learned a lot from him whilst still a Master student, and I learned even more as a Ph.D student. I especially appreciate his support and patience during the more difficult times of my Ph.D.. Alongside I would like to thank my other two supervisors Pierre Parent and Bert van Geemen, from whom I also learned a lot.

This thesis is also thanks to the work of my co-authors, the results in this thesis are only possible through their collaboration, each of them bringing their own invaluable additions. I want to thank William Stein for inspiring me with the topic of rational points on modular curves during his talk at the Lorentz center, Barry Mazur for his seemingly inexhaustible ability to come up with interesting questions, Mark van Hoeij for his getting things done spirit, Sheldon Kamienny for always catching my mistakes, Andrew Sutherland[1] for encouraging me to pick up the low hanging fruit, and Michael Stoll for his trust in me and inviting me for a post doc.

Special thanks also go to Joseph Oesterlé who gave me his notes for his prove of his $(3^{d/2}+1)^2$ bound, and allowed me to use these to write the appendix to Chapter 3 which fills an important gap in the literature.

I would like to thank the reading committee for the time that they took for carefully reading my thesis, especially Marusia Rebolledo for her long list of suggestions for improvements, and the opposition committee for honouring me with their presence.

I would like to thank Marco Streng and John Cremona for inviting me to be a speaker on my first international workshop, the SAGE and the LMFDB communities for all their productive workshops and I would like to thank Peter Bruin and Michiel Kosters for having co-organized the sage days workshop in the Lorentz center with me.

Bedankt Steve voor de origami discussies.

Thank you Carlo, Giulia, Owen, David, Jinbi, Pinar, Ceyda, Isil, Giulio, Chloe, Erik, Maarten, Wouter, Iuliana, Mima, Dino, Eva, Albert, Aryan, Abtien, Zoé, Bruno, Samuel, Alan, Marie, Jocelyn, JB, Nicolas, Samuele, Alberto, Gabe, Fede, Silvia, Giulio, Adéle, Arnoud, Anna, Jet, Kitso, Vera, Fré, Neal, Jacob[2], Jonna,

[1]The article I co-authored with Andrew was only finished shortly before my defense and hence not part of this thesis

Aart, Robert, Arno, Jelle, Bas, Steven, Stijn, Amir, Kees, Kevin, Roosje, Sasja, Anniek and other friends that made these last four years worthwhile.

Als laatse wil ik graag mijn vader, moeder en broer bedanken voor hun steun de afgelopen jaren en Tessa voor de energie die ze mij heeft gegeven.

Samenvatting

Een Pythagorees drietal, vernoemd naar de stelling van Pythagoras, is een drietal van gehele getallen a,b,c zodanig dat $a^2 + b^2 = c^2$. Een voorbeeld van een dergelijk drietal is $3^2 + 4^2 = 5^2$. Dit voorbeeld samen met andere Pythagorese drietallen zijn al te vinden op Babylonische kleitabletten van wiskundige aard stammend uit de periode rond 1800 v.C. Dit voorbeeld illustreerd dat mensen al sinds de oudheid geinterreseerd waren in de vraag of een kwadraat geschreven kan worden als som van kwadraten. Als men het niet erg vind met breuken te werken in plaats van met gehele getallen kan met de vergelijking $a^2+b^2 = c^2$ ook herschrijven tot $y^2 = x^2+1$, met $y = \frac{c}{a}$ en $x = \frac{b}{a}$ en word de vraag dus wanneer is een kwadraad van de vorm van een kwadadraat + 1. Als men het kwadratische polynoom $x^2 + 1$ door een derdegraads polynoom zoals $x^3 + 2x + 2$ vervangt, beland men in de wereld van Elliptische krommen waar dit proefschrift over gaat.

Het is een stelling van Barry Mazur die zegt dat als a en b breuken zijn, dat dan de verzamling van oplossingen (x, y) van $y^2 = x^3 + ax + b$ met x en y breuken, of hooguit 15 elementen bevat of oneindig groot is.

In dit proefschrift word er gekeken naar hoeveel oplossingen (x, y) de vergelijking $y^2 = x^3 + ax + b$ kan hebben als we iets algemener a, b, x, y algebraische getallen van kleine graad laten zijn. Een voorbeeld van een algebraisch getal van graad twee is $\sqrt{3} + 1$.

Hoofdstuk 1 is een inleidend hoofdstuk bedoeld voor voornamelijk Master en Ph.D. studenten in de wiskunde om de rest van dit proefschrift beter begrijpbaar te maken voor hen. De rest van dit proefschrift bestaat uit artikelen.

Hoofdstuk 2 is een artikel dat gepubliseerd is in Journal of Algebra en is samen met Mark van Hoeij geschreven. In dit hoofdstuk ontwikkelen we een strategie voor het uitrekenenen we gonaliteiten van modulaire krommen, ook laten we zien wat voor een gevolgen de uitkomst van deze berekeningen heeft voor het aantal oplossingen van $y^2 = x^3 + ax + b$ in x en y over getallenlichamen van graad ≤ 8.

Chapter 3 is een artikel dat voorkomt uit een samenwerking tussen Sheldon Kamienny, William Stein, Michael Stoll en mij. Dit is nog niet gepubliseerd maar zal zeer binnenkort opgestuurd worden ter publicatie. In dit hoofdstuk worden de priemen bepaald die 1 plus het aantal oplossingen van aantal oplossingen in x en y van $y^2 = x^3+ax+b$ kunnen delen. Dit word gedaan voor x, y, a, b in getallenlichamen van graad ≤ 6.

Het laatste hoofdstuk is een artikel dat zal verschijnen in een herdekings uitgave ter ere van Fumiyuki Momose. De co-auteurs zijn Barry Mazur and Sheldon Kamienny. In dit hoofdstuk word heel expliciet bestudeerd wanneer de vergelijking $y^2 = x^3 + ax + b$ precies 16 oplossingen heeft in x, y over een getallenlichaam van graad 4.

Curriculum vitea

Maarten Derickx was born on the 22nd of juni in 1986 in Voorst (Netherlands) and shortly thereafter moved to the nearby city Zutphen where he won the Nederlandse Wiskunde Olympiade in 2003 and obtained his highschool diploma at the Stedelijk Dalton College in 2004.

He then moved on to study physics and mathematics at Universiteit Twente, but already after the first year he found out that he enjoyed mathematics more and wanted to go to a place where the offered curriculum was more theoretical.

Continuing in Leiden, he first studied two years and then took a break of one year to be treasurer in the Board of the student association VSL Catena and finally obtained his bachelors degree in 2010 under the supervision of prof. Bart de Smit. In Leiden he continued with a master which he received cum laude in 2012 under the Supervision of prof. Bas Edixhoven.

In 2012 he also received a ALGANT doctorate scholarship allowing him to enrol as student of a joint Ph.D. program at the universities of Bordeaux, Leiden, and Milaan under the supervision of supervision of dr. Pierre Parent, prof. Bas Edixhoven and prof. Bert van Geemen, graduating in September 2016.

As of October 2016 he will hold a one year postdoctoral position at the university of Bayreuth in the research group of Michael Stoll.

Maarten enjoys playing improvisational pieces on the piano and a wide variety of dances ranging from Salsa to Rock 'n Roll.