Explicit Division and Torsion Points on Superelliptic Curves and Jacobians

by

Vishal Arul

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Mathematics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2020

Author . . . .
Department of Mathematics
April 28, 2020

Certified by . . . .
Bjorn Mikhail Poonen
Distinguished Professor in Science
Thesis Supervisor

Accepted by . . . .
Davesh Maulik
Chairman, Department Committee on Graduate Theses

Explicit Division and Torsion Points on Superelliptic Curves and Jacobians

by

Vishal Arul

Submitted to the Department of Mathematics
on April 28, 2020, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Mathematics

Abstract

In this thesis, I study two problems in the arithmetic of superelliptic curves. By a superelliptic curve, I mean the smooth projective model of the affine plane curve $y^n = f(x)$ where $f(x)$ is separable, n is coprime to $\deg(f)$, and the characteristic of the ground field does not divide n. When $n = 2$, this is commonly referred to as a hyperelliptic curve.

I first generalize Zarhin's formula for division by 2 [68] on hyperelliptic curves to the superelliptic case. Rather than divide by n, I invert the $1-\zeta$ endomorphism on the jacobian. My formula reduces to Zarhin's when $n = 2$.

Next, I study torsion points on superelliptic curves. Work of Coleman [15] and Grant–Shaulis [29] together classifies all torsion points on the hyperelliptic curve $y^2 = x^d + 1$, where $d \geq 5$ is prime. I extend their results to the superelliptic curve $y^n = x^d + 1$, where $n, d \geq 2$ are coprime. Using a specialization argument, I also classify torsion points on a generic superelliptic curve, extending Theorem 7.1 of Poonen–Stoll [57] to the hyperelliptic case.

In order to classify torsion points, I prove a result about Galois action on the p-torsion of the jacobian of $y^p = x^q + 1$, where p and q are distinct primes. This problem is equivalent to a new p-adic congruence for Jacobi sums, which I state and prove. This congruence is related to (but does not follow from) a congruence of Uehara [63].

Thesis Supervisor: Bjorn Mikhail Poonen
Title: Distinguished Professor in Science

Acknowledgments

First, I would like to thank my advisor Bjorn Poonen. Your kind and patient advising helped me grow greatly as a mathematician and as a mentor. I always looked forward to our weekly meetings; they were one of the high points of graduate school for me. I always felt comfortable asking you questions, no matter how dumb I may have thought they were. Through your patient and clear answers, I learned a great deal of mathematics and learned how to communicate mathematics. Thank you very much for everything you have done for me, including writing recommendation letters, answering my many questions, reading drafts of my work, and providing career advice. I will very much miss our weekly meetings after I graduate.

Without the constant support from my parents and extended family, I would not have pursued a doctorate in mathematics. Mom, thank you for inspiring a love of mathematics when I was in elementary school. Mom and Dad, thank you for prioritizing my education and for all the extracurricular math opportunities you encouraged and enabled me to pursue in school. Thank you for always being there when I needed you the most, and for encouraging me to chase my dreams.

Paula Jurgonski and Susan Holtzapple, thank you for being the best math teachers I could have asked for; both of you truly opened up entire worlds of mathematics to me. Mrs. Jurgonski, before becoming your student, my image of mathematics was that it was a long flight of stairs, and that I would eventually reach the top after taking enough classes. Thank you for showing me that mathematics is much deeper and more vast than I could have ever previously imagined, and for sharing your love of mathematics with me. Mrs. Holtzapple, thank you for introducing me to the world of math competitions and for helping me believe in my ability to do mathematics. Thank you for teaching me about proofs and showing how mathematics is more than just about finding the right answer. To both of you – it was truly a privilege to be your student.

During my time at Stanford, I was lucky to be taught and mentored by many excellent professors. Thank you Brian Conrad, Kannan Soundararajan, and Ravi Vakil for your amazing mentoring, for teaching me so much about algebraic geometry and number theory, for helping me grow as a mathematician, and for writing letters of recommendation for me. Thank you so much for your support and for being my role models. The three of you helped me believe in myself and convinced me that I could pursue a career in mathematics.

I would like to thank the 2013 Pennsylvania State REU for giving me my first experience with research mathematics. I very much enjoyed my time at the REU, and I thank all of the students, staff, and faculty at the program for helping me have such a postive experience. Donald Newhart, thank you for being such an excellent mentor; you were a big reason why my first experience with mathematical research was such an exciting and rewarding one. I am very grateful to have met you on my mathematical journey.

I am very fortunate to have had so many excellent mentors during my time at MIT. I would like to thank Davesh Maulik, Wei Zhang, Drew Sutherland, David Roe, Edgar Costa, Aaron Pixton, and Daniel Kriz for all of your advice and mathematical discussions. Thank you Davesh Maulik and Wei Zhang for being on my thesis committee, and thank you Davesh Maulik and David Roe for writing letters of recommendation for me. Additionally, I would like to thank Larry Guth and Davesh Maulik for being such excellent role models for teaching; I had a blast being your Course Assistant for 18.02(A) and I learned a great deal about teaching undergraduates.

Pavel Etingof, Slava Gerovitch, and Tanya Khovanova – thank you for all of the men-

toring opportunities you provided for me in graduate school, including PRIMES, DRP, and Mathroots. I would like to extend a special “thank you” to all of the Academic Mentors and Resident Counselors who helped make Mathroots such a special program. Jessica Ch’ng, I am very grateful for your support; the help we receive from MIT Admissions is invaluable to Mathroots. Gwen McKinley and Piotr Suwara, thank you for being such excellent Program Directors. I very much enjoyed working with the both of you, and I am very grateful for all the hard work you put into the program.

My (extended) academic family is one of my biggest sources of support, and I fear I cannot adequately express in words how much you all mean to me. Thank you Padmavati Srinivasan, Renee Bell, David Corwin, Isabel Vogt, Nicholas Triantafillou, Atticus Christensen, Borys Kadets, Campbell Hewett, Sachi Hashimoto, Alex Best, and Lynnelle Ye. Padma, Renee, David, Isabel, Nicholas, and Borys – you all made our Bjorn army headquarters truly feel like a second home. One of my biggest fears in graduate school was that I would be isolated working on some difficult research problem every day, and I cannot thank you all enough for making the experience of learning mathematics and doing research much more cooperative and enjoyable. I am very lucky to be a part of such a warm and large academic family.

Thank you Andrew Ahn, Ethan Jaffe, Hood Chatham, and Chris Ryba for keeping me sane throughout graduate school. Eating meals with you all was one of the highlights of my graduate school experience. Andrew and Ethan, I learned a lot about nutrition and fitness by spending time with both of you, and I am grateful that you both made sure I took breaks even when I didn’t realize I needed them. Hood, I learned so much from our random discussions. I enjoyed our hikes and your dinner parties. Chris, I enjoyed your food creations, our walking adventures, and playing squash with you. I will miss you all very much after we graduate.

This research was supported in part by grants from the Simons Foundation (#402472 to Bjorn Poonen, and #550033).

Contents

Chapter 1

Introduction

1.1 History and motivation

Suppose that K is a field such that $\mathrm{char}(K) \notin \{2, 3\}$. Recall that an elliptic curve is the smooth projective model of an affine plane K-curve given by an equation of the form

$$y^2 = f(x) \tag{1.1}$$

where $f(x) \in K[x]$ is separable with $\deg f \in \{3, 4\}$. Elliptic curves are a central object of study in number theory. The proof of Fermat's last theorem uses a special kind of elliptic curve called the Frey curve. Elliptic curve cryptography is one modern approach to cryptography that is based on elliptic curves defined over finite fields. The Birch and Swinnerton-Dyer conjecture, which is one of the open Millenium problems, states that the analytic rank and algebraic rank should agree for every elliptic curve defined over a number field; much of modern number theory is motivated by studying this conjecture.

Hyperelliptic curves are a natural generalization of elliptic curves; a hyperelliptic curve is the smooth projective model of $y^2 = f(x)$ where $f(x) \in K[x]$ is separable, but with no constraint on $\deg f$. Understanding the arithmetic of hyperelliptic curves is a major area of research in arithmetic geometry. In particular, when the genus of the curve is at least 2 (which is equivalent to $\deg f \geq 5$), Faltings' theorem implies that there should only be finitely many rational points.

In this thesis, we study a further generalization by considering curves of the form

$$y^n = f(x)$$

where $\mathrm{char}(K) \nmid n$, $f(x) \in K[x]$ is separable, and $(n, \deg f) = 1$. Such curves are called "superelliptic" curves. Let ζ be a primitive nth root of unity in $\overline{K}$. We will also use ζ to denote the automorphism $(x, y) \to (x, \zeta y)$ of the curve.

Superelliptic curves are a natural generalization of hyperelliptic curves, so it is sensible to investigate the arithmetic of superelliptic curves. Algorithms for computing in the jacobian of superelliptic curves and for the discrete logarithm problem for superelliptic curves are given in [26]. Many techniques for understanding hyperelliptic curves have recently been extended to the superelliptic case, including generalizing Kedlaya's algorithm for computing zeta functions of hyperelliptic curves via Monsky-Washnitzer cohomology [42] to superelliptic curves [7, 27, 28, 49] and generalizing explicit Coleman integration on hyperelliptic curves [9] to the superelliptic curves [13].

In particular, we will generalize three results from hyperelliptic curves to superelliptic curves: in Section 3.2, we generalize Zarhin's "division by 2" formula on hyperelliptic curves and jacobians [68]; in Section 5.2, we generalize Grant and Shaulis's work on determining the cuspidal torsion packet on hyperelliptic Fermat quotients [29]; in Section 5.3, we generalize Theorem 7.1 of [57], which determines the cuspidal torsion packet on a generic hyperelliptic curve.

1.2 Methods and new results

1.2.1 Explicit division on superelliptic curves

In [68], Zarhin considers the following problem: given a point $P = (x_P, y_P) \in \mathcal{C}(K)$, how does one compute its "halves" inside $\mathcal{J}(\overline{K})$? That is, compute every divisor class $[D] \in \mathcal{J}(\overline{K})$ such that

$$2[D] = [P - \infty].$$

To represent divisor classes $[D]$, Zarhin uses the Mumford representation, which is a pair of polynomials $U, V \in K[X]$ that uniquely determines $[D]$. For reference, we restate his result.

Theorem 1.2.1 (Theorem 3.2 of [68])**.** *Let $\mathcal{C}$ be the hyperelliptic curve given by $y^2 = (x-\alpha_1)\cdots(x-\alpha_{2g+1})$ where $\alpha_1, \cdots, \alpha_{2g+1}$ are distinct elements of K. Suppose that $P = (a,b) \in \mathcal{C}(K)$. Then the 2^{2g}-element set*

$$M_{1/2,P} := \{\mathfrak{a} \in \mathcal{J}(\overline{K}) : 2\mathfrak{a} = [P - \infty]\}$$

can be described as follows. Let $\mathfrak{R}_{1/2,P}$ be the set of all $(2g+1)$-tuples $\mathfrak{r} = (\mathfrak{r}_1, \cdots, \mathfrak{r}_{2g+1})$ of elements of $\overline{K}$ such that

$$\mathfrak{r}_i^2 = a - \alpha_i \text{ for all } 1 \le i \le 2g+1, \qquad \prod_{i=1}^{2g+1} \mathfrak{r}_i = -b.$$

Let $s_i(\mathfrak{r})$ be the value of the ith basic symmetric function at $\mathfrak{r}_1, \cdots, \mathfrak{r}_{2g+1}$. We put

$$U_{\mathfrak{r}}(x) = (-1)^g \sum_{j=0}^{g} s_{2j}(\mathfrak{r})(a-x)^{g-j}$$

$$V_{\mathfrak{r}}(x) = \sum_{j=1}^{g} (s_{2j+1}(\mathfrak{r}) - s_1(\mathfrak{r})s_{2j}(\mathfrak{r}))(a-x)^{g-j}.$$

Then there is a natural bijection between $\mathfrak{R}_{1/2,P}$ and $M_{1/2,P}$ such that $\mathfrak{r} \in \mathfrak{R}_{1/2,P}$ corresponds to $\mathfrak{a}_{\mathfrak{r}} \in M_{1/2,P}$ with Mumford representation $(U_{\mathfrak{r}}, V_{\mathfrak{r}})$.

Theorem 3.2.1 extends Zarhin's result to the superelliptic case; setting $n = 2$ in Theorem 3.2.1 recovers Zarhin's theorem. Instead of dividing by 2, we divide by "$1 - \zeta$." One of the challenges is that points of superelliptic jacobians do not, in general, admit a "Mumford representation." Instead, we track the data of a degree zero divisor class with n elements of $K[x, y]$.

1.2.2 Torsion points on superelliptic curves

In [29], Grant and Shaulis consider hyperelliptic curves of the form

$$y^2 = x^d + 1$$

where $d \geq 5$ is prime. A torsion point is a geometric point P on the curve such that the divisor class $[P - \infty]$ is torsion. The set of torsion points includes $\{0, (0, \pm 1), (-\zeta_d^i, 0)\}$; call a torsion point *exceptional* if it does not lie in this list. When $d \geq 7$, Grant and Shaulis prove that there are no exceptional torsion points. When $d = 5$, earlier work of Coleman [15] shows that the only exceptional torsion points are $\{(\zeta_5^i \sqrt[5]{4}, \pm\sqrt{5})\}$.

In Section 5.2, we classify torsion points on curves of the form

$$y^n = x^d + 1$$

where $n, d \geq 2$ are coprime. Denote this curve by $\mathcal{C}_{n,d}$. Let Z be the subgroup of $\operatorname{Aut}(\mathcal{C}_{n,d})$ generated by $(x, y) \mapsto (\zeta_d x, \zeta_n y)$.

Theorem 5.2.73. *Suppose that n, d are coprime integers with $n, d \geq 2$.*

(1) *If $(n, d) = (2, 3)$, then $\mathcal{C}_{2,3}$ is an elliptic curve, so it has infinitely many torsion points.*

(2) *If $(n, d) = (2, 5)$, then the set of exceptional torsion points of $\mathcal{C}_{2,5}$ is the Z-orbit of $(\sqrt[5]{4}, \sqrt{5})$. Each has exact order $(1 - \zeta_5)^3$; in particular, each is killed by 5.*

(3) *If $(n, d) = (4, 3)$, then the set of exceptional torsion points of $\mathcal{C}_{4,3}$ is the Z-orbit of $(2, \sqrt{3})$. Each has exact order $(1 - \zeta_4)(1 - \zeta_3)^2$; in particular, each is killed by 12.*

(4) *If $(n, d) \in \{(3, 2), (5, 2), (3, 4)\}$, then $\mathcal{C}_{n,d} \simeq \mathcal{C}_{d,n}$ via $(x, y) \in \mathcal{C}_{n,d} \mapsto (\zeta_{2n} y, \zeta_{2d} x) \in \mathcal{C}_{d,n}$, so the exceptional torsion points of $\mathcal{C}_{n,d}$ are described by one of Theorem 5.2.73(1), Theorem 5.2.73(2), Theorem 5.2.73(3).*

(5) *Otherwise, $\mathcal{C}_{n,d}$ has no exceptional torsion points.*

The method of proof uses techniques from the “Galois theory of torsion points,” for which there is the excellent survey article of Baker and Ribet [8]. In short, we proceed by contradiction and assume that P is a torsion point of $\mathcal{C}_{n,d}$ that is not among our list. Then,

Step (i) Use the $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-action and the Z-action to produce more torsion points.

Step (ii) Construct relations among the torsion points found in Step (i).

Step (iii) Low-degree relations in Step (ii) produce low-degree maps $\mathcal{C}_{n,d} \to \mathbf{P}^1$. Too many low-degree maps will place upper bounds on the genus (for example, via the Castelnuovo–Severi inequality), which provides a contradiction.

A related result is the following.

Theorem 1.2.2 (Theorem 7.1 of [57]). *Let C be a generic hyperelliptic curve of genus $g > 1$ over a field k of characteristic 0; i.e., the image of the corresponding morphism from* Spec k *to the moduli space over $\mathbf{Q}$ is the generic point. Assume that C has a k-rational Weierstrass point, which is used to embed C into its jacobian J. Then $C(\overline{k}) \cap J(\overline{k})_{\text{tors}}$ consists of only the Weierstrass points.*

Concretely, C is the curve $y^2 = \prod_{i=1}^{2g+1}(x-a_i)$ over $k := \mathbf{Q}(a_1, \cdots, a_{2g+1})$ and it is shown that the only torsion points are $\{\infty, (a_1, 0), \ldots, (a_{2g+1}, 0)\}$. We generalize Theorem 1.2.2 in the following theorem.

Theorem 5.3.1. *Suppose that $n, d \geq 2$ are coprime and satisfy $n + d \geq 7$. Let $\mathscr{C}_n$ be the curve over $k := \mathbf{Q}(a_1, \ldots, a_d)$ defined by the equation*

$$y^n = \prod_{x=1}^{d}(x - a_i).$$

Suppose that $\mathscr{C}_n$ is embedded into its jacobian $\mathscr{J}_n$ using the unique point ∞ at infinity. Points fixed by ζ_n are torsion points of order dividing n.

(1) *If $d \geq 3$, there are no other torsion points defined over $\overline{k}$.*

(2) *If $d = 2$ and $n \neq 5$, the only other torsion points defined over $\overline{k}$ are*

$$\left\{ \left(\frac{a_1 + a_2}{2}, -\zeta_n^i \sqrt[n]{\left(\frac{a_1 - a_2}{2}\right)^2} \right) : 0 \leq i \leq n - 1 \right\}.$$

(3) *If $d = 2$ and $n = 5$, the only other torsion points defined over $\overline{k}$ are*

$$\left\{ \left(\frac{a_1 + a_2}{2}, -\zeta_5^i \sqrt[5]{\left(\frac{a_1 - a_2}{2}\right)^2} \right) : 0 \leq i \leq 4 \right\} \bigcup$$
$$\left\{ \left(\frac{\pm(a_2 - a_1)\sqrt{5} + (a_1 + a_2)}{2}, \zeta_5^i \sqrt[5]{(a_2 - a_1)^2} \right) : 0 \leq i \leq 4 \right\}.$$

The key idea of the proof of Theorem 5.3.1 is a specialization argument; we already know the torsion points when we specialize to $\mathcal{C}_{n,d}$ due to Theorem 5.2.73. A short argument involving specialization to the curve $y^n = x^d + x$ essentially takes care of the rest.

1.2.3 Congruences for Jacobi sums

In Subsection 1.2.2, we mentioned in Step (i) that the core of the proofs required computing $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-action on torsion points. In particular, we needed large Galois action for the rest of the method to succeed.

Suppose that p, q are primes and $\mathcal{J}_{p,q} := \mathrm{Jac}(\mathcal{C}_{p,q})$. One technical ingredient in the proof of Theorem 5.2.73 is the computation of the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_{pq}))$-action on $\mathcal{J}_{p,q}[p]$. This action turns out to factor through a certain p-Kummer extension of $\mathbf{Q}(\zeta_{pq})$. In order to access particular elements of Galois, we turn to explicit Frobenius elements whose eigenvalues are expressible in terms of Jacobi sums. To compute generators for the p-Kummer extension, we need congruences for Jacobi sums. Our goal in Chapter 4 is to obtain the relevant congruences for Jacobi sums.

As we shall see in Section 4.1, congruences for Jacobi sums have many applications in number theory, including but not limited to, quadratic, cubic, and quartic reciprocity. Congruences for Jacobi sums can also be found in [20, 34, 36, 48, 63]. In the language of Anderson and Ihara [2, 1], it seems that our main result is an example of a “higher reciprocity law” for Jacobi sums. We now state our result.

Suppose that ℓ, f are distinct primes and $q \equiv 1 \pmod{\ell f}$ is a prime. Let ζ_ℓ, ζ_f be a primitive ℓth and a primitive fth root of unity in $\mathbf{F}_q$, respectively. For integers i, j satisfying $0 \leq i \leq \ell - 1$ and $1 \leq j \leq f - 1$, define

$$\eta_{i,j} := \prod_{r=0}^{\ell-1} \left(1 - \zeta_f^j \zeta_\ell^r\right)^{\binom{r}{i}} \in \mathbf{F}_q^\times.$$

Theorem 4.2.25. *For $k \in [1, \ell - 1]$, the following are equivalent:*

(1) $J(\ell, f) + 1 \in \pi_\ell^k \mathcal{O}_L$*;*

(2) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, k-2]$ *and* $j \in [1, f-1]$*;*

(3) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, k-2]$ *and* $j \in [1, f/2]$.

In particular, $J(\ell, f) + 1 \in \pi_\ell \mathcal{O}_L$ *always holds.*

1.3 Organization of this thesis

In Chapter 2, we give some background on superelliptic curves. We start in Section 2.1 by setting up some definitions for superelliptic curves. In Section 2.2, we use the Castelnuovo–Severi inequality to obtain bounds on degrees of maps from superelliptic curves to genus zero curves. In Section 2.3, we define the $1 - \zeta$ endomorphism of superelliptic jacobians and sets up the $(1 - \zeta)$-descent map in order to motivate the problem of division by $1 - \zeta$, which is the central object of study in Chapter 3. In Section 2.4, we define torsion points on superelliptic curves, which will be studied in Chapter 5. In Section 2.5, we compute the homology of superelliptic curves; we will use this in Subsection 5.2.1. In Section 2.6, we review the notions of Weierstrass gaps on Riemann surfaces and state Riemann's theorem; we will use these in Section 3.3 and Subsection 5.2.6.

In Chapter 3, we prove our result about division by $1 - \zeta$ on superelliptic curves. We start in Section 3.1 by reviewing Zarhin's work [68] on hyperelliptic curves. In Section 3.2, we state and prove our superelliptic generalization. Our formula implies that for any superelliptic curve $\mathcal{C}$, the intersection of $(1-\zeta)^{-1}\mathcal{C}$ and the theta divisor Θ inside $\mathcal{J} := \mathrm{Jac}(\mathcal{C})$ is contained in $\mathcal{J}[1 - \zeta]$. In Section 3.3, we compute the corresponding intersection multiplicities.

In Chapter 5, we study torsion points on superelliptic curves. We start in Section 5.1 by giving an overview of our new results and how they generalize previous work of Grant and Shaulis [29] and work of Poonen and Stoll [57]. In Section 5.2, we state and prove our classification of torsion points on the superelliptic “Catalan curve” $y^n = x^d + 1$. In Section 5.3, we state and prove our classification of torsion points on a generic superelliptic curve.

The aim of Chapter 4 is to prove a congruence for Jacobi sums which shows up as a key technical ingredient in Section 5.2. We begin in Section 4.1 by recalling the definition of Jacobi sum and explain how they arise when computing point counts of the superelliptic Catalan curve over finite fields. As an application, we calculate the field $\mathbf{Q}(\mu_{15}, \mathcal{J}_{3,5}[2])$. In Section 4.2, we state and prove our new congruence for Jacobi sums.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2

Background on Superelliptic Curves

2.1 Definitions

Definition 2.1.1. Let $n, d \geq 2$ be coprime integers and let K be a field such that $\operatorname{char}(K) \nmid n$. Suppose that $f(x) \in K[x]$ is separable with $\deg(f) = d$. Let $\mathcal{C}$ be the smooth projective model of the affine plane K-curve given by the equation

$$y^n = f(x).$$

Then we call $\mathcal{C}$ a superelliptic curve. When $n = 2$, we call $\mathcal{C}$ a hyperelliptic curve.

Since n and d are coprime, $\mathcal{C}$ has a unique point at infinity, denoted by ∞. The Riemann-Hurwitz formula implies that the genus of $\mathcal{C}$ is

$$g = (n-1)(d-1)/2.$$

Furthermore, suppose that

$$f(x) = (x + \alpha_1) \cdots (x + \alpha_d)$$

where $\alpha_1, \cdots, \alpha_d \in \overline{K}$. Since f is separable, the α_i are distinct.

Let $\mathcal{J}$ be the jacobian of $\mathcal{C}$. Then $\mathcal{C}$ naturally embeds into $\mathcal{J}$ via the Abel–Jacobi map $P \mapsto [P - \infty]$; that is, the point P of $\mathcal{C}$ goes to the divisor class $[P - \infty]$. Given divisors X and Y on $\mathcal{C}$, we write "$X \sim Y$" to indicate that X is linearly equivalent to Y. Moreover, the notation "$X \geq Y$" means that $X - Y$ is effective. Define the "gcd" of a collection of divisors $\{X_i\}$ to be the maximal X such that $X \leq X_i$ for all i. See [25, 56] for more details about curves, their jacobians, and divisor classes.

Given a rational function f on $\mathcal{C}$, we write

$$\operatorname{div}(f) := \sum_P v_P(f) P$$

to denote the principal divisor associated to f and

$$\operatorname{div}_0(f) := \sum_{P \colon v_P(f) \geq 0} v_P(f) P$$

to denote the effective portion of $\operatorname{div}(f)$.

2.2 Some consequences of the Castelnuovo–Severi inequality

Proposition 2.2.1 (Castelnuovo–Severi inequality)**.** *Let k be a perfect field. Let F, F_1, F_2 be function fields of curves over k, of genera g, g_1, g_2, respectively. Suppose that $F_i \subseteq F$ for $i = 1, 2$ and the compositum of F_1 and F_2 in F equals F. Let $d_i = [F : F_i]$ for $i = 1, 2$. Then*

$$g \leq d_1 g_1 + d_2 g_2 + (d_1 - 1)(d_2 - 1).$$

Proof. See Theorem 3.11.3 of [62]. □

As in Section 2.1, assume that $\mathcal{C}$ is the superelliptic curve $y^n = f(x)$ where $\deg f = d$ from now on.

Corollary 2.2.2. *Suppose that $\mathcal{C}$ has a degree d_1 map to a genus zero curve and a degree d_2 map to a genus zero curve. If d_1 and d_2 are coprime, then*

$$(n-1)(d-1)/2 \leq (d_1 - 1)(d_2 - 1).$$

Proof. Let F be the function field of $\mathcal{C}$. Each map gives an embedding of the function field of a genus zero curve into F; let their images be F_1 and F_2. Since $[F : F_i] = d_i$ and the d_i are coprime, the compositum $F_1 F_2$ is F. Since $g = (n-1)(d-1)/2$, we are done by applying Proposition 2.2.1 in this situation with $g_1 = g_2 = 0$. □

Lemma 2.2.3. *If $n, d \geq 3$, then $\mathcal{C}$ cannot have a 2-to-1 map to a genus zero curve.*

Proof. For contradiction, suppose that φ is a map from $\mathcal{C}$ to a genus 0 curve. We also have the degree d map $y : \mathcal{C} \to \mathbf{P}^1$ and the degree n map $x : \mathcal{C} \to \mathbf{P}^1$. Since n and d are coprime, they cannot both be even.

Suppose that n is odd. Applying Corollary 2.2.2 with φ and the x-map yields $(n-1)(d-1)/2 \leq (2-1)(n-1)$, which implies $d \leq 3$, so since $d \geq 3$ by assumption, $d = 3$. Now d is odd, so similarly, $n = 3$, contradicting the assumption that n and d are coprime.

The case d is odd is similar. □

2.3 The $1 - \zeta$ endomorphism and $(1 - \zeta)$-descent

Now we assume that K contains a primitive nth root of unity ζ. We also use ζ to denote the automorphism $\zeta \colon \mathcal{C} \to \mathcal{C}$ which acts on points of $\mathcal{C}$ via

$$\zeta \colon (x, y) \mapsto (x, \zeta y).$$

Then ζ also induces an automorphism of $\mathcal{J}$, which we will also denote by ζ. Then $1 - \zeta$ is an endomorphism of $\mathcal{J}$. In Chapter 3, we aim to invert this endomorphism.

We now state a few properties about the $1 - \zeta$ endomorphism. We adapt the main results of Sections 6.1, 6.2, and 6.3 of [56], which states everything in the hyperelliptic case. However, the extension to superelliptic curves is straightforward and we omit aspects of the proofs that generalize immediately. The case when n is prime is considered in [55, 59].

We need a few more definitions.

$$\begin{aligned}
\overline{K} &:= \text{a separable closure of } K \\
\overline{\mathcal{C}} &:= \mathcal{C} \times_K \overline{K} \\
G &:= \mathrm{Gal}(\overline{K}/K) \\
\pi &:= \text{the } x\text{-coordinate map } \mathcal{C} \to \mathbf{P}^1 \\
\mathcal{W}_i &:= (-\alpha_i, 0) \in \mathcal{C}(\overline{K}) \\
\mathcal{W} &:= \{\mathcal{W}_1, \dots, \mathcal{W}_d\} \\
(\mathbf{Z}/n\mathbf{Z})^{\mathcal{W}} &:= \text{the free } \mathbf{Z}/n\mathbf{Z}\text{-module with basis } \mathcal{W}_1, \dots, \mathcal{W}_d.
\end{aligned}$$

Observe that $\mathcal{W} \cup \{\infty\}$ is the set of ramification points of π over $\overline{K}$ and that $\mathcal{W}$ is a G-module.

Proposition 2.3.1. *There is a split exact sequence of G-modules*

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{Z}/n\mathbf{Z} \arrow[r, "\Delta"] & (\mathbf{Z}/n\mathbf{Z})^{\mathcal{W}} \arrow[r, "s"] & \mathcal{J}[1-\zeta] \arrow[r] & 0
\end{tikzcd}$$

where

$$\Delta(1) = (1,\ \dots,\ 1)$$
$$s(a_1, \dots, a_d) = \sum_{i=1}^{d} a_i[\mathcal{W}_i - \infty].$$

Proof. (c.f. [56], Proposition 6.1.1)

Step 1: *s is well-defined.*

Each point in $\mathcal{W} \cup \{\infty\}$ is fixed by ζ, so $[\mathcal{W}_i - \infty] \in \mathcal{J}[1-\zeta]$. The calculation

$$\mathrm{div}(x + \alpha_i) = n\mathcal{W}_i - n\infty \tag{2.1}$$

shows that the divisor classes $[\mathcal{W}_i - \infty]$ are n-torsion.

Step 2: *Δ and s are G-module homomorphisms.*

This is clear.

Step 3: *$s \circ \Delta = 0$.*

This follows from $\mathrm{div}(y) = \sum_{i=1}^{d} [\mathcal{W}_i - \infty]$.

Step 4: $\ker(s)$ *is generated by* $(1, \dots, 1)$.

Step 5: *s is surjective.*

We modify the proof of Proposition 3.2 in [59] to prove Step 4 and Step 5 simultaneously. Use Div^0 to denote the degree-zero divisors on $\mathcal{C}$ and use Princ to denote the subgroup of principal divisors. The following are exact sequences of $\mathbf{Z}[\zeta]$-modules.

$$\begin{tikzcd}
0 \arrow[r] & \overline{K}^\times \arrow[r] & \overline{K}(\mathcal{C})^\times \arrow[r] & \mathrm{Princ} \arrow[r] & 0; \\
0 \arrow[r] & \mathrm{Princ} \arrow[r] & \mathrm{Div}^0 \arrow[r] & \mathcal{J} \arrow[r] & 0.
\end{tikzcd}$$

We now apply group cohomology with the group $Z_n = \langle \zeta \rangle$.

(i) Since $Z_n \simeq \mathrm{Gal}(\overline{K}(\mathcal{C})/\overline{K}(x))$,

$$H^0(\overline{K}(\mathcal{C})^\times) = \overline{K}(x)^\times \tag{2.2}$$

and Hilbert's Theorem 90 yields

$$H^1(\overline{K}(\mathcal{C})^\times) = 0. \tag{2.3}$$

(ii) Since $\overline{K}^\times$ is a trivial Z_n-module,

$$H^0(\overline{K}^\times) = 0 \tag{2.4}$$

$$H^1(\overline{K}^\times) = \mu_n(\overline{K}) \tag{2.5}$$

$$H^2(\overline{K}^\times) = \overline{K}^\times/\overline{K}^{\times n} = 0. \tag{2.6}$$

Substituting (2.3) and (2.6) into

$$\begin{tikzcd}
H^1(\overline{K}(\mathcal{C})^\times) \arrow[r] & H^1(\mathrm{Princ}) \arrow[r] & H^2(\overline{K}^\times).
\end{tikzcd}$$

yields

$$H^1(\mathrm{Princ}) = 0. \tag{2.7}$$

(iii) Substituting (2.4), (2.2), (2.5), (2.3) into

$$\begin{tikzcd}
H^0(\overline{K}^\times) \arrow[r] & H^0(\overline{K}(C)^\times) \arrow[r] & H^0(\mathrm{Princ}) \arrow[r] & H^1(\overline{K}^\times) \arrow[r] & H^1(\overline{K}(\mathcal{C})^\times)
\end{tikzcd}$$

yields

$$\begin{tikzcd}
0 \arrow[r] & \overline{K}(x)^\times \arrow[r] & H^0(\mathrm{Princ}) \arrow[r] & \mu_n(\overline{K}) \arrow[r] & 0,
\end{tikzcd}$$

so since the image of $\mathrm{div}(y) \in H^0(\mathrm{Princ})$ generates $\mu_n(\overline{K})$,

$$H^0(\mathrm{Princ}) \text{ is generated by } \{\mathrm{div}(y)\} \cup \{\mathrm{div}(u) \colon u \in \overline{K}(x)^\times\}. \tag{2.8}$$

(iv) We substitute (2.7) into the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & H^0(\mathrm{Princ}) \arrow[r] & H^0(\mathrm{Div}^0) \arrow[r] & \mathcal{J}[1-\zeta] \arrow[r] & H^1(\mathrm{Princ})
\end{tikzcd}$$

to obtain

$$\begin{tikzcd}
0 \arrow[r] & H^0(\mathrm{Princ}) \arrow[r] & H^0(\mathrm{Div}^0) \arrow[r] & \mathcal{J}[1-\zeta] \arrow[r] & 0.
\end{tikzcd}$$

The group $H^0(\mathrm{Div}^0)$ consists of the ζ-fixed divisors, so it is generated by $[\mathcal{W}_i - \infty]$ and $\mathrm{Norm}(P - \infty)$ for arbitrary $P \in \mathcal{C}(\overline{K})$. Observe that

$$\begin{aligned} \mathrm{div}(x - x(P)) &= \mathrm{Norm}(P - \infty), \\ \mathrm{div}(y) &= \sum [\mathcal{W}_i - \infty], \end{aligned}$$

so by (2.8), $H^0(\mathrm{Princ})$ is generated by $\sum [\mathcal{W}_i - \infty]$ and $\mathrm{Norm}(P - \infty)$ for arbitrary $P \in \mathcal{C}(\overline{K})$. Therefore, the $[\mathcal{W}_i - \infty]$ generate $\mathcal{J}[1-\zeta] \simeq H^0(\mathrm{Div}^0)/H^0(\mathrm{Princ})$ and the only relation is $\sum [\mathcal{W}_i - \infty] = 0$.

Step 6: *The exact sequence in the statement of Proposition 2.3.1 splits.*

The splitting is given by

$$\begin{tikzcd} (\mathbf{Z}/n\mathbf{Z})^{\mathcal{W}} \arrow[r] & \mathbf{Z}/n\mathbf{Z} \\ (a_1, \ldots, a_d) \arrow[r] & d^{-1} \sum a_i. \end{tikzcd}$$ □

Corollary 2.3.2. *Each element of $\mathcal{J}[1-\zeta]$ has a unique representation of the form*

$$\sum_{i=1}^{d} a_i [\mathcal{W}_i - \infty]$$

for $a_i \in \mathbf{Z}/n\mathbf{Z}$ satisfying $a_1 + \cdots + a_d \equiv 0 \pmod{n}$.

Proof. If $\sum_{i=1}^{d} a_i [\mathcal{W}_i - \infty] = 0$, then Proposition 2.3.1 implies that $a_1 \equiv \cdots \equiv a_d \pmod{n}$, so since $a_1 + \cdots + a_d = 0$ and $(n, d) = 1$, we see that $a_1 \equiv \cdots \equiv a_d \equiv 0 \pmod{n}$; hence the representation is unique.

For existence, Proposition 2.3.1 implies that each element of $\mathcal{J}[1-\zeta]$ has a representation of the form $\sum_{i=1}^{d} a_i' [\mathcal{W}_i - \infty]$ for $a_i' \in \mathbf{Z}/n\mathbf{Z}$, so if we let $a_i = a_i' - d^{-1}(a_1' + \cdots + a_d')$, then $a_1 + \cdots + a_d \equiv 0 \pmod{n}$ and

$$\begin{aligned} \sum_{i=1}^{d} a_i [\mathcal{W}_i - \infty] &= \sum_{i=1}^{d} a_i' [\mathcal{W}_i - \infty] - d^{-1}\left(a_1' + \cdots + a_d'\right) \sum_{i=1}^{d} [\mathcal{W}_i - \infty] \\ &= \sum_{i=1}^{d} a_i' [\mathcal{W}_i - \infty] \end{aligned}$$

since $\sum_{i=1}^{d} [\mathcal{W}_i - \infty] = 0$. □

Define

$$L := K[T]/(f(T)).$$

and

$$\overline{L} := L \otimes_K \overline{K} \simeq \overline{K}[T]/(f(T)) \simeq \prod \overline{K}[T]/(T + \alpha_i) \simeq \overline{K}^{\mathcal{W}}.$$

We have the natural norm homomorphism $\mathrm{Norm} \colon \overline{L} \to \overline{K}$ which sends a tuple $(a_1, \ldots, a_d) \in \overline{K}^{\mathcal{W}}$ to the product $a_1 \cdots a_d \in \overline{K}$. For any ring R, let $\mu_n(R) := \{r \in R \colon r^n = 1\}$.

Proposition 2.3.3. *There is a split exact sequence of G-modules*

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{J}[1-\zeta] \arrow[r] & \mu_n(\overline{L}) \arrow[r, "\text{Norm}"] & \mu_n(\overline{K}) \arrow[r] & 0. \end{tikzcd}$$

Proof. This is a straightforward generalization of Proposition 6.1.2 of [56]. □

Proposition 2.3.4. *We have*

$$H^1(K, \mathcal{J}[1-\zeta]) \simeq \ker\left(\frac{L^\times}{L^{\times n}} \xrightarrow{\text{Norm}} \frac{K^\times}{K^{\times n}}\right). \tag{2.9}$$

Proof. (c.f. Proposition 6.2.1 of [56]). Since the short exact sequence in Proposition 2.3.3 is split, it induces short exact sequences after applying $H^1(K, -)$, so

$$H^1(K, \mathcal{J}[1-\zeta]) \simeq \ker\left(H^1(K, \mu_n(\overline{L})) \xrightarrow{\text{Norm}} H^1(K, \mu_n(\overline{K}))\right). \tag{2.10}$$

Applying an extension of Hilbert's Theorem 90 (exercise 2 on page 152 of [60]) gives the identifications

$$H^1(K, \mu_n(\overline{L})) \simeq L^\times / L^{\times n} \tag{2.11}$$
$$H^1(K, \mu_n(\overline{K})) \simeq K^\times / K^{\times n}, \tag{2.12}$$

so we are done by substituting (2.11) and (2.12) into (2.10). □

Consider the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{J}[1-\zeta] \arrow[r] & \mathcal{J} \arrow[r, "1-\zeta"] & \mathcal{J} \arrow[r] & 0. \end{tikzcd}$$

The first coboundary map in Galois cohomology induces the following injective homomorphism, which we denote by δ.

$$\frac{\mathcal{J}(K)}{(1-\zeta)\mathcal{J}(K)} \overset{\delta}{\hookrightarrow} H^1(K, \mathcal{J}[1-\zeta]).$$

Composing with the isomorphism of (2.9), we obtain an injective homomorphism

$$\frac{\mathcal{J}(K)}{(1-\zeta)\mathcal{J}(K)} \hookrightarrow \ker\left(\frac{L^\times}{L^{\times n}} \xrightarrow{\text{Norm}} \frac{K^\times}{K^{\times n}}\right). \tag{2.13}$$

Theorem 2.3.5.

(1) *Suppose that $P = (x_P, y_P) \in \mathcal{C}(K)$ and that $y_P \neq 0$. The image of*

$$[P - \infty] \in \frac{\mathcal{J}(K)}{(1-\zeta)\mathcal{J}(K)}$$

under the map (2.13) equals

$$[x_P - T] \in \ker\left(\frac{L^\times}{L^{\times n}} \xrightarrow{\text{Norm}} \frac{K^\times}{K^{\times n}}\right).$$

(2) *Suppose that $\mathcal{W}_1, \cdots, \mathcal{W}_d$ are defined over K. The image of*

$$[\mathcal{W}_j - \infty] \in \frac{\mathcal{J}(K)}{(1-\zeta)\mathcal{J}(K)}$$

under the map (2.13) is

$$(-\alpha_j - T) + \prod_{i \neq j}(-\alpha_i - T)^{n-1} \pmod{L^{\times n}}.$$

Proof. This is a straightforward generalization of Proposition 3.3 of [59]; see the computation on page 461 of [59]. □

As is standard, we will call (2.13) the "$x - T$" descent map.

Lemma 2.3.6. *Suppose that $\alpha_1, \ldots, \alpha_d \in K$ and that $P = (x_P, y_P) \in \mathcal{C}(K)$. Then*

$$[P - \infty] \in (1-\zeta)\mathcal{J}(K)$$

if and only if

$$x_P + \alpha_i \in K^n \textit{ for all } i \in [1, d].$$

Proof. Since $\alpha_1, \ldots, \alpha_d \in K$, we have an isomorphism

$$L \simeq \prod_{i=1}^{d} \frac{K[T]}{(T + \alpha_i)} \simeq \prod_{i=1}^{d} K, \tag{2.14}$$

such that the image of $g(T) \in L$ is $(g(-\alpha_1), \ldots, g(-\alpha_d))$.

Since the map of (2.13) is an embedding, $[P - \infty] \in (1-\zeta)\mathcal{J}(K)$ if and only if

$$\text{the image of } [P-\infty] \text{ in } \ker\left(\frac{L^\times}{L^{\times n}} \xrightarrow{\text{Norm}} \frac{K^\times}{K^{\times n}}\right) \text{ is trivial.} \tag{2.15}$$

Case A: $P \notin \mathcal{W}$

Theorem 2.3.5(1) implies (2.15) is equivalent to $[x_P - T] \in L^{\times n}$, which from (2.14) is equivalent to $x_P + \alpha_i \in K^{\times n}$ for $i \in [1, d]$, and since $x_P \notin \{-\alpha_i : i \in [1, d]\}$, this is equivalent to $x_P + \alpha_i \in K^n$ for $i \in [1, d]$.

Case B: $P = \mathcal{W}_j$

Theorem 2.3.5(2) implies (2.15) is equivalent to

$$(-\alpha_j - T) + \prod_{i \neq j}(-\alpha_i - T)^{n-1} \in L^{\times n},$$

which from (2.14) is equivalent to the two conditions

(a) $\alpha_i - \alpha_j \in K^{\times n}$ for all $i \in [1, d] \setminus \{j\}$

(b) $\prod_{i \neq j}(\alpha_j - \alpha_i)^{n-1} \in K^{\times n}$

Note that (a) implies that $K^{\times n} \ni \prod_{i \neq j}(\alpha_i - \alpha_j)^{n-1} = \prod_{i \neq j}(\alpha_j - \alpha_i)^{n-1}$ since $(n-1)(d-1) = 2g$ is even, so (a) implies (b). In particular, the two conditions together are equivalent to $\alpha_i - \alpha_j \in K^n$ for all $i \in [1, d]$. □

Corollary 2.3.7. *Suppose that $P = (x_P, y_P) \in \mathcal{C}(K)$. Let K' be the field*

$$K' = K\left([D] \in \mathcal{J}(\overline{K})\colon (1-\zeta)[D] = [P - \infty]\right).$$

Then

$$K' = K(\sqrt[n]{x_P + \alpha_i}\colon 1 \leq i \leq d).$$

Proof. To avoid confusion, define

$$\begin{aligned} K_1 &:= K\left([D] \in \mathcal{J}(\overline{K})\colon (1-\zeta)[D] = [P - \infty]\right) \\ K_2 &:= K(\sqrt[n]{x_P + \alpha_i}\colon 1 \leq i \leq d). \end{aligned}$$

For any $[D_1] \in \mathcal{J}(\overline{K})$ satisfying $(1-\zeta)[D_1] = [P - \infty]$,

$$\{[D] \in \mathcal{J}(\overline{K})\colon (1-\zeta)[D] = [P-\infty]\} = \{[D_1] + T\colon T \in \mathcal{J}[1-\zeta]\},$$

so

$$K_1 = K\left(\mathcal{J}[1-\zeta], [D_1]\right) = K\left(\alpha_1, \ldots, \alpha_d, [D_1]\right). \tag{2.16}$$

Observe that $\alpha_i = \left(\sqrt[n]{x_P + \alpha_i}\right)^n - x_P$ must lie in K_2, so we may as well assume that K contains $\alpha_1, \ldots, \alpha_d$.

Let $M \supseteq K$ be any extension. By (2.16), $M \supseteq K_1$ if and only if $[P - \infty] \in (1-\zeta)\mathcal{J}(M)$, which by Lemma 2.3.6 holds if and only if $x_P + \alpha_i \in M^n$, which is equivalent to $M \supseteq K_2$. Hence $K_1 = K_2$. □

Hence, our formulas for "division by $1-\zeta$" in Chapter 3 will have coefficients in K'.

Corollary 2.3.8. $K\left(\mathcal{J}[(1-\zeta)^2]\right) = K\left(\alpha_1, \ldots, \alpha_d, \sqrt[n]{\alpha_i - \alpha_j}\colon 1 \leq i, j \leq d\right)$.

Proof. Since

$$K\left(\mathcal{J}[(1-\zeta)]\right) = K\left(\alpha_1, \ldots, \alpha_d\right),$$

we may as well assume that K contains $\alpha_1, \ldots, \alpha_d$. Since the $[\mathcal{W}_i - \infty]$ generate $\mathcal{J}[(1-\zeta)]$,

$$K\left(\mathcal{J}[(1-\zeta)^2]\right) = K\left([D] \in \mathcal{J}(\overline{K}) : (1-\zeta)[D] \in \{[\mathcal{W}_i - \infty]\colon i \in [1, d]\}\right),$$

so we are done by applying Corollary 2.3.7 to $P \in \mathcal{W}$. □

2.4 Torsion points

Suppose that X is a smooth proper geometrically irreducible curve defined over a field K of characteristic zero. Let J be the jacobian variety of X. Suppose that $B \in X(\overline{K})$; then one may define the Abel–Jacobi map with respect to B as follows:

$$\mathrm{AJ}_B\colon P \in X \mapsto [P - B] \in J.$$

Definition 2.4.1. We say that $P \in X(\overline{K})$ is a torsion point of X (with respect to the basepoint B) if its Abel–Jacobi image $[P - B]$ has finite order in $J(\overline{K})$. Denote by $T_B(X)$ the set of torsion points with respect to B.

Raynaud's theorem (formerly the Manin-Mumford conjecture) states that when the genus of X is at least 2, each $T_B(X)$ is finite.

Now suppose that $\mathcal{C}$ is a superelliptic curve of genus at least 2. In Chapter 5, we will determine the finite set $T_\infty(\mathcal{C})$ in two instances: when $\mathcal{C}$ is the "superelliptic Catalan curve" $\mathcal{C}_{n,d}$ given by the equation $y^n = x^d + 1$ and when $\mathcal{C}$ is an appropriate "generic superelliptic curve."

We already saw some examples of torsion points on superelliptic curves in Section 2.3 since (2.1) implies $T_\infty(\mathcal{C}) \supseteq \mathcal{W} \cup \{\infty\}$. The examples in Chapter 5 will demonstrate that it is possible for this containment to be an equality and also possible for it to not to be.

2.5 Homology of superelliptic curves

In this section, we compute $H_1(\mathcal{C}, \mathbf{Z})$ using topology. We will apply results in Section 3 of [51].

Fix $B \in \mathcal{C}(\mathbf{C}) \setminus (\mathcal{W} \cup \{\infty\})$. For each $i \in [1, d]$, choose a loop β_i in $\mathbf{P}^1 \setminus \pi(\mathcal{W} \cup \{\infty\})$ that starts and ends at $\pi(B)$ which goes around $-\alpha_i$ once and does not go around ∞ or $-\alpha_k$ for any $k \neq i$.

Then $\pi_1(\mathbf{P}^1 \setminus \pi(\mathcal{W} \cup \{\infty\}), \pi(B))$ is the free group generated by $\beta_1, \cdots, \beta_d$. Take the subscripts of β modulo d, so that $\beta_{i+d} := \beta_i$. By Galois theory of covering spaces, $\pi_1(\mathcal{C} \setminus (\mathcal{W} \cup \{\infty\}), B)$ is the kernel of the map

$$\nu \colon \pi_1(\mathbf{P}^1 \setminus \pi(\mathcal{W} \cup \{\infty\}), \pi(B)) \to \mathbf{Z}/n\mathbf{Z}$$

which sends each β_i to 1 (mod n). By the van Kampen theorem, $\pi_1(\mathcal{C}, B)$ is a quotient of $\pi_1(\mathcal{C} \setminus (\mathcal{W} \cup \{\infty\}), B)$. In this way, we will view $\pi_1(\mathcal{C}, B)$ as a subquotient of the free group generated by $\beta_1, \cdots, \beta_d$. Recall that $H_1(\mathcal{C}, \mathbf{Z})$ is the abelianization of $\pi_1(\mathcal{C}, B)$, so for each $\beta \in \pi_1(\mathcal{C}, B)$ we will use $[\beta]$ to denote the class of β in $H_1(\mathcal{C}, \mathbf{Z})$.

Definition 2.5.1. For each $i \in [1, d]$, $\beta_i\beta_{i+1}^{-1}$ lies in $\ker \nu$, so for each $j \in [0, n-1]$, define $\psi_{i,j} := \zeta_n^j[\beta_i\beta_{i+1}^{-1}]$. Define $\Psi := \{\psi_{i,j} : i \in [1, d-1] \text{ and } j \in [0, n-2]\}$.

Lemma 2.5.2. *For each $j \in [0, n-1]$,*

$$\psi_{1,j} + \psi_{2,j} + \cdots + \psi_{d,j} = 0.$$

Proof. Observe that $(\beta_1\beta_2^{-1})(\beta_2\beta_3^{-1}) \cdots (\beta_d\beta_1^{-1}) = 1$ $\pi_1(\mathbf{P}^1 \setminus \pi(\mathcal{W} \cup \{\infty\}), \pi(B))$, so taking its image in $H_1(\mathcal{C}, \mathbf{Z})$ yields $\psi_{1,0} + \psi_{2,0} + \cdots + \psi_{d,0} = 0$. Apply ζ_n^j to both sides to finish. □

Lemma 2.5.3. *For each $i \in [1, d]$,*

$$\psi_{i,0} + \psi_{i,1} + \cdots + \psi_{i,n-1} = 0.$$

Proof. This is shown in the proof of Theorem 3.6 of [51]. Briefly, the idea is that there exists a path p_i from $\mathcal{W}_i$ to $\mathcal{W}_{i+1}$ in $\mathcal{C}$ and some $l \in \mathbf{Z}/n\mathbf{Z}$ such that the cycle $\psi_{i,0}$ is homotopic to $(\zeta_n^l p_i)(\zeta_n^{-(l+1)} p_i)^{-1}$, so the sum $\psi_{i,0} + \psi_{i,1} + \cdots + \psi_{i,n-1}$ telescopes to give zero. □

Proposition 2.5.4. *The inclusion $\Psi \subseteq H_1(\mathcal{C}, \mathbf{Z})$ induces an isomorphism*

$$\mathbf{Z}^\Psi \to H_1(\mathcal{C}, \mathbf{Z}).$$

Proof. This is Theorem 3.6 of [51]. □

Definition 2.5.5. Let $S := \mathbf{Z}[T]/(1 + T + \cdots + T^{n-1})$.

Corollary 2.5.6. *$H_1(\mathcal{C}, \mathbf{Z})$ is a free S-module of rank $d-1$ for which T acts as ζ.*

Proof. Lemma 2.5.3 implies that $1 + \zeta + \cdots + \zeta^{n-1}$ acts trivially on all the $\psi_{i,j}$, and since these generate $H_1(\mathcal{C}, \mathbf{Z})$ by Proposition 2.5.4, $H_1(\mathcal{C}, \mathbf{Z})$ is an S-module for which T acts as ζ. From Proposition 2.5.4, $\psi_{1,0}, \ldots, \psi_{d-1,0}$ is an S-module basis for $H_1(\mathcal{C}, \mathbf{Z})$. □

Suppose now that $n = p$ is a prime. Then $S \simeq \mathbf{Z}[\zeta_p]$.

Definition 2.5.7. Define the Tate module $T_p\mathcal{J} \simeq \varprojlim_i \mathcal{J}[p^i]$. Since $T_p\mathcal{J} \simeq H_1(\mathcal{C}, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}_p$, Corollary 2.5.6 gives that $T_p\mathcal{J}$ is a free $\mathbf{Z}_p[\zeta_p]$-module of rank $d-1$. Define $\operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$ to be the ring of endomorphisms of $T_p\mathcal{J}$ that commute with ζ_p. Then

$$\operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}) \simeq M_{d-1}(\mathbf{Z}_p[\zeta_p]).$$

The relation $(1-\zeta_p)^{p-1} \in pS^\times$ implies $\mathcal{J}[p] = \mathcal{J}[(1-\zeta_p)^{p-1}]$, so we also make the identifications

$$T_p\mathcal{J} \simeq \varprojlim_i \mathcal{J}[(1-\zeta_p)^i]$$

and

$$\mathcal{J}[(1-\zeta_p)^i] \simeq T_p\mathcal{J}/(1-\zeta_p)^i.$$

Lemma 2.5.8. *Suppose $\eta \in \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$. Then η kills $\mathcal{J}[(1-\zeta_p)^i]$ if and only if $\eta \in (1-\zeta_p)^i \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$.*

Proof. Note that η kills $\mathcal{J}[(1-\zeta_p)^i]$ if and only if it lies in the kernel of the reduction map

$$\operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}) \longrightarrow \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}\left(T_p\mathcal{J}/(1-\zeta_p)^i\right) = \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}\left(\mathcal{J}[(1-\zeta_p)^i]\right).$$

Since $\operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}) \simeq M_{d-1}(\mathbf{Z}_p[\zeta_p])$ and $\operatorname{End}_{\mathbf{Z}_p[\zeta_p]}\left(T_p\mathcal{J}/(1-\zeta_p)^i\right) \simeq M_{d-1}(\mathbf{Z}_p[\zeta_p]/(1-\zeta_p)^i)$, the kernel of the reduction map is $(1-\zeta_p)^i \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$, so we are done. □

Definition 2.5.9. Define

$$\theta_p \colon \mathbf{Z}_p\left[\operatorname{Gal}\left(\mathbf{Q}(\mu_p, \mathcal{J}[p^\infty])/\mathbf{Q}(\mu_p)\right)\right] \to \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$$

to be the map which sends $\gamma \in \mathbf{Z}_p\left[\operatorname{Gal}\left(\mathbf{Q}(\mu_p, \mathcal{J}[p^\infty])/\mathbf{Q}(\mu_p)\right)\right]$ to its action on $T_p\mathcal{J}$.

Corollary 2.5.10. *An element $\epsilon \in \mathbf{Z}_p\left[\operatorname{Gal}\left(\mathbf{Q}(\mu_p, \mathcal{J}[p^\infty])/\mathbf{Q}(\mu_p)\right)\right]$ kills $\mathcal{J}[(1-\zeta_p)^i]$ if and only if*

$$\theta_p(\epsilon) \in (1-\zeta_p)^i \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}).$$

Proof. This follows from the definition of θ_p and Lemma 2.5.8. □

Lemma 2.5.11. *Let $i \geq 0$ be an integer and $\gamma \in \mathbf{Z}_p\left[\operatorname{Gal}\left(\mathbf{Q}(\mu_p, \mathcal{J}[p^\infty])/\mathbf{Q}(\mu_p)\right)\right]$. Suppose that $\gamma - 1$ kills $\mathcal{J}[(1-\zeta_p)^i]$.*

(1) *For any integer $k \geq 0$, $(\gamma-1)^k$ kills $\mathcal{J}[(1-\zeta_p)^{ik}]$.*

(2) *$\gamma^{p-1} + \gamma^{p-2} + \cdots + 1$ kills $\mathcal{J}[p] = \mathcal{J}[(1-\zeta_p)^{p-1}]$.*

(3) $\gamma^p - 1$ *kills* $\mathcal{J}[(1-\zeta_p)^{p-1+i}]$.

Proof. Define $\varepsilon := \gamma - 1$ and $\eta := \theta_p(\varepsilon)$. Then ε kills $\mathcal{J}[(1-\zeta_p)^i]$, so Corollary 2.5.10 implies that $\eta \in (1-\zeta_p)^i \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$.

(1) Then $\eta^k \in (1-\zeta_p)^{ik} \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J})$, so we are done by Corollary 2.5.10.

(2) Using

$$\gamma^{p-1} + \gamma^{p-2} + \cdots + 1 \in (\gamma - 1)^{p-1} + p\mathbf{Z}[\gamma]$$

yields

$$\theta_p(\gamma^{p-1} + \gamma^{p-2} + \cdots + 1) \in p \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}) = (1-\zeta_p)^{p-1} \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}), \quad (2.17)$$

and we are done by Corollary 2.5.10.

(3) Multiplying both sides of (2.17) by $\theta_p(\gamma - 1)$ yields

$$\theta_p(\gamma^p - 1) \in (1-\zeta_p)^{p-1+i} \operatorname{End}_{\mathbf{Z}_p[\zeta_p]}(T_p\mathcal{J}),$$

so we are done by Corollary 2.5.10. □

Corollary 2.5.12. *For any integer $i \geq 1$, the exponent of the group* $\operatorname{Gal}(\mathbf{Q}(\mu_p, \mathcal{J}[(1-\zeta_p)^{i(p-1)+1}])/\mathbf{Q}(\mu_p, \mathcal{J}[1-\zeta_p]))$ *divides p^i.*

Proof. Suppose that $\gamma \in \operatorname{Gal}(\mathbf{Q}(\mu_p, \mathcal{J}[p^\infty])/\mathbf{Q}(\mu_p, \mathcal{J}[1-\zeta_p]))$. By assumption, $\gamma - 1$ kills $\mathcal{J}[1-\zeta_p]$, so by induction with Lemma 2.5.11(3), $\gamma^{p^i} - 1$ kills $\mathcal{J}[(1-\zeta_p)^{i(p-1)+1}]$, which means that γ^{p^i} acts as the identity on $\mathcal{J}[(1-\zeta_p)^{i(p-1)+1}]$. □

2.6 Weights and gaps on compact Riemann surfaces

Let

X be a compact Riemann surface
g be the genus of X
$\mathscr{O}_X$ be the structure sheaf of X.

For each line bundle $\mathcal{L}$ on X, define

$$h^0(\mathcal{L}) := \dim H^0(\mathcal{L}).$$

Definition 2.6.1. For each point P on X, define $\operatorname{WM}(P)$ to be the set of pole orders at P of meromorphic functions on X which are holomorphic on $X \setminus \{P\}$. Then $\operatorname{WM}(P)$ is a monoid, and it is called the Weierstrass monoid of P.

We define gaps as Nakayashiki does in [53].

Definition 2.6.2. For each point P on X and degree zero line bundle $\mathcal{L}$ on X, define

$$G_P(\mathcal{L}) = \{k \in \mathbf{Z}_{\geq 0} \colon h^0(\mathcal{L}(kP)) = h^0(\mathcal{L}((k-1)P))\}$$

to be the set of gaps for $\mathcal{L}$ at P.

Lemma 2.6.3. *$G_P(\mathcal{L})$ is a subset of $[0, 2g-1]$ of size exactly g.*

Proof. This is a straightforward consequence of the Riemann–Roch theorem. □

Lemma 2.6.4. *$G_P(\mathcal{L}) = \mathbf{Z}_{\geq 0} \setminus \mathrm{WM}(P)$.*

Proof. This follows from the definitions. □

We define weights as Nakayashiki does in [53].

Definition 2.6.5. For each point P on X and degree zero line bundle $\mathcal{L}$ on X, let $k_1 < k_2 < \cdots < k_g$ be the gaps for $\mathcal{L}$ at P. Define

$$\mathrm{wt}_P(\mathcal{L}) := \sum_{i=1}^{g} (k_i - (i-1)).$$

Also, define $\mathrm{wt}(P) := \mathrm{wt}_P(\mathscr{O}_X)$. A point P on X is called a Weierstrass point if $\mathrm{wt}(P) \geq 1$.

Theorem 2.6.6. *Suppose that $g \geq 1$. Then*

$$\sum_{P \in X} \mathrm{wt}(P) = g^3 - g.$$

In particular, X only has finitely many Weierstrass points.

Proof. See equation (5.11.1) on page 88 of [21]. □

Chapter 3

Division by $1 - \zeta$ on Superelliptic Curves and Jacobians

The main goal of this chapter is to understand how to invert the $1-\zeta$ endomorphism defined in Section 2.3. We first give an introduction to this problem in Section 3.1 and highlight how earlier work by Zarhin in the hyperelliptic case provided the motivation to generalize to the superelliptic setting. In Section 3.2, we state and prove the formula for division by $1-\zeta$. In Section 3.3, we study a problem motivated by our formula; namely, we study the intersection of $(1-\zeta)^{-1}\mathcal{C}$ and the theta divisor Θ inside the jacobian.

Sections 3.1 to 3.3 form the content of my paper [4] on division by $1-\zeta$.

3.1 Introduction and motivation

As in Section 2.1, we let $\mathcal{C}$ be the superelliptic curve given by the equation

$$y^n = (x+\alpha_1)\cdots(x+\alpha_d) \tag{3.1}$$

where $n, d \geq 2$ are coprime and $\alpha_1, \cdots, \alpha_d \in K$ where K is a field with $\operatorname{char}(K) \nmid n$. We will furthermore assume that K is algebraically closed. Every point of the jacobian $\mathcal{J}$ of $\mathcal{C}$ can be represented as $[D - g\infty]$ for some effective degree g divisor D.

Our goal is to provide formulas for "division by $1-\zeta$" for points of $\mathcal{C}$. For a fixed point P on $\mathcal{C}$, we seek to find rational functions on $\mathcal{C}$ which cut out an effective degree g divisor D satisfying the property

$$(1-\zeta)[D - g\infty] = [P - \infty],$$

which is equivalent to

$$(1-\zeta)D \sim P - \infty.$$

When $n = 2$, the curve $\mathcal{C}$ is hyperelliptic and we seek to divide by $1-\zeta = 2$. Let ι be the hyperelliptic involution on $\mathcal{C}$. In [68], Zarhin provides formulas for division by 2 in the hyperelliptic setting. His formulas are written in terms of the Mumford representation (see [52], page 3.17). More specifically, Zarhin finds two rational functions f_1, f_2 on $\mathcal{C}$ for which there exist effective degree g divisors D and E such that

$$\begin{aligned}\operatorname{div}(f_1) &= D + \iota(E) - 2g\infty\\ \operatorname{div}(f_2) &= D + E + \iota(P) - (2g+1)\infty.\end{aligned}$$

From this, we get $(1-\iota)D \sim P - \infty$, or equivalently, $2(D - g\infty) \sim P - \infty$.

In the superelliptic setting, there is no direct analogue of the Mumford representation. Instead, we find n rational functions $f_1, \cdots, f_n$ such that for some degree g effective divisors D and E,

$$\begin{aligned} \operatorname{div}(f_1) &= D + \zeta^{-1}(E) - 2g\infty \\ \operatorname{div}(f_2) &= D + \zeta^{-2}(E) + \zeta^{-1}(P) - (2g+1)\infty \\ &\vdots \\ \operatorname{div}(f_n) &= D + E + \zeta^{-1}(P) + \zeta^{-2}(P) + \cdots + \zeta^{-(n-1)}(P) - (2g+n-1)\infty. \end{aligned}$$

The first two equations yield $\operatorname{div}(f_1/\zeta^* f_2) = (1-\zeta)D - (P - \infty)$, so $(1-\zeta)D \sim P - \infty$. Moreover, we will show that

$$D = \gcd_{1 \le j \le n} \operatorname{div}_0 f_j. \tag{3.2}$$

When $n = 2$, our formulas reduce to Zarhin's. However, Zarhin's techniques do not readily extend from $n = 2$ to general n; the main obstruction is the lack of a Mumford representation when $n > 2$.

- When $n = 2$, it is the case that

  $$\begin{aligned} f_1 &= U(x) \\ f_2 &= y - V(x) \end{aligned}$$

  for some $U(x), V(x) \in K[x]$ satisfying $U | (V^2 - \prod(x + \alpha_i))$. (The pair (U, V) is called the Mumford representation of D.) Assuming that f_1, f_2 are in this special format greatly simplifies the rest of the computation. However, even when $n = 3$, one cannot assume that f_1, f_2 will have this special form; one must work with the more general $f_i = U_{0,i}(x) + U_{1,i}(x)y + U_{2,i}(x)y^2$.

- There are other ways to represent divisor classes on superelliptic curves; see [26] for another possible representation and algorithms for computations in that representation. However, we were not able to use their representation for our formulas.

As an application, we can divide any point $(-\alpha_i, 0)$ by $1 - \zeta$. Since $[(-\alpha_i, 0) - \infty]$ generate $\mathcal{J}[1-\zeta]$, we obtain generators for $\mathcal{J}[(1-\zeta)^2]$. In particular, for the case $n = 3$ we know that $\mathcal{J}[(1-\zeta_3)^2] = \mathcal{J}[3]$, so our formulas give a representation for each 3-torsion divisor class on a trigonal superelliptic curve. We also hope that our formula can be used to perform explicit descent and compute the rational points on some superelliptic curves.

One curious aspect of this formula is that whenever $P \neq \infty$, no D satisfying $(1-\zeta)D \sim P - \infty$ lands on the theta divisor Θ of the jacobian. That is, $\mathcal{C} \cap (1-\zeta)\Theta = \{0\}$, which implies that $(1-\zeta)^{-1}\mathcal{C} \cap \Theta = \mathcal{J}[1-\zeta]$. In Section 3.3, we compute the intersection multiplicity of $(1-\zeta)^{-1}\mathcal{C}$ and Θ at each point of $\mathcal{J}[1-\zeta]$.

3.2 The formula for division by $1 - \zeta$

Let T be an $n \times n$ matrix. Let $T_{i,j}$ denote the (i,j)-th entry of T. The indices i, j will be taken modulo n to make sense of expressions of the form $T_{-1,2n}$ (this means $T_{n-1,n}$). The notation

$T^{(i,j)}$ represents the submatrix of T obtained by removing the ith row and jth column of T. The notation "$\operatorname{adj} T$" stands for the adjugate matrix of T; its (i,j)-th entry is defined to be $(\operatorname{adj} T)_{i,j} := (-1)^{i+j} \det T^{(j,i)}$. It is a fact that $T(\operatorname{adj} T) = (\operatorname{adj} T)T = (\det T)I_n$.

3.2.1 Statement of main result

Suppose that $P = (a, b)$. By translating P and $\mathcal{C}$, we may assume that the the x-coordinate of P is zero; that is, $P = (0, b)$. Choose r_i such that

$$\begin{aligned} r_i^n &= \alpha_i \\ \prod r_i &= b \end{aligned}$$

Let s_j be the jth elementary symmetric polynomial evaluated on the r_i, where the convention is that $s_m = 0$ for $m \notin [0, d]$. (So $b = s_d$.) For each $\ell \in \mathbf{Z}$, define

$$A_\ell(x) = \sum_{k \geq 0} (-1)^{(n-1)k} s_{\ell - nk} x^k \in K[x].$$

Let A, Z, M, N be the following $n \times n$ matrices with entries in $K[x, y]$.

$$\begin{aligned}
A &:= \begin{bmatrix} A_d & A_{d-1} & \cdots & A_{d-n+2} & A_{d-n+1} \\ A_{d+1} & A_d & \cdots & A_{d-n+3} & A_{d-n+2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ A_{d+n-2} & A_{d+n-3} & \cdots & A_d & A_{d-1} \\ A_{d+n-1} & A_{d+n-2} & \cdots & A_{d+1} & A_d \end{bmatrix} \\
Z &:= \begin{bmatrix} \zeta^0 & 0 & \cdots & 0 & 0 \\ 0 & \zeta^{-1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \zeta^{-(n-2)} & 0 \\ 0 & 0 & \cdots & 0 & \zeta^{-(n-1)} \end{bmatrix} \\
M &:= A - yZ \\
N &:= \operatorname{adj} M.
\end{aligned}$$

The goal is to prove the following theorem.

Theorem 3.2.1. *The divisor*

$$D := \gcd_{1 \leq j \leq n} \operatorname{div}_0 N_{1,j}$$

is an effective degree g divisor on $\mathcal{C}$ such that

$$(1 - \zeta)D \sim P - \infty.$$

Proof. We will prove this theorem at the end of Subsection 3.2.3. □

3.2.2 Computational lemmas

As mentioned before, view the entries of A, Z, M, N as elements of $K[x, y]$.

Definition 3.2.2. Define σ to be the automorphism of $K[x, y]$ over $K[x]$ sending $y \mapsto \zeta^{-1} y$.

Now we seek to understand how σ operates on the entries of M and N. We do so in Lemma 3.2.4, and the following notation makes it easier to express those relations.

Definition 3.2.3. Define

$$\delta_{i,j} := \begin{cases} 1 & \text{if } i \equiv j \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3.2.4. *We have*

$$M_{i+1,j+1} = ((-1)^{n-1}x)^{\delta_{j,n}-\delta_{i,n}} \cdot \sigma M_{i,j} \tag{3.3}$$

$$N_{i+1,j+1} = ((-1)^{n-1}x)^{\delta_{j,n}-\delta_{i,n}} \cdot \sigma N_{i,j}. \tag{3.4}$$

Equivalently, if C is the $n \times n$ matrix

$$C = \left[\begin{array}{c|c} 0 & I_{n-1} \\ \hline (-1)^{n-1}x & 0 \end{array}\right]$$

(where the I_{n-1} block is the $(n-1) \times (n-1)$ identity matrix) then

$$\sigma M = CMC^{-1} \tag{3.5}$$

$$\sigma N = CNC^{-1}. \tag{3.6}$$

Proof. (3.3) follows from the fact that for $\ell \geq d+1$, $A_\ell = (-1)^{n-1}xA_{\ell-n}$ and the fact that for $i, j \in [1, n]$, $M_{i,j} = A_{d+i-j} - \delta_{i,j}\zeta^{1-i}y$. (3.3) is equivalent to (3.5). Both σ and conjugation commute with the adj-operation, so taking adj of both sides of (3.5) gives (3.6). (3.6) is equivalent to (3.4). □

Lemma 3.2.5. *$N_{1,j}$ lies in the ideal*

$$\left(x, \prod_{k=j}^{n-1}(y - \zeta^k s_d)\right)$$

of $K[x, y]$.

Proof. Since $A_\ell \equiv 0 \pmod{x}$ whenever $\ell \notin [0, d]$,

$$N_{1,j} = (-1)^{j+1} \det M^{(j,1)} \equiv (-1)^{j+1} \det \left[\begin{array}{c|c} U & V \\ \hline 0 & W \end{array}\right] \pmod{x},$$

where

$$U = \begin{bmatrix} s_{d-1} & s_{d-2} & s_{d-3} & \cdots & s_{d-j+1} \\ s_d - \zeta^{-1}y & s_{d-1} & s_{d-2} & \cdots & s_{d-j+2} \\ & s_d - \zeta^{-2}y & s_{d-1} & \cdots & s_{d-j+3} \\ & & \ddots & \ddots & \vdots \\ & & & s_d - \zeta^{2-j}y & s_{d-1} \end{bmatrix}$$

$$V = \begin{bmatrix} s_{d-j} & s_{d-j-1} & \cdots & s_{d-n+1} \\ s_{d-j+1} & s_{d-j} & \cdots & s_{d-n+2} \\ s_{d-j+2} & s_{d-j+1} & \cdots & s_{d-n+3} \\ \vdots & \vdots & \ddots & \vdots \\ s_{d-2} & s_{d-3} & \cdots & s_{d-n+j-1} \end{bmatrix}$$

$$W = \begin{bmatrix} s_d - \zeta^{-j}y & s_{d-1} & \cdots & s_{d-n+j+1} \\ & s_d - \zeta^{-(j+1)}y & \cdots & s_{d-n+j+2} \\ & & \ddots & \vdots \\ & & & s_d - \zeta^{-(n-1)}y \end{bmatrix}.$$

Hence $N_{1,j} \equiv (-1)^{j+1} \det U \cdot \det W \pmod{x}$. Since W is upper triangular,

$$\det W = \prod_{k=j}^{n-1} (s_d - \zeta^{-k}y)$$

which implies

$$N_{1,j} \equiv (-1)^{j+1} (\det U) \cdot \prod_{k=j}^{n-1} (s_d - \zeta^{-k}y) \pmod{x},$$

as desired. □

We work in a slightly larger ring L where the eigenvalues of A are defined.

Definition 3.2.6. Define

$$L := K[x, y, T]/(T^n + (-1)^n x) \simeq K[y, T].$$

Then σ extends to an automorphism of L over $K[T]$ sending $y \mapsto \zeta^{-1}y$.

Lemma 3.2.7. *For $1 \leq k \leq n$, define*

$$\lambda_k := \prod_{i=1}^{d} (r_i + \zeta^k T) \in K[T] \subseteq L.$$

Then the λ_k are distinct and form the complete set of eigenvalues of A.

Proof. The λ_k are distinct because the T^d-coefficient of λ_k is ζ^{kd} and d is coprime to n.

Now we show that each λ_k is an eigenvalue of A by showing that

$$v_k := \begin{bmatrix} 1 & \zeta^k T & \cdots & \zeta^{(n-1)k} T^{n-1} \end{bmatrix}^\top$$

is a corresponding eigenvector. We will show that $Av_k = \lambda_k v_k$ by showing that their jth entries for $j \in [1, n]$ are the same. This will complete the proof.

We first compute $(Av_k)_j$ as follows:

$$\begin{aligned}
(Av_k)_j &= \sum_{i=1}^{n} \zeta^{k(i-1)} T^{i-1} A_{d+j-i} \\
&= \sum_{i=1}^{n} \zeta^{k(i-1)} T^{i-1} \sum_{m \geq 0} (-1)^{(n-1)m} s_{d+j-i-mn} x^m \\
&= \sum_{i=1}^{n} \zeta^{k(i-1)} T^{i-1} \sum_{m \geq 0} (-1)^{(n-1)m} s_{d+j-i-mn} (-(-T)^n)^m \\
&= \sum_{i=1}^{n} \sum_{m \geq 0} \zeta^{k(i-1)} s_{d+j-i-mn} T^{i+nm-1} \\
&= \sum_{i=1}^{n} \sum_{m \geq 0} \zeta^{k(i+mn-1)} s_{d+j-i-mn} T^{i+nm-1}.
\end{aligned}$$

As i and m vary in the range $1 \leq i \leq n$ and $m \geq 0$, the quantity $i + mn$ represents every positive integer exactly once. However, $s_{d+j-i-mn}$ will be zero whenever $i + mn - j \notin [0, d]$. So we may perform the change of coordinates $a := i + mn - j$ and turn this into the finite sum

$$\begin{aligned}
(Av_k)_j &= \sum_{a=0}^{d} \zeta^{k(j+a-1)} s_{d-a} T^{j+a-1} \\
&= \zeta^{k(j-1)} T^{j-1} \sum_{a=0}^{d} (\zeta^k T)^a s_{d-a} \\
&= \zeta^{k(j-1)} T^{j-1} \sum_{a=0}^{d} (\zeta^k T)^a \sum_{i_1 < i_2 < \cdots < i_{d-a}} r_{i_1} \cdots r_{i_{d-a}} \\
&= \zeta^{k(j-1)} T^{j-1} \prod_{i=1}^{d} (r_i + \zeta^k T) \\
&= \zeta^{k(j-1)} T^{j-1} \lambda_k \\
&= (\lambda_k v_k)_j.
\end{aligned}$$

Hence, v_k is a nonzero eigenvector of A with eigenvalue λ_k. Since we have shown that $\{\lambda_k\}$ are n distinct eigenvalues of A, they must be all the eigenvalues of A. □

Lemma 3.2.8. *We have*

$$\det A = \prod_{i=1}^{d} (x + \alpha_i)$$

$$\det M = \prod_{i=1}^{d} (x + \alpha_i) - y^n.$$

Proof. The first equality comes directly from multiplying the eigenvalues computed in Lemma 3.2.7 and by observing that

$$\prod_{k=0}^{n-1}(r_i + \zeta^k T) = r_i^n - (-1)^n T^n = \alpha_i + x.$$

Observe that $\det M$ is a polynomial in y of degree n with leading term $\prod_{i=0}^{n-1}(-\zeta^i y) = -y^n$. By taking the determinant of both sides of (3.5), we deduce that $\det M$ is invariant under σ. Therefore $\det M$ can have no other terms in y, so it is of the form $\det M = q(x) - y^n$. By plugging in $y = 0$ we see that $q(x) = \det(A - 0 \cdot Z) = \det A$, so the rest comes from the computation of $\det A$. □

Lemma 3.2.9. *The determinant of any 2×2 submatrix of N is divisible by $y^n - (x + \alpha_1) \cdots (x + \alpha_d)$.*

Proof. We show this for the submatrix of N obtained by taking the $\{i, k\}$ rows and $\{j, \ell\}$ columns. Let F be the submatrix of M obtained by deleting the $\{i, k\}$ rows and $\{j, \ell\}$ columns. Apply Jacobi's complementary minor formula (Theorem 2.5.2 of [58]) with these rows and columns to obtain

$$\det \begin{bmatrix} N_{i,j} & N_{i,\ell} \\ N_{k,j} & N_{k,\ell} \end{bmatrix} = \pm \det M \cdot \det F.$$

Since $-\det M = y^n - (x + \alpha_1) \cdots (x + \alpha_d)$ by Lemma 3.2.8, we are done. □

For $t_x, t_y \in K$, define $A(t_x), M(t_x, t_y), N(t_x, t_y) \in M_n(K)$ by substituting $x = t_x$ and $y = t_y$.

Lemma 3.2.10. *For any $t_x \in K$, the rank of $A(t_x)$ is at least $n - 1$.*

Proof. The eigenvalues of A were computed in Lemma 3.2.7. Define $T(t_x) \in K$ to be an nth root of $-(-1)^n t_x$ and define $\lambda_k(t_x) := \prod_{i=1}^{d}(r_i + \zeta^k T(t_x))$. Then the eigenvalues of $A(t_x)$ are $\lambda_1(t_x), \cdots, \lambda_n(t_x)$.

Case A: $t_x \neq 0$

Suppose that $\lambda_k(t_x) = \lambda_\ell(t_x) = 0$. Then there exist i, j such that $T(t_x) = -\zeta^{-k} r_i$ and $T(t_x) = -\zeta^{-\ell} r_j$. Hence $\alpha_i = r_i^n = (-T(t_x))^n = r_j^n = \alpha_j$, so $i = j$. Then $\zeta^k = -r_i T(t_x)^{-1} = -r_j T(t_x)^{-1} = \zeta^\ell$, so $k = \ell$. Hence $\lambda_k(t_x) = 0$ for at most one k, so the rank of $A(t_x)$ is at least $n - 1$.

Case B: $t_x = 0$

Since $A_\ell \equiv s_\ell \pmod{x}$ for all ℓ and $s_\ell = 0$ when $\ell \notin [0, d]$, we see that $A(0)$ is an upper triangular matrix with diagonal entries s_d and "super-diagonal" entries s_{d-1}. If $s_d \neq 0$, then $A(0)$ is invertible and we are done. If $s_d = 0$ and $s_{d-1} \neq 0$, then the submatrix obtained by deleting the first column and last row of $A(0)$ is upper-triangular with diagonal entries s_{d-1} and is therefore invertible, implying that the rank of $A(0)$ is at least $n - 1$.

If $s_d = s_{d-1} = 0$, then at least two of the $\{\alpha_1, \cdots, \alpha_d\}$ are zero, which is impossible. □

Lemma 3.2.11. *For any $t_x, t_y \in K$, the matrix $N(t_x, t_y)$ is not zero.*

Proof. We will use the following fact: for each square matrix F, the rank of F is at most $n-2$ if and only if $\operatorname{adj} F = 0$.

Consider the matrix $N + \sigma N + \cdots + \sigma^{n-1}N$; it is σ-invariant and it involves powers of y only between 0 and $n-1$, so it is independent of y. Hence

$$(N + \sigma N + \cdots + \sigma^{n-1}N)(x,y) = (N + \sigma N + \cdots + \sigma^{n-1}N)(x,0) = nN(x,0) = n \operatorname{adj} A(x). \tag{3.7}$$

Case A: $t_x \neq 0$

If $N(t_x, t_y) = 0$, then (3.4) implies that $(\sigma^i N)(t_x, t_y) = 0$ for all i. Substituting this into (3.7) yields

$$0 = (N + \sigma N + \cdots + \sigma^{n-1}N)(t_x, t_y) = n \operatorname{adj} A(t_x).$$

Since $\operatorname{char}(K) \nmid n$, we may divide by n on both sides to see that $\operatorname{adj} A(t_x) = 0$, so $A(t_x)$ has rank at most $n-2$, contradicting Lemma 3.2.10.

Case B: $t_x = 0$

Then the matrix $M(0, t_y) = A(0) - t_y Z$ is upper triangular with diagonal entries $s_d - t_y \zeta^i$. If $t_y \neq 0$, then these diagonal entries will all be distinct; in particular, at most one is zero, so $M(0, t_y)$ will have rank at least $n-1$. If $t_y = 0$, then $M(0, t_y) = A(0)$ and we are done by Lemma 3.2.10. □

3.2.3 Main proof

Vanishing loci of $N_{i,j}$

We will now view entries of N as elements of the function field $K(\mathcal{C})$ when writing expressions of the form $\operatorname{div} N_{i,j}$ or $\operatorname{div}_0 N_{i,j}$. In order to make sense of such expressions, we need to check that $N_{i,j}$ reduces to a *nonzero* element of $K(\mathcal{C})$.

Lemma 3.2.12.

(1) $-v_\infty(x) = n$

(2) $-v_\infty(y) = d$

(3) *For* $\ell \geq 0$,
$$-v_\infty(A_\ell) \leq \ell, \tag{3.8}$$
with equality holding if and only if $\ell \equiv 0 \pmod{n}$.

(4) *For* $1 \leq u, v \leq n$,
$$-v_\infty(M_{u,v}) \leq d + u - v, \tag{3.9}$$
with equality holding if and only if $u = v$ *or* $u - v \equiv -d \pmod{n}$.

Proof. Lemma 3.2.12(1) and Lemma 3.2.12(2) follow directly from (3.1), the equation of $\mathcal{C}$.

(3) Since
$$A_\ell = \sum_{k \geq 0} (-1)^{(n-1)k} s_{\ell - nk} x^k$$

and $s_{\ell-nk} = 0$ whenever $\ell - nk \notin [0, d]$,

$$\deg_x A_\ell \le \lfloor \ell/n \rfloor,$$

so by Lemma 3.2.12(1),

$$-v_\infty(A_\ell) \le n\lfloor \ell/n \rfloor.$$

Since $n\lfloor \ell/n \rfloor \le \ell$, we obtain (3.8). If $\ell \not\equiv 0 \pmod{n}$, then $n\lfloor \ell/n \rfloor < \ell$, so the inequality must be strict. If $\ell \equiv 0 \pmod{n}$, then the $x^{\ell/n}$-coefficient of A_ℓ is $(-1)^{(n-1)\ell/n} s_0 = (-1)^{(n-1)\ell/n} \neq 0$ and hence $-v_\infty(A_\ell) = n(\ell/n) = \ell$.

(4) Since

$$M_{u,v} = A_{d+u-v} - \zeta^{1-u}\delta_{u,v} y,$$

(3.9) follows by breaking into cases depending on whether or not $u = v$ and then applying Lemma 3.2.12(2) and Lemma 3.2.12(3). If $u \neq v$, then $M_{u,v} = A_{d+u-v}$, so Lemma 3.2.12(3) gives that equality holds in (3.9) if and only if $u - v \equiv -d \pmod{n}$. If $u = v$, then equality holds in (3.9) because $-v_\infty(A_d) < d$ (since $d \not\equiv 0 \pmod{n}$) and $-v_\infty(y) = d$. □

Lemma 3.2.13.

(1) $-v_\infty(N_{i,j}) = 2g + (i-1) + (n-j)$. *In particular,* $N_{i,j} \neq 0$.

(2) *Each* $N_{i,j}$ *satisfies*

$$\operatorname{div}_0 N_{i,j} \ge \sum_{k=j-n}^{i-2} \zeta^k P$$

Proof.

(1) For every integer k, let $L(k\infty)$ be the subspace of $K(\mathcal{C})$ consisting of meromorphic functions that are holomorphic everywhere except at ∞ and whose valuation at ∞ is at least $-k$. Define $\ell := 2g + (i-1) + (n-j)$.

Label the rows of $M^{(j,i)}$ by $\{1, 2, \ldots, j-1, j+1, \ldots, n\}$ and the columns of $M^{(j,i)}$ by $\{1, 2, \ldots, i-1, i+1, \ldots, n\}$. We remind the reader that row and column indices are taken modulo n.

Expand $\det M^{(j,i)}$ as a sum over permutations

$$\det M^{(j,i)} = \sum_{\substack{\sigma \in S_n \\ \sigma(j) = i}} \operatorname{sign}(\sigma) M_{1,\sigma(1)} \cdots M_{j-1,\sigma(j-1)} M_{j+1,\sigma(j+1)} \cdots M_{n,\sigma(n)}.$$

For every $\sigma \in S_n$ satisfying $\sigma(j) = i$, apply (3.9) to the summand corresponding to σ

to get

$$\begin{aligned}
&-v_\infty(\operatorname{sign}(\sigma)M_{1,\sigma(1)}\cdots M_{j-1,\sigma(j-1)}M_{j+1,\sigma(j+1)}\cdots M_{n,\sigma(n)})\\
&=\sum_{\substack{1\le k\le n\\ k\ne j}} -v_\infty(M_{k,\sigma(k)})\\
&\le \sum_{\substack{1\le k\le n\\ k\ne j}} (d+k-\sigma(k))\\
&=-(d+j-i)+\sum_{k=1}^{n} d+(k-\sigma(k))\\
&=-(d+j-i)+nd\\
&=\ell
\end{aligned}$$

and hence

$$-v_\infty(\det M^{(j,i)})\le \ell.$$

Furthermore, $\det M^{(j,i)} \pmod{L((\ell-1)\infty)}$ will be unchanged if we replace the (u,v)-entry of M with zero whenever we do not have equality in (3.9). That is, the $n\times n$ matrix $\widetilde{M}$ defined by

$$\widetilde{M}_{u,v}=\begin{cases} M_{u,v} & \text{if } u-v\in\{0,-d\} \pmod{n},\\ 0 & \text{otherwise}\end{cases}$$

satisfies

$$\det M^{(j,i)}\equiv \det \widetilde{M}^{(j,i)} \pmod{L((\ell-1)\infty)}. \tag{3.10}$$

Claim. Let $u\in[0,n-1]$ be the unique integer such that $j\equiv i+ud \pmod{n}$. Then

$$\begin{aligned}\det \widetilde{M}^{(j,i)} &= \pm M_{i,i+d}\cdots M_{i+(u-1)d,i+ud}\\ &\quad\times M_{i+(u+1)d,i+(u+1)d}\cdots M_{i+(n-1)d,i+(n-1)d}\end{aligned} \tag{3.11}$$

Proof of claim. Write

$$\det \widetilde{M}^{(j,i)}=\sum_{\substack{\sigma\in S_n\\ \sigma(j)=i}} \operatorname{sign}(\sigma)\widetilde{M}_{1,\sigma(1)}\cdots \widetilde{M}_{j-1,\sigma(j-1)}\widetilde{M}_{j+1,\sigma(j+1)}\cdots\widetilde{M}_{n,\sigma(n)}. \tag{3.12}$$

Suppose that $\sigma\in S_n$ satisfies $\sigma(j)=i$ and $\sigma(m)\in\{m,m+d\} \pmod{n}$ for every $m\in[1,n]\setminus\{j\}$; otherwise, the summand corresponding to σ in (3.12) is zero. Then:

(i) $\sigma(i+kd)=i+(k+1)d$ for $k\in[0,u-1]$.
Induct on k. If $k=0$, then $u\ne 0$ and hence $i\ne j=\sigma^{-1}(i)$, so $\sigma(i)\ne i$. Since $\sigma(i)\in\{i,i+d\}$, this forces $\sigma(i)=i+d$. Now suppose that $\sigma(i+kd)=i+(k+1)d$ for some $k\in[0,u-2]$. Then $i+(k+1)d\ne i+kd=\sigma^{-1}(i+(k+1)d)$, so $\sigma(i+(k+1)d)\ne i+(k+1)d$. Since $\sigma(i+(k+1)d)\in\{i+(k+1)d,i+(k+2)d\}$, this forces $\sigma(i+(k+1)d)=i+(k+2)d$.

(ii) $\sigma(i-kd)=i-kd$ for $k\in[1,n-u-1]$.

Induct on k. If $k=1$, then $u \neq n-1$ and hence $i-d \neq j = \sigma^{-1}(i)$, so $\sigma(i-d) \neq i$. Since $\sigma(i-d) \in \{i-d, i\}$, this forces $\sigma(i-d) = i-d$. Now suppose that $\sigma(i-kd) = i-kd$ for some $k \in [1, n-u-2]$. Then $i-(k+1)d \neq i-kd = \sigma^{-1}(i-kd)$, so $\sigma(i-(k+1)d) \neq i-kd$. Since $\sigma(i-(k+1)d) \in \{i-(k+1)d, i-kd\}$, this forces $\sigma(i-(k+1)d) = i-(k+1)d$.

Properties (i) and (ii) uniquely determine σ, so **the proof of the claim is complete.**

We attain the upper bound in (3.9) for every term on the right hand side of (3.11), so applying $-v_\infty$ to both sides of (3.11) yields

$$-v_\infty(\det \widetilde{M}^{(j,i)}) = \ell. \tag{3.13}$$

Combining (3.10) and (3.13), we conclude that $-v_\infty(\det M^{(j,i)}) = \ell$. Since $N_{i,j} = (-1)^{i+j} \det M^{(j,i)}$, we are done.

(2) Use (3.4) to reduce to the case $i=1$. Lemma 3.2.13(1) implies that $N_{1,j}$ is not identically zero, so applying div_0 to Lemma 3.2.5 (which makes sense since polynomials in x, y can only have poles at ∞) yields

$$\begin{aligned}\operatorname{div}_0 N_{1,j} &\geq \gcd\left\{\operatorname{div}_0 x, \operatorname{div}_0 \prod_{k=j-n}^{-1} (y - \zeta^k s_d)\right\} \\ &\geq \sum_{k=j-n}^{-1} \zeta^k P.\end{aligned}$$

□

Definition 3.2.14. Define

$$\begin{aligned}Q_{i,j} &:= \operatorname{div}_0 N_{i,j} - \sum_{k=j-n}^{i-2} \zeta^k P \\ D_i &:= \gcd_{1\leq k\leq n} Q_{i,k} \\ E_j &:= Q_{1,j} - \gcd_{1\leq k \leq n} Q_{1,k}\end{aligned}$$

By Lemma 3.2.13(2), $Q_{i,j} \geq 0$, so $D_i \geq 0$. Also, $E_j \geq 0$.

Our first task is to translate the lemmas in the previous section to results about the effective divisors $Q_{i,j}, D_i, E_j$.

Lemma 3.2.15. *The effective divisors D_i, E_j satisfy*

$$D_i + E_j = Q_{i,j}.$$

Proof. Apply Lemma 3.2.9 to the 2×2 submatrix of N obtained by taking rows $\{i,k\}$ and columns $\{j,\ell\}$ to obtain the equality $N_{i,j}N_{k,\ell} = N_{i,\ell}N_{k,j}$ *as elements of* $K(\mathcal{C})$. Since the entries of N have poles only at ∞, we may take div_0 of both sides to obtain $\operatorname{div}_0 N_{i,j} + \operatorname{div}_0 N_{k,\ell} = \operatorname{div}_0 N_{i,\ell} + \operatorname{div}_0 N_{k,j}$. Therefore,

$$Q_{i,j} + Q_{k,\ell} = Q_{i,\ell} + Q_{k,j}, \tag{3.14}$$

and hence

$$\begin{aligned}
D_i + E_j &= \left(\gcd_{1\le k\le n} Q_{i,k} \right) + Q_{1,j} - \gcd_{1\le k\le n} Q_{1,k} \\
&= \left(\gcd_{1\le k\le n} (Q_{i,1} - Q_{1,1} + Q_{1,k}) \right) + Q_{1,j} - \gcd_{1\le k\le n} Q_{1,k} && \text{(by (3.14))} \\
&= (Q_{i,1} - Q_{1,1}) + \left(\gcd_{1\le k\le n} Q_{1,k} \right) + Q_{1,j} - \gcd_{1\le k\le n} Q_{1,k} \\
&= Q_{i,1} - Q_{1,1} + Q_{1,j} \\
&= Q_{i,j} && \text{(by (3.14))}. \qquad \square
\end{aligned}$$

Lemma 3.2.16. *We have*

$$\gcd_{1\le i\le n} D_i = \gcd_{1\le j\le n} E_j = 0.$$

Proof. If there existed a point R on $\mathcal{C}$ such that $Q_{i,j} \ge R$ for all i, j, then all the $N_{i,j}$ would vanish on R, which contradicts Lemma 3.2.11. Therefore $0 \ge \gcd_{i,j} Q_{i,j}$. Since each $Q_{i,j}$ is effective, we get the reverse inequality $\gcd_{i,j} Q_{i,j} \ge 0$. Hence

$$\gcd_{1\le i,j\le n} Q_{i,j} = 0.$$

Taking $\gcd_{1\le i,j\le n}$ of both sides of Lemma 3.2.15 yields

$$\gcd_{1\le i\le n} D_i + \gcd_{1\le j\le n} E_j = \gcd_{1\le i,j\le n} Q_{i,j}.$$

Therefore $\gcd_i D_i$ and $\gcd_j E_j$ are effective divisors whose sum is 0; hence both are 0. □

Lemma 3.2.17. *For* $1 \le i, j \le n$,

$$D_i = \zeta^{i-1} D_1 \tag{3.15}$$
$$E_j = \zeta^{j-1} E_1. \tag{3.16}$$

Proof. Taking div_0 of both sides of (3.4) yields

$$\operatorname{div}_0 N_{i+1,j+1} = (\delta_{j,n} - \delta_{i,n}) \operatorname{div}_0 x + \zeta \operatorname{div}_0 N_{i,j}.$$

Breaking into cases depending whether $i = n$ and/or $j = n$, we obtain

$$Q_{i+1,j+1} = \zeta Q_{i,j},$$

so by Lemma 3.2.15,

$$D_{i+1} + E_{j+1} = \zeta D_i + \zeta E_j. \tag{3.17}$$

Taking $\gcd_j$ of both sides and applying Lemma 3.2.16 yields $D_{i+1} = \zeta D_i$. Similarly, $E_{j+1} = \zeta E_j$. □

Definition 3.2.18. Define $D := D_1$ and $E := E_1$.

We summarize our work in the following proposition.

Proposition 3.2.19. *For $1 \leq i, j \leq n$,*

$$\operatorname{div}_0 N_{i,j} = \zeta^{i-1}D + \zeta^{j-1}E + \left(\sum_{k=j-n}^{i-2} \zeta^k P\right)$$

$$\operatorname{div} N_{i,j} = \zeta^{i-1}D + \zeta^{j-1}E + \left(\sum_{k=j-n}^{i-2} \zeta^k P\right) - (2g + (i-1) + (n-j))\infty.$$

Proof. Combine Definition 3.2.14, Lemma 3.2.15, (3.15), (3.16), and Lemma 3.2.13(1). □

Orders at infinity

Lemma 3.2.20. *There is no $f \in K(\mathcal{C})^\times$ having a pole only at ∞ such that the pole order at ∞ is $nd - n - d$.*

Proof. Let R be the ring $R = K[x,y]/(y^n - \prod_{i=1}^d (x + \alpha_i))$; this is the affine coordinate ring of $\mathcal{C} \setminus \{\infty\}$. A K-basis for R is $\{x^a y^b \colon 0 \leq a \text{ and } 0 \leq b \leq n-1\}$; since Lemma 3.2.12(1) and Lemma 3.2.12(2) implies $-v_\infty(x^a y^b) = na + db$ and $(d,n) = 1$ by assumption, each element of this basis has a different order pole at ∞. Therefore, the order of the pole at ∞ of any element of R is of the form $na + db$ for nonnegative a, b.

Suppose that $f \in K(\mathcal{C})^\times$ has a pole only at ∞. Then $f \in R$. From the previous paragraph, we have $-v_\infty(f) = na + db$ for nonnegative a, b. If it were the case that $na + db = nd - n - d$, then $a \equiv -1 \pmod{d}$ and $b \equiv -1 \pmod{n}$, so by nonnegativity of a, b we conclude that $a \geq d - 1$ and $b \geq n - 1$. But then

$$nd - n - d = na + db \geq (nd - n) + (nd - d) = 2nd - n - d,$$

which is a contradiction. □

Definition 3.2.21. Define the Abel–Jacobi map

$$\begin{tikzcd} \mathcal{C} \arrow[r, "\mathrm{AJ}_\infty"] & \mathcal{J} \\ P \arrow[r, mapsto] & {[P - \infty].} \end{tikzcd}$$

For every $r \geq 1$, this induces a map $\mathcal{C}^r \to \mathcal{J}^r$. Denote by W_r the image of the composite morphism $\mathcal{C}^r \to \mathcal{J}^r \to \mathcal{J}$, where the second map is the addition map. We define $\Theta := W_{g-1}$ to be the theta divisor.

Lemma 3.2.22. *For $r \geq g$, $W_r = \mathcal{J}$.*

Proof. It is a simple consequence of the Riemann-Roch theorem that any degree zero divisor on $\mathcal{C}$ has a representation as $[P_1 + \ldots + P_g - g\infty]$ for points $P_1, \ldots, P_g$ of $\mathcal{C}$. □

The $n = 2$ case of the following theorem is Theorem 2.5 of [68] (on page 506).

Theorem 3.2.23.

(1) *The intersection of $\mathrm{AJ}_\infty(\mathcal{C})$ and $(1-\zeta)\Theta$ in $\mathcal{J}$ is exactly $\{0\}$.*

(2) *The intersection of* $\mathrm{AJ}_\infty(\mathcal{C})$ *and* $(\zeta - 1)\Theta$ *in* $\mathcal{J}$ *is also exactly* $\{0\}$.

Proof.

(1) Suppose that there were some $P \in \mathcal{C} \setminus \{\infty\}$ such that $[P - \infty]$ lies in $(1 - \zeta)\Theta$. Then there is some effective divisor D of degree $r \leq g - 1$ such that $(1 - \zeta)D \sim P - \infty$ and $v_\infty(D) = 0$. By Lemma 3.2.22, there is an effective divisor E of degree $s \leq g$ such that $D + E \sim (r + s)\infty$ and $v_\infty(E) = 0$. Define

$$t := (nd - n - d) - (r + s).$$

Since $r \leq g - 1$, $s \leq g$, and $nd - n - d = 2g - 1$, we have $t \geq 0$. Consider the divisor

$$F := \zeta^t D + E + \sum_{i=0}^{t-1} \zeta^i P.$$

Since $E \sim (r + s)\infty - D$ and $P \sim \infty + (1 - \zeta)D$,

$$\begin{aligned} F &\sim \zeta^t D - D + \sum_{i=0}^{t-1}(\zeta^i D - \zeta^{i+1} D) + (r + s + t)\infty \\ &= 0 + (r + s + t)\infty \\ &= (nd - n - d)\infty. \end{aligned}$$

Since $v_\infty(F) = 0$ and $F \sim (nd - n - d)\infty$, this contradicts Lemma 3.2.20.

(2) Applying the previous part to ζ^{-1} instead of ζ, we see that $\mathcal{C} \cap (1 - \zeta^{-1})\Theta = \{0\}$. Applying ζ to both sides gives $\zeta\mathcal{C} \cap (\zeta - 1)\Theta = \{0\}$. Since $\zeta\mathcal{C} = \mathcal{C}$, we are done. □

Lemma 3.2.24.

(1) *We have* $\deg D = \deg E = g$.

(2) *The support of* D *avoids* $\{(-\alpha_1, 0), \cdots, (-\alpha_d, 0), \infty\}$. *The same holds for* E.

Proof.

(1) Applying Proposition 3.2.19 gives

$$\begin{aligned} \operatorname{div}(N_{1,n}/\zeta^* N_{1,n-1}) &= \operatorname{div} N_{1,n} - \zeta \operatorname{div} N_{1,n-1} \\ &= (D + \zeta^{-1}E - 2g\infty) - \zeta(D + \zeta^{-2}E + \zeta^{-1}P - (2g + 1)\infty) \\ &= (1 - \zeta)D - (P - \infty). \end{aligned} \tag{3.18}$$

Suppose that $\deg D \leq g - 1$. Then $[(1 - \zeta)D] \in (1 - \zeta)\Theta$. Since $[(1 - \zeta)D]$ also equals $[P - \infty] \in \mathrm{AJ}_\infty(\mathcal{C}) \setminus \{0\}$, we have found an element of $(1 - \zeta)\Theta \cap (\mathrm{AJ}_\infty(\mathcal{C}) \setminus \{0\})$, contradicting Theorem 3.2.23(1). Hence,

$$\deg D \geq g. \tag{3.19}$$

Similarly,

$$\operatorname{div}(\zeta^{2*} N_{1,n}/\zeta^* N_{2,n}) = (\zeta - 1)E - (\zeta P - \infty), \tag{3.20}$$

and a similar argument with Theorem 3.2.23(2) implies

$$\deg E \geq g. \tag{3.21}$$

Taking $i = 1$ and $j = n$ in Proposition 3.2.19 yields $D + \zeta^{-1}E - 2g\infty = \operatorname{div} N_{1,n}$, so

$$\deg D + \deg E = 2g. \tag{3.22}$$

Combining (3.19), (3.21), and (3.22) gives $\deg D = \deg E = g$, as desired.

(2) Suppose that $R \in \{(-\alpha_1, 0), \cdots, (-\alpha_d, 0), \infty\}$ and $D \geq R$. Then $(1-\zeta)[D-R] \in (1-\zeta)\Theta$. Since $R \in \mathcal{J}[1-\zeta]$, (3.18) implies that $(1-\zeta)[D-R] = [P-\infty] \in \mathrm{AJ}_\infty(\mathcal{C}) \setminus \{0\}$. Hence $(1-\zeta)[D-R]$ is an element of $(1-\zeta)\Theta \cap \mathrm{AJ}_\infty(\mathcal{C}) \setminus \{0\}$, contradicting Theorem 3.2.23(1).

Similarly, if $S \in \{(-\alpha_1, 0), \cdots, (-\alpha_d, 0), \infty\}$ and $E \geq S$, then (3.20) implies $(\zeta - 1)[E-S] = [\zeta P - \infty]$, so $(\zeta-1)[E-S] \in (\zeta-1)\Theta \cap \mathrm{AJ}_\infty(\mathcal{C}) \setminus \{0\}$, contradicting Theorem 3.2.23(2). □

Corollary 3.2.25. *$P \not\leq E$.*

Proof. Suppose that $P \leq E$ and let $E' = \zeta^{-1}E - \zeta^{-1}P$, so that by Lemma 3.2.24(1), E' is an effective degree $g-1$ divisor on $\mathcal{C}$ satisfying

$$\begin{aligned}
(\zeta-1)E' &= (\zeta-1)\zeta^{-1}E - (\zeta-1)\zeta^{-1}P \\
&\sim (\zeta-1)(2g\infty - D) - (P - \zeta^{-1}P) \quad \text{(by Proposition 3.2.19 with } i=1, j=n) \\
&= (1-\zeta)(D) - (P-\zeta^{-1}P) \\
&\sim P - \infty - (P - \zeta^{-1}P) \qquad \text{(by (3.18))} \\
&= \zeta^{-1}P - \infty,
\end{aligned}$$

which contradicts Theorem 3.2.23(2). □

Proof of Theorem 3.2.1. We wish to check $\gcd_{1\leq j\leq n} \operatorname{div}_0 N_{1,j} = D$. Applying Proposition 3.2.19 with $i = 1$ and then taking gcd yields

$$\gcd_{1\leq j\leq n} \operatorname{div}_0 N_{1,j} \geq D.$$

For contradiction, suppose that Q is a point on $\mathcal{C}$ such that

$$Q \leq \gcd_{1\leq j\leq n} (\operatorname{div}_0 N_{1,j} - D).$$

Then Proposition 3.2.19 implies that for all $j \in [1, n]$,

$$Q \leq \zeta^{j-1}E + \sum_{k=j-n}^{-1} \zeta^k P = E_j + \sum_{k=j-n}^{-1} \zeta^k P \tag{3.23}$$

by (3.16). By Lemma 3.2.16, there must be some $u \in [1, n]$ such that $Q \not\leq E_u$. Then

$$Q \leq \sum_{k=u-n}^{-1} \zeta^k P,$$

so $Q = \zeta^v P$ for some $v \in [u - n, -1]$.

Case A: P is fixed by ζ

Then $Q = \zeta^v P = P$. Substituting $j = n$ into (3.23) produces $Q \leq \zeta^{n-1} E$, so we conclude that $P = \zeta P = \zeta Q \leq E$, contradicting Corollary 3.2.25.

Case B: P is not fixed by ζ

Then the $\zeta^k P$ are distinct. Applying (3.23) with $j = v + n + 1$ then gives

$$Q \leq \zeta^v E + \sum_{k=v+1}^{-1} \zeta^k P$$

Since $Q = \zeta^v P$ and the $\zeta^k P$ are distinct, we conclude that $\zeta^v P \leq \zeta^v E$, which implies that $P \leq E$, again contradicting Corollary 3.2.25. □

3.2.4 Varying the choice of r_i

Recall that $(r_1, \cdots, r_d)$ is any d-tuple of elements of K satisfying

$$\begin{gathered} r_i^n = \alpha_i \\ \prod r_i = b. \end{gathered}$$

Write $\mathbf{r}$ to denote $(r_1, \ldots, r_d)$. Since the D in Theorem 3.2.1 depends on the choice of $\mathbf{r}$, we will denote it $D_{\mathbf{r}}$ from now on. For $\mathbf{a} = (a_1, \ldots, a_d) \in (\mathbf{Z}/n\mathbf{Z})^d$, write $\zeta^{\mathbf{a}}\mathbf{r}$ to denote $(\zeta^{a_1} r_1, \ldots, \zeta^{a_d} r_d)$.

Applying Theorem 3.2.1 with b replaced by $\zeta^{-(a_1+\cdots+a_d)} b$ and $\mathbf{r}$ replaced with $\zeta^{-\mathbf{a}}\mathbf{r}$, we obtain

$$(1 - \zeta) D_{\zeta^{-\mathbf{a}}\mathbf{r}} \sim \zeta^{-(a_1+\cdots+a_d)} P - \infty,$$

so

$$D_{\mathbf{r}} - \zeta^{a_1+\ldots+a_d} D_{\zeta^{-\mathbf{a}}\mathbf{r}} \in \mathcal{J}[1 - \zeta].$$

Our goal is to write down $D_{\mathbf{r}} - \zeta^{a_1+\ldots+a_d} D_{\zeta^{-\mathbf{a}}\mathbf{r}}$ in terms of a basis for $\mathcal{J}[1 - \zeta]$. First, we recall our description of $\mathcal{J}[1 - \zeta]$.

Definition 3.2.26. For $1 \leq i \leq d$, define $P_i := (-\alpha_i, 0) \in \mathcal{C}(K)$.

Lemma 3.2.27. *The map*

$$\begin{gathered} (\mathbf{Z}/n\mathbf{Z})^d \longrightarrow \mathcal{J}[1 - \zeta] \\ \mathbf{a} \longmapsto \textstyle\sum_{i=1}^d a_i [P_i - \infty] \end{gathered}$$

is surjective and its kernel is generated by $(1, \ldots, 1)$.

Proof. This is Proposition 2.3.1. □

The $n = 2$ case of the following theorem is Theorem 1.1 of [69].

Theorem 3.2.28. *For each* $\mathbf{a} \in (\mathbf{Z}/n\mathbf{Z})^d$,

$$D_{\mathbf{r}} - \zeta^{a_1+\ldots+a_d} D_{\zeta^{-\mathbf{a}}\mathbf{r}} \sim a_1P_1 + \cdots + a_dP_d - \left(\sum a_j\right)\infty.$$

Proof. By induction, it suffices to treat the case $\mathbf{a} = (1, 0, \ldots, 0)$. To do so, we will first reformulate Theorem 3.2.1 in terms of a family over an open subset of $\mathbf{A}^d_K = \operatorname{Spec} K[r_1, \ldots, r_d]$.

Let U be the open subset of $\mathbf{A}^d_K = \operatorname{Spec} K[r_1, \ldots, r_d]$ given by removing every hyperplane of the form $r_i^n = r_j^n$. Let $\mathscr{C}$ be the smooth proper family of superelliptic curves over U given by the equation

$$y^n = \prod_{i=1}^{d} (x + r_i^n).$$

The morphism $\mathscr{C} \to U$ admits two sections of interest to us; these are the "∞ section" which sends $(r_1, \ldots, r_d)$ to the point at ∞ on the fiber and the "P section" which sends $(r_1, \ldots, r_d)$ to the point $(0, r_1 \cdots r_d)$ on the fiber. Let $\mathscr{J}$ be the relative jacobian of the family $\mathscr{C}$ and embed $\mathscr{C}$ into $\mathscr{J}$ using the Abel–Jacobi map induced by the ∞ section (denoted AJ_∞). We seek to compare the two sections $D_{\mathbf{r}}$ and $\zeta D_{\zeta^{-\mathbf{a}}\mathbf{r}}$ of the map $\mathscr{J} \to U$. Here is a diagram representing all the morphisms considered thus far.

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "\mathrm{AJ}_\infty"] \arrow[dr] & \mathscr{J} \arrow[r, "1-\zeta"] \arrow[d] & \mathscr{J} \arrow[dl] \\
& U \arrow[ul, dotted, bend left=20, "\infty"'] \arrow[ul, dotted, bend left=50, "P"] \arrow[u, dotted, bend left=15, "D_{\mathbf{r}}"] \arrow[u, dotted, bend right=15, "\zeta D_{\zeta^{-\mathbf{a}}\mathbf{r}}"'] &
\end{tikzcd}$$

In this language, Theorem 3.2.1 says that the following two morphisms are the same:

$$\begin{tikzcd}
U \arrow[r, "P"] & \mathscr{C} \arrow[r, "\mathrm{AJ}_\infty"] & \mathscr{J} \\
U \arrow[r, "D_{\mathbf{r}}"] & \mathscr{J} \arrow[r, "1-\zeta"] & \mathscr{J}
\end{tikzcd}$$

The map $\mathscr{J}[1-\zeta] \to U$ is smooth of relative dimension 0; it is étale. Consider the sections $\gamma, \gamma' \colon U \to \mathscr{J}[1-\zeta]$ given in coordinates by

$$\gamma\colon (r_1, \ldots, r_d) \mapsto D_{\mathbf{r}} - \zeta D_{\zeta^{-\mathbf{a}}\mathbf{r}}$$
$$\gamma'\colon (r_1, \ldots, r_d) \mapsto (0, 0) - \infty.$$

We wish to show that $\gamma = \gamma'$. Let H_1 be the hyperplane of U cut out by $r_1 = 0$. On H_1, we know that $\zeta^{-\mathbf{a}}\mathbf{r} = \mathbf{r}$, so

$$D_{\mathbf{r}} - \zeta D_{\zeta^{-\mathbf{a}}\mathbf{r}} = (1-\zeta)D_{\mathbf{r}} \sim (0, 0) - \infty.$$

Therefore, the sections γ, γ' agree on the nonempty closed subset H_1. Every section of an unramified cover with connected base is uniquely determined by its image on a single point (by Corollaire 5.3, Exposé 1 of SGA 1 [32]), so $\gamma = \gamma'$. □

Remark 3.2.29. Lemma 3.2.27 and Theorem 3.2.28 together imply that our formula in Theorem 3.2.1 produces every effective degree g divisor D satisfying $(1-\zeta)D \sim P - \infty$.

3.3 Application to the intersection of $(1-\zeta)^{-1}\,\mathrm{AJ}_\infty(\mathcal{C})$ and Θ

Let $\mathcal{C}' := (1-\zeta)^{-1}\,\mathrm{AJ}_\infty(\mathcal{C})$. Theorem 3.2.23(1) implies that the intersection of $\mathcal{C}'$ and Θ is contained in $\mathcal{J}[1-\zeta]$. In this section, we will compute the intersection multiplicities at each intersection point. We will work over the complex numbers; that is, $K = \mathbf{C}$.

We identify points of $\mathcal{J}$ with degree zero divisor classes, and in this section, we use D to denote degree zero divisor classes (as opposed to effective divisors).

For each $P \in \mathcal{C}$ and $D \in \mathcal{J}$, recall the definition of the gap set $G_P(D)$ from Section 2.6.

Definition 3.3.1. Suppose that $D \in \mathcal{J}$. By Lemma 2.6.3, $G_\infty(D) = \{b_1, \cdots, b_g\}$ for integers $0 \leq b_1 < b_2 < \ldots < b_g \leq 2g-1$. As on page 5204 of [53], define the partition

$$\lambda_D := (b_g - (g-1),\; b_{g-1} - (g-2),\; \ldots,\; b_1 - 0)\,.$$

Let $|\lambda_D|$ be the size of λ_D, i.e.,

$$|\lambda_D| = \sum_{i=1}^{g} (b_i - (i-1))\,.$$

Definition 3.3.2. For each $D \in \mathcal{J}$, define $i(D)$ to be the intersection multiplicity of $\mathcal{C}'$ and Θ at D.

The main theorem of this section is the following.

Theorem 3.3.3. *For each $D \in \mathcal{C}' \cap \Theta$,*

$$i(D) = |\lambda_D|.$$

Proof. This theorem will be proved at the end of the section. □

Remark 3.3.4. We warn the reader that textbooks on Riemann surfaces [21, 50] usually define gaps differently. For a point P and linear system Q on a Riemann surface X, let $G'_P(Q)$ be the gaps for Q at P defined in [50]. Let $\omega_{\mathcal{C}}$ be the canonical bundle on $\mathcal{C}$ and $\mathcal{L}$ be the line bundle associated to D. Applying the Riemann–Roch theorem shows that the relationship between the two notions of gaps is

$$G_P(D) = \{b \in \mathbf{Z}_{\geq 0} : b+1 \in G'_P(\omega_C \otimes \mathcal{L}^{-1} \otimes \mathscr{O}_X(P))\}$$

and that $|\lambda_D|$ coincides with the inflectionary weight for $\omega_C \otimes \mathcal{L}^{-1} \otimes \mathscr{O}_X(\infty)$ at ∞.

Definition 3.3.5. Define the ring

$$R := \mathbf{Z}[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]/(X_1^n - 1, \ldots, X_d^n - 1, X_1 \cdots X_d - 1).$$

Then R has a natural basis of the form $\{X_1^{a_1} \cdots X_{d-1}^{a_{d-1}} \colon 0 \le a_j < n\}$. Define

$$\mathrm{pr}_{a_1,\dots,a_{d-1}} \colon R \to \mathbf{Z}$$

to be the map that extracts the $X_1^{a_1} \cdots X_{d-1}^{a_{d-1}}$-coefficient. By abuse of notation, we also use $\mathrm{pr}_{a_1,\dots,a_{d-1}}$ to denote the same map, but tensored up to $\mathbf{Z}[\![T]\!]$:

$$\mathrm{pr}_{a_1,\dots,a_{d-1}} \colon R[\![T]\!] \to \mathbf{Z}[\![T]\!].$$

Finally, define

$$\begin{aligned} \rho &:= (1 + T^n + T^{2n} + \cdots) \cdot \prod_{i=1}^{d} (1 + X_i T + \cdots + X_i^{n-1} T^{n-1}) && \in R[\![T]\!] \\ \rho_{a_1,\dots,a_{d-1}} &:= \mathrm{pr}_{a_1,\dots,a_{d-1}}(\rho) && \in \mathbf{Z}[\![T]\!]. \end{aligned}$$

Lemma 3.3.6. *Every element of $\mathcal{J}[1-\zeta]$ has a unique representation of the form*

$$[a_1 P_1 + \cdots + a_{d-1} P_{d-1} - (a_1 + \cdots + a_{d-1})\,\infty]$$

for some $0 \le a_j < n$.

Proof. This is an immediate consequence of Lemma 3.2.27. □

Proposition 3.3.7. *Suppose that $D = [a_1 P_1 + \cdots + a_{d-1} P_{d-1} - (a_1 + \cdots + a_{d-1})\,\infty]$ for some $0 \le a_j < n$. Then*

$$\rho_{a_1,\dots,a_{d-1}} = \sum_{i \in \mathbf{Z}_{\ge 0} \setminus G_\infty(D)} T^i.$$

Proof. Writing out an explicit sum for ρ gives

$$\begin{aligned} \rho &= \left(\sum_{m \ge 0} (T^n)^m \right) \left(\sum_{e_1,\dots,e_d=0}^{n-1} X_1^{e_1} \cdots X_d^{e_d} T^{e_1 + \cdots + e_n} \right) \\ &= \sum_{e_1,\dots,e_d \in [0,n-1], m \ge 0} X_1^{e_1} \cdots X_d^{e_d} T^{e_1 + \cdots + e_d + nm} \end{aligned}$$

Using the relation $X_1 X_2 \cdots X_d = 1$, the above equals

$$\rho = \sum_{e_1,\dots,e_d \in [0,n-1], m \ge 0} X_1^{e_1 - e_d} \cdots X_{d-1}^{e_{d-1} - e_d} T^{(e_1 - e_d) + \ldots + (e_{d-1} - e_d) + nm + de_d},$$

Perform the change of variables $a_j \equiv e_j - e_d \pmod{n}$ where $a_j \in [0, n-1]$. Then using $e_j = a_j + e_d - n\lfloor \frac{a_j + e_d}{n} \rfloor$ and $X_1^n = \cdots = X_{d-1}^n = 1$ yields

$$\rho = \sum_{a_1,\dots,a_{d-1},e_d \in [0,n-1], m \ge 0} X_1^{a_1} \cdots X_{d-1}^{a_{d-1}} T^{(\sum a_j) + n\left(m - \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) + de_d}$$

and hence

$$\rho_{a_1,\dots,a_{d-1}} = \sum_{e_d=0}^{n-1} \sum_{m \ge 0} T^{(\sum a_j) + n\left(m - \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor \right) + de_d} \tag{3.24}$$

For each $e_d \in [0, n-1]$ and $m \geq 0$, define

$$E(e_d, m) := \left(\sum a_j\right) + n\left(m - \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor\right) + de_d \tag{3.25}$$

to be the exponents arising in (3.24). Observe that $E(e_d, m)$ uniquely determines e_d and m:

$$e_d \equiv d^{-1}\left(E(e_d, m) - \sum a_j\right) \pmod{n} \tag{3.26}$$

uniquely determines e_d, and then

$$m = \frac{1}{n}\left(E(e_d, m) - \left(\sum a_j\right) - de_d\right) + \sum \left\lfloor \frac{a_j + e_d}{n} \right\rfloor$$

is uniquely determined by e_d and $E(e_d, m)$. Therefore, no terms in (3.24) combine.

For each pair (e_d, m), the function

$$h_{e_d,m} := y^{e_d}(x + \alpha_d)^m \prod_{j=1}^{d-1} (x + \alpha_j)^{-\left\lfloor \frac{a_j + e_d}{n} \right\rfloor}$$

satisfies

$$\begin{aligned}\operatorname{div}(h_{e_d,m}) = (nm + e_d)P_d + \sum_{j=1}^{d-1} \left(e_d - n\left\lfloor \frac{a_j + e_d}{n} \right\rfloor\right) P_j \\ - \left(n\left(m - \sum_{j=1}^{d-1} \left\lfloor \frac{a_j + e_d}{n} \right\rfloor\right) + de_d\right)\infty\end{aligned}$$

and hence

$$\begin{aligned}&\operatorname{div}(h_{e_d}, m) + \sum_{i=1}^{d-1} a_i(P_i - \infty) \\ &= (nm + e_d)P_d + \sum_{j=1}^{d-1} \left(a_j + e_d - n\left\lfloor \frac{a_j + e_d}{n} \right\rfloor\right) P_j \\ &\quad - \left(\left(\sum_{j=1}^{d-1} a_j\right) + n\left(m - \sum_{j=1}^{d-1} \left\lfloor \frac{a_j + e_d}{n} \right\rfloor\right) + de_d\right)\infty \\ &= (nm + e_d)P_d + \left(\sum_{j=1}^{d-1} \left(a_j + e_d - n\left\lfloor \frac{a_j + e_d}{n} \right\rfloor\right) P_j\right) - E(e_d, m)\infty,\end{aligned}$$

so $E(e_d, m) \in \mathbf{Z}_{\geq 0} \setminus G_\infty(D)$.

To finish, we must check the reverse containment $\mathbf{Z}_{\geq 0} \setminus G_\infty(D) \subseteq \{E(e_d, m) : e_d \in [0, n-1], m \geq 0\}$. By Lemma 3.3.8 below, $\#\{E(e_d, m) : e_d \in [0, n-1], m \geq 0\} = g$, so we are done. □

Lemma 3.3.8. *Suppose that $a_1, \cdots, a_{d-1} \in [0, n-1]$. For each $e_d \in [0, n-1]$ and $m \geq 0$,* *define $E(e_d, m)$ as in (3.25). Define*

$$S := \{E(e_d, m) \colon e_d \in [0, n-1], m \geq 0\}\,.$$

Then $\mathbf{Z}_{\geq 0} \setminus S$ is finite and has size exactly g.

Proof. For any real number x, define $\{x\} := x - \lfloor x \rfloor$. Let $a_d = 0$ and $a = \sum_{j=1}^{d} a_j$. For each $e \in [0, n-1]$, (3.26) implies that the subset of S congruent to $a + de \pmod{n}$ is

$$\begin{aligned}
S_e &:= \{E(e, m) : m \geq 0\} \\
&= E(e, 0) + n\mathbf{Z}_{\geq 0} \\
&= \left(\left(\sum_{j=1}^{d-1} a_j \right) - n \left(\sum_{j=1}^{d-1} \left\lfloor \frac{a_j + e}{n} \right\rfloor \right) + de \right) + n\mathbf{Z}_{\geq 0} \\
&= \left(\sum_{j=1}^{d} \left(a_j + e - n \left\lfloor \frac{a_j + e}{n} \right\rfloor \right) \right) + n\mathbf{Z}_{\geq 0} \qquad \text{(since } a_d = 0\text{)} \\
&= \left(n \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\} \right) + n\mathbf{Z}_{\geq 0}.
\end{aligned}$$

Therefore,

$$\#\left((\mathbf{Z}_{\geq 0} \cap (a + de + n\mathbf{Z})) \setminus S_e \right) = \left\lfloor \sum_{j=1}^{d} \left\{ \frac{a_j + e}{n} \right\} \right\rfloor$$

and hence

$$\begin{aligned}
\#\left(\mathbf{Z}_{\geq 0} \setminus S\right) &= \sum_{e=0}^{n-1} \#\left(\left(\mathbf{Z}_{\geq 0} \cap (a+de+n\mathbf{Z})\right) \setminus S_e\right) \\
&= \sum_{e=0}^{n-1} \left\lfloor \sum_{j=1}^{d} \left\{ \frac{a_j+e}{n} \right\} \right\rfloor \\
&= \sum_{e=0}^{n-1} \left\lfloor \sum_{j=1}^{d} \frac{a_j+e}{n} - \left\lfloor \frac{a_j+e}{n} \right\rfloor \right\rfloor \\
&= \sum_{e=0}^{n-1} \left(\left\lfloor \frac{a+de}{n} \right\rfloor - \sum_{j=1}^{d} \left\lfloor \frac{a_j+e}{n} \right\rfloor \right) \\
&= \sum_{e=0}^{n-1} \left(\left(\frac{a+de}{n} - \left\{ \frac{a+de}{n} \right\} \right) - \sum_{j=1}^{d} \left(\frac{a_j+e}{n} - \left\{ \frac{a_j+e}{n} \right\} \right) \right) \\
&= \sum_{e=0}^{n-1} \left(- \left\{ \frac{a+de}{n} \right\} + \sum_{j=1}^{d} \left\{ \frac{a_j+e}{n} \right\} \right) \\
&= - \left(\sum_{e=0}^{n-1} \left\{ \frac{a+de}{n} \right\} \right) + \left(\sum_{j=1}^{d} \sum_{e=0}^{n-1} \left\{ \frac{a_j+e}{n} \right\} \right). \qquad (3.27)
\end{aligned}$$

Note that the numbers $\{a+de \colon e \in [0, n-1]\}$ hit each residue class modulo n exactly once. The same goes for $\{a_j + e \colon e \in [0, n-1]\}$. Hence,

$$\sum_{e=0}^{n-1} \left\{ \frac{a+de}{n} \right\} = \sum_{e=0}^{n-1} \left\{ \frac{a_j+e}{n} \right\} = \frac{0}{n} + \frac{1}{n} + \cdots + \frac{n-1}{n} = \frac{n-1}{2}, \qquad (3.28)$$

and substituting (3.28) into (3.27) yields

$$\#\left(\mathbf{Z}_{\geq 0} \setminus S\right) = - \left(\frac{n-1}{2} \right) + \sum_{j=1}^{d} \left(\frac{n-1}{2} \right) = \frac{(n-1)(d-1)}{2} = g. \qquad \square$$

The next step is to extract $|\lambda_D|$ from $\rho_{a_1,\ldots,a_{d-1}}$, which we will do in Corollary 3.3.10.

Definition 3.3.9. For $h \in \mathbf{Z}[\![T]\!]$ and $i \geq 0$, write $[T^i]h$ to denote the T^i-coefficient of h.

Corollary 3.3.10. *Keeping the notation of Proposition 3.3.7, we have*

$$|\lambda_D| + \frac{g(g-1)}{2} = [T^{2g}]\{T^2(1+T+\cdots)^2 \rho_{a_1,\ldots,a_{d-1}}\}.$$

Proof. We have

$$\begin{aligned}
&[T^{2g}]\{T^2(1+T+\cdots)^2\rho_{a_1,\ldots,a_{d-1}}\}\\
&=[T^{2g-1}]\{T(1+T+\cdots)^2\rho_{a_1,\ldots,a_{d-1}}\}\\
&=[T^{2g-1}]\{(T+2T^2+3T^3+\ldots)\rho_{a_1,\ldots,a_{d-1}}\}\\
&=\sum_{i\in[0,2g-1]\setminus G_\infty(D)}(2g-1-i) && \text{(by Proposition 3.3.7)}\\
&=g(2g-1)-\sum_{i\in[0,2g-1]\setminus G_\infty(D)} i\\
&=g(2g-1)-\left(\left(\sum_{i=0}^{2g-1} i\right)-\left(\sum_{i\in G_\infty(D)} i\right)\right)\\
&=\sum_{i\in G_\infty(D)} i\\
&=|\lambda_D|+\frac{g(g-1)}{2}. && \square
\end{aligned}$$

Lemma 3.3.11. *We have*

$$\sum_{D\in\mathcal{J}[1-\zeta]}|\lambda_D|=\frac{g(n+1)n^{d-1}}{12}.$$

Proof. Using Lemma 3.3.6 to sum both sides of Corollary 3.3.10 over all $D\in\mathcal{J}[1-\zeta]$ yields

$$\left(\sum_{D\in\mathcal{J}[1-\zeta]}|\lambda_D|\right)+\frac{g(g-1)n^{d-1}}{2}=[T^{2g}]\{T^2(1+T+\cdots)^2\rho|_{X_1=\cdots=X_n=1}\},$$

and since

$$\begin{aligned}
\rho|_{X_1=\cdots=X_n=1}&=(1+T^n+T^{2n}+\cdots)(1+T+\cdots+T^{n-1})^d\\
&=(1+T+T^2+\cdots)(1+T+\cdots+T^{n-1})^{d-1},
\end{aligned}$$

we have

$$\left(\sum_{D\in\mathcal{J}[1-\zeta]}|\lambda_D|\right)+\frac{g(g-1)n^{d-1}}{2}=[T^{2g}]\{T^2(1+T+\cdots)^3(1+T+\cdots+T^{n-1})^{d-1}\}. \tag{3.29}$$

Define c_i so that

$$\sum_{i=0}^{(n-1)(d-1)}c_iT^i=(1+T+\cdots+T^{n-1})^{d-1}. \tag{3.30}$$

Since $2g=(n-1)(d-1)$,

$$[T^{2g}]\{T^2(1+T+\cdots)^3(1+T+\cdots+T^{n-1})^{d-1}\}=\sum_{i=0}^{2g}\binom{2g-i}{2}c_i. \tag{3.31}$$

The 0th, 1st, and 2nd derivatives of (3.30) are

$$\sum_{i=0}^{2g} c_i T^i = (1 + T + \cdots + T^{n-1})^{d-1}$$
$$\sum_{i=0}^{2g} i c_i T^{i-1} = (d-1)(1 + 2T + 3T^2 + \ldots + (n-1)T^{n-2})(1 + T + \cdots + T^{n-1})^{d-2}$$
$$\begin{aligned}&\sum_{i=0}^{2g} i(i-1) c_i T^{i-2} \\ &= (d-1)(2 + 6T + \ldots + (n-1)(n-2)T^{n-3})(1 + T + \cdots + T^{n-1})^{d-2} \\ &+ (d-1)(d-2)(1 + 2T + 3T^2 + \ldots + (n-1)T^{n-2})^2(1 + T + \cdots + T^{n-1})^{d-3}\end{aligned}$$

Substituting $T = 1$ everywhere above gives

$$\begin{aligned}\sum_{i=0}^{2g} c_i &= n^{d-1} \\ \sum_{i=0}^{2g} i c_i &= (d-1)\left(\frac{n-1}{2}\right) n^{d-1} \\ &= g n^{d-1} \\ \sum_{i=0}^{2g} i(i-1) c_i &= (d-1)\left(\frac{(n-1)(n-2)}{3}\right) n^{d-1} + (d-1)(d-2)\left(\frac{n-1}{2}\right)^2 n^{d-1} \\ &= g\left(g + \frac{n-5}{6}\right) n^{d-1},\end{aligned}$$

so the right hand side of (3.31) is

$$\begin{aligned}\sum_{i=0}^{2g} \binom{2g-i}{2} c_i &= \frac{1}{2}\left(\sum_{i=0}^{2g} (i^2 - i) c_i\right) - (2g-1)\left(\sum_{i=0}^{2g} i c_i\right) + g(2g-1)\left(\sum_{i=0}^{2g} c_i\right) \\ &= \left(\frac{1}{2} g\left(g + \frac{n-5}{6}\right) - (2g-1)g + g(2g-1)\right) n^{d-1} \\ &= \left(\frac{1}{2} g^2 + \frac{g(n-5)}{12}\right) n^{d-1}. \qquad (3.32)\end{aligned}$$

Combining (3.29), (3.31), and (3.32) finishes the proof. □

Lemma 3.3.12. *If $D \notin \Theta$, then $|\lambda_D| = 0$.*

Proof. Suppose that $D \notin \Theta$. If $k \in [0, g-1] \setminus G_\infty(D)$, then there would be an effective degree k divisor E such that $D = [E - k\infty] = [(E + g - 1 - k)\infty - (g-1)\infty] \in \Theta$, which contradicts the assumption that $D \notin \Theta$. Therefore $G_\infty(D) = [0, g-1]$, so $|\lambda_D| = 0$. □

Lemma 3.3.13. *We have*

$$\sum_{D \in \mathcal{C}' \cap \Theta} |\lambda_D| \geq \frac{g(n+1)n^{d-1}}{12}.$$

Proof. We have

$$\begin{aligned}\sum_{D\in\mathcal{C}'\cap\Theta}|\lambda_D| &\geq \sum_{D\in\mathcal{J}[1-\zeta]\cap\Theta}|\lambda_D| && (\text{since } \mathcal{C}'\supseteq\mathcal{J}[1-\zeta])\\ &= \sum_{D\in\mathcal{J}[1-\zeta]}|\lambda_D| && (\text{by Lemma 3.3.12})\\ &= \frac{g(n+1)n^{d-1}}{12} && (\text{by Lemma 3.3.11}). \qquad\square\end{aligned}$$

For the next couple lemmas, we recall some notions of singular cohomology with integral coefficients:

$$\begin{aligned}H^1(\mathcal{C},\mathbf{Z}) &= H^1(\mathcal{J},\mathbf{Z})\simeq\mathbf{Z}^{2g}\\ H^*(\mathcal{J},\mathbf{Z}) &= \bigwedge^*(H^1(\mathcal{J},\mathbf{Z})).\end{aligned}$$

The wedge product provides the cup product pairing $\smile$ on $H^*(\mathcal{J},\mathbf{Z})$. The automorphism ζ of $\mathcal{C}$ induces the pullback automorphism ζ^* of $H^1(\mathcal{C},\mathbf{Z})$.

Lemma 3.3.14. *The characteristic polynomial of ζ^* acting on $H^1(\mathcal{C},\mathbf{Z})$ is*

$$\left(1+T+T^2+\cdots+T^{n-1}\right)^{d-1}.$$

Proof. Since $H^1(\mathcal{C},\mathbf{Z})$ is the dual of $H_1(\mathcal{C},\mathbf{Z})$, this follows immediately from Corollary 2.5.6. □

Definition 3.3.15. Denote the singular cohomology classes of the cycles $\{0\}, \mathrm{AJ}_\infty(\mathcal{C}), \mathcal{C}'$, Θ on $\mathcal{J}$ by $[\infty]\in H^{2g}(\mathcal{J},\mathbf{Z})$, $[\mathcal{C}],[\mathcal{C}']\in H^{2g-2}(\mathcal{J},\mathbf{Z})$, $[\Theta]\in H^2(\mathcal{J},\mathbf{Z})$ respectively.

For $r\geq 0$, define W_r as in Definition 3.2.21 to be the image of the composite morphism $\mathcal{C}^r\to\mathcal{J}^r\overset{\text{sum}}{\to}\mathcal{J}$ and denote its cohomology class by $[W_r]\in H^{2(g-r)}(\mathcal{J},\mathbf{Z})$. In our notation, $[W_0]=[\infty]$, $[W_1]=[\mathcal{C}]$, $[W_{g-1}]=[\Theta]$ by Lemma 3.2.22.

Lemma 3.3.16. *There is a* $\mathbf{C}$*-basis* $\{a_1,\dots,a_g,b_1,\dots,b_g\}$ *for* $H^1(\mathcal{J},\mathbf{C})$ *such that*

(1) *The basis is symplectic: for every* $1\leq i,j\leq n$,

$$\begin{aligned}a_i\smile b_j &= \delta_{i,j}\\ a_i\smile a_j &= 0\\ b_i\smile b_j &= 0.\end{aligned}$$

(2) *Each a_i and b_j is an eigenvector for ζ^*.*

(3) *Let $\lambda(a_i)$, $\lambda(b_j)$ be the eigenvalues corresponding to a_i, b_j, respectively. Then $\lambda(b_i)=\lambda(a_i)^{-1}$.*

Proof. From symplectic linear algebra, each diagonalizable matrix M in $\mathrm{Sp}(2g,\mathbf{C})$ has a symplectic eigenbasis. To see this, let E_λ be the eigenspace corresponding to the eigenvalue $\lambda\in\mathbf{C}$. Since M respects the symplectic pairing, the eigenvalues come in pairs $\{\lambda,\lambda^{-1}\}$. For $\lambda\notin\{\pm1\}$, select any basis for E_λ and take the corresponding dual basis for $E_{\lambda^{-1}}$. For $\lambda\in\{\pm1\}$, the dimension of E_λ must be even so one may pick any symplectic basis for E_λ.

The lemma now follows from the observation in the previous paragraph since the pullback of any automorphism of a manifold respects its cup product and Lemma 3.3.14 implies that the action of ζ^* on $H^1(\mathcal{J}, \mathbf{C})$ is diagonalizable. □

Lemma 3.3.17. *The following equality holds in $H^0(\mathcal{J}, \mathbf{Z})$:*

$$[\mathcal{C}'] \smile [\Theta] = \frac{g(n+1)n^{d-1}}{12}[\infty].$$

Proof. The following proof was suggested by Aaron Pixton.

We may as well verify this identity after tensoring up to $\mathbf{C}$. Let $\{a_1, \ldots, a_g, b_1, \ldots, b_g\}$ be a $\mathbf{C}$-basis for $H^1(\mathcal{J}, \mathbf{C})$ as in Lemma 3.3.16.

"Poincaré's Formula 11.2.1" of [14] implies that for $r \in [0, g]$,

$$[W_r] = \sum_{1 \le i_1 < i_2 < \cdots < i_{g-r} \le g} (a_{i_1} \wedge b_{i_1}) \wedge \cdots \wedge (a_{i_{g-r}} \wedge b_{i_{g-r}}),$$

so

$$\begin{aligned}
[\Theta] = [W_{g-1}] &= \sum_{i=1}^{g} a_i \wedge b_i \\
[\mathcal{C}] = [W_1] &= \sum_{i=1}^{g} a_1 \wedge b_1 \wedge \cdots \wedge \widehat{a_i \wedge b_i} \wedge \cdots \wedge a_g \wedge b_g \\
[\infty] = [W_0] &= a_1 \wedge b_1 \wedge \cdots \wedge a_g \wedge b_g.
\end{aligned}$$

(The hat indicates that the term is not there.)

Since $[\mathcal{C}'] = (1-\zeta)^*[\mathcal{C}]$, a computation using Lemma 3.3.14 and Lemma 3.3.16 yields

$$\begin{aligned}
[\mathcal{C}'] \smile [\Theta] &= ((1-\zeta)^*[\mathcal{C}]) \smile [\Theta] \\
&= \left(\prod_{i=1}^{g} (1-\lambda(a_i))(1-\lambda(b_i))\right) \cdot \left(\sum_{i=1}^{g} \frac{1}{(1-\lambda(a_i))(1-\lambda(b_i))}\right) [\infty] \\
&= \left(\prod_{i=1}^{n-1} (1-\zeta^i)\right)^{d-1} \cdot \left(\frac{g}{n-1} \sum_{i=1}^{n-1} \frac{1}{(1-\zeta^i)(1-\zeta^{-i})}\right) [\infty] \\
&= n^{d-1} \cdot \left(\frac{g}{n-1} \cdot \frac{n^2-1}{12}\right) [\infty] \quad \text{(from Lemma 3.3.19)} \\
&= \left(\frac{g(n+1)n^{d-1}}{12}\right) [\infty].
\end{aligned}$$

□

Corollary 3.3.18. *We have*

$$\sum_{D \in \mathcal{C}' \cap \Theta} i(D) = \frac{g(n+1)n^{d-1}}{12}.$$

Proof. The dual of Lemma 3.3.17 implies that the total intersection of $\mathcal{C}'$ and Θ in $\mathcal{J}$ is $g(n+1)n^{d-1}/12$. □

Lemma 3.3.19. *We have*

$$\sum_{i=1}^{n-1} \frac{1}{(1-\zeta^i)(1-\zeta^{-i})} = \frac{n^2-1}{12}.$$

Proof. The following proof was suggested by Bjorn Poonen.

The differential $d(z^n-1)/(z^n-1)$ has a simple pole with residue 1 at each nth root of unity and a simple pole with residue $-n$ at infinity. Therefore the sum equals the sum of the residues of

$$\omega := \left(\frac{1}{(1-z)(1-z^{-1})}\right)\frac{d(z^n-1)}{z^n-1}.$$

at nth roots of unity not 1, or equivalently $-\operatorname{Res}_\infty(\omega) - \operatorname{Res}_1(\omega)$. Since $1/((1-z)(1-z^{-1}))$ vanishes at ∞, ω is holomorphic at ∞. On the other hand, Mathematica computes that $\operatorname{Res}_1(\omega) = (1-n^2)/12$. □

Definition 3.3.20. Let

$\omega_{\mathcal{C}}$	be the canonical bundle of $\mathcal{C}$
V	be $H^0(\mathcal{C}, \omega_{\mathcal{C}})$
$\Lambda \subseteq V^\vee$	be the period lattice of $\mathcal{C}$
z	be a local coordinate for $\mathcal{C}$ at ∞
A	be the set $\{(a,b) \in \mathbf{Z}^2 \colon 1 \le a \le d-1,\ 1 \le b \le n-1,\ na < db\}$.

We abuse notation and also use z to denote a local coordinate for $\operatorname{AJ}_\infty(\mathcal{C})$ at 0.

Theorem 3.3.21. *There is an isomorphism $\xi \colon \mathcal{J} \to V^\vee/\Lambda$ such that for all $P \in \mathcal{C}$, if γ is a path on $\mathcal{C}$ from ∞ to P, then*

$$\xi\left(\operatorname{AJ}_\infty(P)\right) = \left(\kappa \in V \mapsto \int_\gamma \kappa \in \mathbf{C}\right) \pmod{\Lambda} \in V^\vee/\Lambda.$$

Proof. See Section A.6.3 of [3]. □

Definition 3.3.22. Let π be the composite $V^\vee \to V^\vee/\Lambda \xrightarrow{\xi^{-1}} \mathcal{J}$. The kernel of π is Λ and π expresses $V^\vee$ as the universal cover of $\mathcal{J}$.

Definition 3.3.23. Define $\psi \colon A \to \mathbf{Z}$ by $\psi(a,b) = db - na$. For all $(a,b) \in A$, note that $\psi(a,b) \ge 1$ and $\psi(a,b) = db - na \le d(n-1) - n = 2g-1$, so the image of ψ is contained in $[1, 2g-1]$.

Lemma 3.3.24.

(1) *ψ is an injection.*

(2) *The set $\{x^{a-1}y^{-b}\,dx \colon (a,b) \in A\}$ is a basis of V.*

(3) *There exist nonzero constants $C_{a,b}$ such that*

$$x^{a-1}y^{-b}\,dx = C_{a,b}z^{bd-an-1}\left(1+O(z)\right)\,dz.$$

Proof.

(1) If $\psi(a,b)=\psi(a',b')$, then $d(b-b')=n(a-a')$, and since d is coprime to n, this would imply $d|a-a'$, and since $a,a'\in[1,d-1]$, this means $a=a'$. Similarly, $b=b'$.

(2) Applying Theorem 2.2 of [18] to $\mathcal{C}$ gives a basis of V, which we reindex and rescale to produce the basis in the statement of Lemma 3.3.24(2).

(3) Since $-v_\infty(x)=n$ and $-v_\infty(y)=d$ by Lemma 3.2.12(1) and Lemma 3.2.12(2), there exist constants C_x and C_y such that $x^{-1}=C_xz^n+O(z^{n+1})$ and $y^{-1}=C_yz^d+O(z^{d+1})$, so we are done by substituting these into $x^{a-1}y^{-b}\,dx$. □

In light of Lemma 3.3.24, we make the following definition.

Definition 3.3.25. Let the image of ψ be $\{w_1,\cdots,w_g\}$ for $w_1<w_2<\cdots<w_g$. Let (a_i,b_i) be the unique element of A such that $\psi(a_i,b_i)=w_i$. Define

$$\kappa_i:=C_{a_i,b_i}^{-1}x^{a_i-1}y^{-b_i}\,dx.$$

Corollary 3.3.26. *The set $\{\kappa_1,\cdots,\kappa_g\}$ is a basis for V such that*

$$\kappa_i=z^{w_i-1}\left(1+O(z)\right)dz. \tag{3.33}$$

Proof. This is a restatement of Lemma 3.3.24(3). □

Definition 3.3.27. Let u_{w_i} be the coordinate function on $V^\vee$ associated to κ_i, i.e., if $\langle\cdot,\cdot\rangle:V^\vee\times V\to\mathbf{C}$ is the natural bilinear pairing, then for all $v\in V^\vee$, $u_{w_i}(v)=\langle v,\kappa_i\rangle$.

Definition 3.3.28. Let ζ^* be the automorphism of V induced by ζ and let ζ_* be corresponding dual automorphism of $V^\vee$.

Lemma 3.3.29. *For all $v\in V^\vee$,*

$$u_{w_i}(\zeta_*v)=\zeta^{-b_i}u_{w_i}(v).$$

Proof. Since ζ acts on the function field of $\mathcal{C}$ by $\zeta^*x=x$ and $\zeta^*y=\zeta y$, it follows that $\zeta^*\kappa_i=\zeta^{-b_i}\kappa_i$, and the lemma follows by taking the dual of this relationship. □

Definition 3.3.30. Let U be a small simply-connected neighborhood of 0 in $\mathrm{AJ}_\infty(\mathcal{C})$. Note that $z\circ\mathrm{AJ}_\infty^{-1}$ is a local coordinate on U; we will abuse notation and denote it by z.

Since $1-\zeta$ is a covering map, let U' be the neighborhood of 0 in $\mathcal{C}'$ such that $(1-\zeta)(U')=U$ and $(1-\zeta)|_{U'}:U'\to U$ is an isomorphism. Let $t=(1-\zeta)^*z$ be a local coordinate on U'.

We have the following commutative diagram.

$$\begin{tikzcd}
\{0\} \arrow[r, hook] \arrow[d, "1-\zeta"] & U' \arrow[r, hook] \arrow[d, "1-\zeta"] & \mathcal{C}' \arrow[r, hook] \arrow[d, "1-\zeta"] & \mathcal{J} \arrow[d, "1-\zeta"] \\
\{0\} \arrow[r, hook] & U \arrow[r, hook] & \mathrm{AJ}_\infty(\mathcal{C}) \arrow[r, hook] & \mathcal{J}
\end{tikzcd}$$

Definition 3.3.31. Since π is also a covering map, let $\widetilde{U}\subseteq\pi^{-1}(\mathrm{AJ}_\infty(\mathcal{C}))$ be a neighborhood of 0 in $\pi^{-1}(\mathrm{AJ}_\infty(\mathcal{C}))$ such that $\pi(\widetilde{U})=U$ and $\pi|_{\widetilde{U}}:\widetilde{U}\to U$ is an isomorphism. Similarly, let $\widetilde{U'} \subseteq \pi^{-1}(\mathcal{C}')$ be a neighborhood of 0 in $\pi^{-1}(\mathcal{C}')$ such that $\pi(\widetilde{U'}) = U'$ and $\pi|_{\widetilde{U'}} \colon \widetilde{U'} \to U'$ is an isomorphism.

Note that $z \circ \pi$ is a local coordinate on $\widetilde{U}$; we will abuse notation and denote it by z. Similarly, we will abuse notation and write t to be the analogous local coordinate on $\widetilde{U'}$.

Going to the universal cover yields the following commutative diagram.

$$\begin{tikzcd}
\{0\} \arrow[r, hook] \arrow[d, "(1-\zeta)_*"] & \widetilde{U'} \arrow[r, hook] \arrow[d, "(1-\zeta)_*"] & \pi^{-1}\mathcal{C}' \arrow[r, hook] \arrow[d, "(1-\zeta)_*"] & V^\vee \arrow[d, "(1-\zeta)_*"] \\
\{0\} \arrow[r, hook] & \widetilde{U} \arrow[r, hook] & \pi^{-1}(\mathrm{AJ}_\infty(\mathcal{C})) \arrow[r, hook] & V^\vee
\end{tikzcd}$$

Lemma 3.3.32.

(1) *The following equality holds in* $\widetilde{U}$*:*

$$u_{w_i} = w_i^{-1} z^{w_i}(1 + O(z)).$$

(2) *The following equality holds in* $\widetilde{U'}$*:*

$$u_{w_i} = w_i^{-1}(1 - \zeta^{-b_i})^{-1} t^{w_i}(1 + O(t)).$$

Proof.

(1) Let $\kappa \in V$. Suppose that $P \in \mathcal{C}$ is such that $\mathrm{AJ}_\infty(P) \in U$ and γ is a path from ∞ to P that lies in U. Since U is simply-connected, the value of the integral $\int_\gamma \kappa$ is independent of the choice of γ (as long as γ is contained in U), so we will denote this integral by $\int_\infty^P \kappa$. By Theorem 3.3.21,

$$\xi\left(\mathrm{AJ}_\infty(P)\right) = \left(\kappa \in V \mapsto \int_\infty^P \kappa \in \mathbf{C}\right) \pmod{\Lambda} \in V^\vee/\Lambda.$$

Since U is simply-connected, we may lift this equality to $\widetilde{U}$; that is, there exists some $\lambda \in \Lambda$ such that for all $v \in \widetilde{U}$,

$$v = \lambda + \left(\kappa \mapsto \int_\infty^{\mathrm{AJ}_\infty^{-1}(\pi(v))} \kappa\right).$$

Taking $v = 0$ shows that $\lambda = 0$. Hence, by definition of u_{w_i},

$$u_{w_i}(v) = \int_\infty^{\mathrm{AJ}_\infty^{-1}(\pi(v))} \kappa_i \text{ for all } v \in \widetilde{U}. \tag{3.34}$$

Let $P = \mathrm{AJ}_\infty^{-1}(\pi(v))$, so that Corollary 3.3.26 implies

$$\int_\infty^P \kappa_i = \int_0^{z(P)} z^{w_i - 1}(1 + O(z))\, dz = w_i^{-1}(z(P))^{w_i}\left(1 + O(z(P))\right). \tag{3.35}$$

Since $z(v)$ was defined to be $z(P)$, we are done by (3.34) and (3.35).

(2) Lemma 3.3.29 implies that for all $v \in V^\vee$,

$$u_{w_i}(v) = (1-\zeta^{-b_i})^{-1} u_{w_i}((1-\zeta)_* v), \tag{3.36}$$

so since $\widetilde{U} = (1-\zeta)_* \widetilde{U'}$, Lemma 3.3.32(2) is a consequence of (3.36), the definition of t, and Lemma 3.3.32(1). □

Suppose that $D \in \mathcal{C}' \cap \Theta$. Let $e_D \in \pi^{-1}(D)$.

Definition 3.3.33. Define θ, Δ, δ as on page 5208 of [53] to be the theta function, the Riemann divisor, and Riemann's constant, respectively. (Nakayashiki mentions on the same page that $\delta = \Delta - (g-1)\infty$.) Then $\delta \in \mathcal{J}$, so let $e_\delta \in \pi^{-1}(\delta)$.

Definition 3.3.34. For $F \in \mathcal{J}$, let $T_F : \mathcal{J} \to \mathcal{J}$ be the "translation by F" map. For $e \in V^\vee$, let $T_e : V^\vee \to V^\vee$ be the "translation by e" map.

Theorem 3.3.35. *The vanishing locus of θ is $(\pi \circ T_{e_\delta})^{-1}\Theta$.*

Proof. Riemann's vanishing theorem (see pages 6–7 of [24]) states that the vanishing locus of θ is $\pi^{-1}T_\delta^{-1}\Theta = (T_\delta \circ \pi)^{-1}\Theta$. Since $T_\delta \circ \pi = \pi \circ T_{e_\delta}$, we are done. □

Corollary 3.3.36. *$i(D)$ is the order of vanishing of $(\theta \circ T_{e_D - e_\delta})|_{\widetilde{U'}}$ at 0.*

Proof. By definition, $i(D)$ is the intersection multiplicity of Θ and $\mathcal{C}'$ at D. Since $\pi \circ T_{e_\delta}$ is a local diffeomorphism at $e_D - e_\delta$, we know that $i(D)$ is the intersection multiplicity of $(\pi \circ T_{e_\delta})^{-1}\Theta$ and $(\pi \circ T_{e_\delta})^{-1}\mathcal{C}'$ at $e_D - e_\delta$, so by Theorem 3.3.35,

$$i(D) \text{ is the order of vanishing of } \theta|_{(\pi \circ T_{e_\delta})^{-1}\mathcal{C}'} \text{ at } e_D - e_\delta. \tag{3.37}$$

Since $D \in \mathcal{J}[1-\zeta]$, $T_D(U')$ is a neighborhood of D in $\mathcal{C}'$, so $T_{e_D - e_\delta}(\widetilde{U'})$ is a neighborhood of $e_D - e_\delta$ in $(\pi \circ T_{e_\delta})^{-1}\mathcal{C}'$, so (3.37) yields

$$i(D) \text{ is the order of vanishing of } \theta|_{T_{e_D - e_\delta}(\widetilde{U'})} \text{ at } e_D - e_\delta,$$

which is equivalent to

$$i(D) \text{ is the order of vanishing of } (\theta \circ T_{e_D - e_\delta})|_{\widetilde{U'}} \text{ at } 0$$

since translation by $e_D - e_\delta$ is an isomorphism on $V^\vee$. □

Definition 3.3.37. As on page 5211 of [53], let $s_{\lambda_D} \in \mathbf{Q}[t_1, t_2, \cdots]$ be the Schur function associated to the partition λ_D. Nakayashiki proves that s_{λ_D} lies in the subring $\mathbf{Q}[t_{w_1}, \cdots, t_{w_g}]$ (Proposition 1 on page 5211 of [53]). Assign weight w_i to the variable t_{w_i}. Then s_{λ_D} is weight-homogeneous and it has weight $|\lambda_D|$.

Proposition 3.3.38. *For all $D \in \mathcal{C}' \cap \Theta$,*

$$i(D) \geq |\lambda_D|.$$

Proof. Applying Theorem 10 on page 5232 of [53] to $e = e_D - e_\delta$ (the period matrix $2\omega_1$ defined on page 5231 is the identity matrix in our application) shows that there is a nonzero constant C such that for all $u \in V^\vee$,

$$C\theta(u + e_D - e_\delta) = s_{\lambda_D}(t)|_{t_{w_i} = u_{w_i}} + \text{higher weight terms},$$

which we rewrite as

$$(\theta \circ T_{e_D - e_\delta})(u) = C^{-1} s_{\lambda_D}(t)|_{t_{w_i} = u_{w_i}} + \text{higher weight terms.}$$

Restricting to $u \in \widetilde{U'}$ and applying Lemma 3.3.32(2) yields

$$\theta \circ T_{e_D - e_\delta} = O(t^{|\lambda_D|}) \text{ on } \widetilde{U'},$$

so we are done by Corollary 3.3.36. □

Proof of Theorem 3.3.3. Combining Lemma 3.3.13 and Corollary 3.3.18 yields

$$\sum_{D \in \mathcal{C}' \cap \Theta} (i(D) - |\lambda_D|) \leq 0,$$

so we are done by Proposition 3.3.38. □

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 4

Congruences for Jacobi Sums

In this chapter, we take a brief break from superelliptic curves to study Jacobi sums. The main result is a new congruence for Jacobi sums (Theorem 4.2.25) which we will re-interpret in Subsection 5.2.4 as a statement about the field of definition of the p-torsion of the jacobian of the superelliptic Catalan curve $y^p = x^q + 1$ (Theorem 5.2.28). In Chapter 5, we will use Theorem 5.2.28 as a key technical ingredient to classify torsion points on the superelliptic Catalan curve (Theorem 5.2.73) and also on a generic superelliptic curve (Theorem 5.3.1). First, we will review the definition of Jacobi sums and explain their connection to the zeta function of the Catalan curve in Section 4.1.

The contents of Section 4.2 are the same as that of my paper [5] on Jacobi sums.

4.1 Jacobi sums and the Catalan curve

Definition 4.1.1. Fix a finite field $\mathbf{F}_q$, a field L, and two nontrivial multiplicative characters $\chi, \psi : \mathbf{F}_q^\times \to L^\times$. Then the Jacobi sum $J(\chi, \psi)$ is

$$J(\chi, \psi) := \sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \chi(x)\psi(1-x) \in L.$$

Jacobi sums (and the closely related Gauss sums) have many applications in number theory [11]. As the introduction of [11] mentions, they also have applications in physics [12, 33, 46, 70], quantum algebra [61], graph theory and combinatorics [67, 66], operator theory [23, 22], coding theory [45, 47], cryptography [43], combinatorial designs [10, 39, 40], and algebraic combinatorics [35].

Definition 4.1.2. For $n, d \geq 2$ coprime, define $\mathcal{C}_{n,d}$ to be the smooth projective model of the curve $y^n = x^d + 1$. Let $\mathcal{J}_{n,d}$ be its jacobian. For every prime ℓ, define the Tate module

$$T_\ell \mathcal{J}_{n,d} := \varprojlim_i \mathcal{J}_{n,d}[\ell^i]$$

with the "multiplication by ℓ" transition maps $\mathcal{J}_{n,d}[\ell^{i+1}] \to \mathcal{J}_{n,d}[\ell^i]$.

Definition 4.1.3. Suppose $\mathcal{C}$ is a projective curve defined over a finite field $\mathbf{F}_r$. Then the zeta function of $\mathcal{C}$ is

$$Z(\mathcal{C}/\mathbf{F}_r, T) := \exp\left(\sum_{s=1}^{\infty} \frac{\#\mathcal{C}(\mathbf{F}_{r^s})}{s} T^s \right).$$

Theorem 4.1.4. *Suppose $n, d \geq 2$ are coprime and $r \equiv 1 \pmod{nd}$ is a prime power. Then*

(1) *We have*

$$Z(\mathcal{C}_{n,d}/\mathbf{F}_r, T) = \frac{\prod_{\chi\colon \mathbf{F}_r^\times \twoheadrightarrow \langle\zeta_d\rangle} \prod_{\psi\colon \mathbf{F}_r^\times \twoheadrightarrow \langle\zeta_n\rangle} (1 + \chi(-1)J(\chi,\psi)T)}{(1-T)(1-rT)}, \tag{4.1}$$

where the double product is over all multiplicative characters χ, ψ of order exactly d, n, respectively.

(2) *For any prime $\ell \nmid ndr$, the numerator of $Z(\mathcal{C}_{n,d}/\mathbf{F}_r, T)$ equals*

$$\det\left(I - T \operatorname{Frob}_r | T_\ell \mathcal{J}_{n,d}\right).$$

Proof. (4.1) is a special case of Weil's computation of the zeta function of a diagonal hypersurface [65]. Theorem 4.1.4(2) holds for any smooth projective curve, and it is a special case of the Weil conjectures [19, 31]. □

By applying Lemma 1.1 of Katz [41], we will deduce a refined version of Theorem 4.1.4 in Proposition 5.2.16(2). Computations with (4.1) are used in [37, 38]. A similar computation is done for Fermat curves in [41].

Example: Determination of $\mathbf{Q}(\zeta_{15}, \mathcal{J}_{3,5}[2])$

In this section, we will use (4.1) with $(\ell, n, d) = (2, 3, 5)$ to compute the torsion field

$$L := \mathbf{Q}(\zeta_{15}, \mathcal{J}_{3,5}[2]).$$

Let

E be $\mathbf{Q}(\zeta_{15})$,
$\mathfrak{r}$ be a prime of E,
$\mathfrak{B}$ be a prime of L above $\mathfrak{r}$,
$\mathbf{F}_\mathfrak{r}$ be the residue field of E at $\mathfrak{r}$,
$\mathbf{F}_\mathfrak{B}$ be the residue field of L at $\mathfrak{B}$.

For any finite set S of primes of E, let

$$\mathcal{O}_S := \{\alpha \in E\colon \operatorname{ord}_v(\alpha) \geq 0 \text{ for all } v \notin S\},$$
$$\operatorname{Cl}_S(E) := \text{the } S\text{-ideal class group of } E,$$

and for any integer m, define

$$E(S, m) := \{a \in E^\times/E^{\times m}\colon \operatorname{ord}_v(a) \equiv 0 \pmod{m} \text{ for all } v \notin S\}.$$

From algebraic number theory, the natural map $\mathcal{O}_S^\times/\mathcal{O}_S^{\times m} \hookrightarrow E(S, m)$ is an injection and it is a surjection if and only if $\operatorname{Cl}_S(E)[m] = 0$.

(4.1) implies the eigenvalues of $\mathrm{Frob}_{\mathfrak{r}} \in \mathrm{Gal}(L/E)$ acting on $T_2\mathcal{J}_{3,5}$ are

$$-\chi(-1)J(\chi,\psi) \in \mathbf{Z}_2[\zeta_{15}]$$

for multiplicative characters $\chi, \psi : \mathbf{F}_{\mathfrak{r}}^{\times} \to \mathcal{O}_L^{\times}$ of orders 5 and 3, respectively. Since $(\mathbf{Z}_2[\zeta_{15}]^{\times})^{15} \subseteq 1 + 2\mathbf{Z}_2[\zeta_{15}]$, $\mathrm{Frob}_{\mathfrak{r}}^{15}$ operates as the identity on $\mathcal{J}_{3,5}[2]$. By the Chebotarev density theorem, every element of $\mathrm{Gal}(L/E)$ must have order dividing 15. We will see in Lemma 5.2.11 that L is an abelian extension of E, so L is an abelian extension of E of exponent dividing 15.

By Kummer theory, L/E must be generated by 15th roots of elements of $E^{\times}/E^{\times 15}$. Let S be the primes of E that lie above either 2, 3, or 5. Since $\mathcal{C}_{3,5}$ has good reduction away from 3 and 5, the extension L/E is unramified outside S, so L/E is generated by 15th roots of elements of elements of $E(S, 15)$. The `S_class_group` functionality of `Sage` shows that $\mathrm{Cl}_S(E) = 0$, so $E(S,15) \simeq \mathcal{O}_S^{\times}/\mathcal{O}_S^{\times 15}$. Hence, there is some subgroup

$$A \leq \mathcal{O}_S^{\times}/\mathcal{O}_S^{\times 15}$$

such that

$$L = E(\sqrt[15]{a} : a \in A).$$

For each prime r of $\mathbf{Q}$, define

$$C_r(T) := \det\left(I - T\,\mathrm{Frob}_r \,|T_2\mathcal{J}_{3,5}\right).$$

For any number field K, define

$$\mathrm{Spl}(K) := \{\text{prime } r \text{ of } \mathbf{Q} : r \text{ splits completely in } K\}.$$

Note that

$$\mathrm{Spl}(E) = \{\text{prime } r \text{ of } \mathbf{Q} : r \equiv 1 \pmod{15}\}.$$

Also, $r \in \mathrm{Spl}(L)$ if and only if $r \in \mathrm{Spl}(E)$ and Frob_r acts as the identity on $\mathcal{J}_{3,5}[2]$, which is equivalent to $C_r(T) \equiv (1-T)^8 \pmod 2$. Since $C_r(T)$ is the numerator of the zeta function by Theorem 4.1.4(2), we may apply efficient computer algorithms which calculate the zeta function for superelliptic curves over finite fields [7, 28, 49] to test whether a prime r lies in $\mathrm{Spl}(L)$.

For each prime $\mathfrak{r}$ of E not in S, define the reduction map

$$\varphi_{\mathfrak{r}} \colon \mathcal{O}_S^{\times}/\mathcal{O}_S^{\times 15} \to \mathbf{F}_{\mathfrak{r}}^{\times}/\mathbf{F}_{\mathfrak{r}}^{\times 15}.$$

If $r \in \mathrm{Spl}(L) \setminus \{2,3,5\}$ and $\mathfrak{r}$ lies above r, then $\ker \varphi_{\mathfrak{r}}$ contains A. So

$$A \subseteq \bigcap_{r \in \mathrm{Spl}(L)\setminus\{2,3,5\}} \; \bigcap_{\mathfrak{r} \text{ above } r} \ker \varphi_{\mathfrak{r}}. \tag{4.2}$$

Though we will not need this, the Chebotarev density theorem implies that (4.2) is an equality.

Step 1: We prove that $A \neq \{1\}$ by using a computer to show that $31 \notin \mathrm{Spl}(E) \setminus \mathrm{Spl}(L)$:

$$\begin{aligned} C_{31}(T) &= 923521T^8 + 208537T^7 - 30752T^6 - 5921T^5 + 355T^4 - 191T^3 - 32T^2 + 7T + 1 \\ &\not\equiv T^8 + 1 \pmod 2 \\ &\equiv (1-T)^8 \pmod 2. \end{aligned}$$

Step 2: Sage gives a set of generators for $\mathcal{O}_S^\times$:

$$\mathcal{O}_S^\times = \langle -\zeta_{15},\ \zeta_{15} - 1,\ \zeta_{15}^2 - 1,\ \zeta_{15}^3 + 1,\ \zeta_{15}^4 + \zeta_{15} + 1,\ 2,\ 1 - \zeta_{15}^5,\ 1 - \zeta_{15}^3 \rangle. \tag{4.3}$$

Step 3: A computer shows that $1321, 1831 \in \mathrm{Spl}(L)$, so (4.2) implies

$$\begin{aligned} A &\subseteq \bigcap_{r \in \{1321, 1831\}} \ \bigcap_{\mathfrak{r} \text{ above } r} \ker \varphi_{\mathfrak{r}} \\ &= \langle (1 + \zeta_{15}^3)^{10} \cdot 2^2 \cdot (1 - \zeta_{15}^5)^3 \cdot (1 - \zeta_{15}^3)^5 \rangle \quad \text{(by computer calculation using (4.3))}, \end{aligned}$$

which must be an equality since $A \neq \{1\}$ (by Step 1), so

$$\mathbf{Q}(\zeta_{15}, \mathcal{J}_{3,5}[2]) = \mathbf{Q}\left(\zeta_{15},\ \sqrt[15]{(1 + \zeta_{15}^3)^{10} \cdot 2^2 \cdot (1 - \zeta_{15}^5)^3 \cdot (1 - \zeta_{15}^3)^5}\right).$$

4.2 A new congruence for Jacobi sums

Congruences for Jacobi sums have many applications in number theory [17, 20, 34, 36, 48, 63]. In this section, we prove a new congruence for Jacobi sums of the type considered by Uehara [63].

Fix two distinct primes ℓ and f, a finite field $\mathbf{F}_q$ satisfying $q \equiv 1 \pmod{\ell f}$, and a primitive ℓfth root of unity $\zeta_{\ell f} \in \overline{\mathbf{Q}}$. Let

$$\begin{aligned} L &:= \mathbf{Q}(\zeta_{\ell f}) \\ \mathcal{O}_L &:= \mathbf{Z}[\zeta_{\ell f}] \\ \zeta_f &:= \zeta_{\ell f}^{\ell} \\ M &:= \mathbf{Q}(\zeta_f) \\ \mathcal{O}_M &:= \mathbf{Z}[\zeta_f] \\ \zeta_\ell &:= \zeta_{\ell f}^{f} \\ \pi_\ell &:= \zeta_\ell - 1. \end{aligned}$$

Let $\xi_\ell, \xi_f \in \overline{\mathbf{Q}}$ be ℓth and fth roots of unity such that

$$\begin{aligned} \xi_\ell^f &= \zeta_\ell \\ \xi_f^\ell &= \zeta_f. \end{aligned}$$

Let $\chi : \mathbf{F}_q^\times \to L^\times$ be a character of order ℓf.

Let g be a generator of the multiplicative group $\mathbf{F}_q^\times$ and abuse notation to define $\zeta_{\ell f} := g^{(q-1)/(\ell f)}$ and $\zeta_f, \zeta_\ell, \xi_f, \xi_\ell$ analogously to be elements of $\mathbf{F}_q^\times$.

Lemma 4.2.1. *We have* $\zeta_{\ell f} = \xi_\ell \xi_f$.

Proof. Since ℓ and f are coprime, ξ_ℓ is the unique ℓth root of unity such that $\xi_\ell^f = \zeta_\ell$. Since

$$\begin{aligned}\left(\frac{\zeta_{\ell f}}{\xi_f}\right)^\ell &= \frac{\zeta_f}{\zeta_f} = 1; \text{ and}\\ \left(\frac{\zeta_{\ell f}}{\xi_f}\right)^f &= \frac{\zeta_\ell}{1} = \zeta_\ell,\end{aligned}$$

we are done. □

Definition 4.2.2. For integers a, b, define

$$J(a,b) := J(\chi^a, \chi^b) = \sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \chi^a(x)\chi^b(1-x) \in \mathcal{O}_L.$$

Definition 4.2.3. For $i \in [0, \ell-1]$ and $j \in [1, f-1]$, define

$$\eta_{i,j} := \prod_{r=0}^{\ell-1} \left(1 - \xi_\ell^r \xi_f^j\right)^{\binom{r}{i}} \in \mathbf{F}_q^\times.$$

Our main result is the following.

Theorem 4.2.25. *For* $k \in [1, \ell-1]$*, the following are equivalent:*

(1) $J(\ell, f) + 1 \in \pi_\ell^k \mathcal{O}_L$;

(2) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, k-2]$ *and* $j \in [1, f-1]$;

(3) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, k-2]$ *and* $j \in [1, f/2]$.

In particular, $J(\ell, f) + 1 \in \pi_\ell \mathcal{O}_L$ *always holds.*

Our methods allow us to even reach the case $k = \ell$, which we analyze in Subsection 4.2.8.

Theorem 4.2.29. *The following are equivalent:*

(1) $J(\ell, f) + 1 \in \pi_\ell^\ell \mathcal{O}_L$

(2) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \xi_\ell^i \xi_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, \ell-1]$ *and* $j \in [1, f-1]$;

(3) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \xi_\ell^i \xi_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, \ell-1]$ *and* $j \in [1, f/2]$.

4.2.1 A few properties of binomial coefficients

Lemma 4.2.4.

(1) *For* $a \in \mathbf{Z}$ *and* $b \in [0, a]$,

$$\binom{a}{b} = \binom{a}{a-b}.$$

(2) *For* $a \in \mathbf{Z}$ *and* $b \in \mathbf{Z}_{\geq 0}$,

$$\binom{a}{b+1} = \frac{a}{b+1}\binom{a-1}{b}.$$

(3) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$,*

$$\binom{a}{b+1} = \binom{a-1}{b} + \binom{a-1}{b+1}.$$

(4) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$,*

$$a\binom{a}{b} = (b+1)\binom{a}{b+1} + b\binom{a}{b}.$$

(5) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$,*

$$\sum_{c=0}^{a-1} \binom{c}{b} = \binom{a}{b+1}.$$

(6) *For $a, b \in \mathbf{Z}$ and $c \in \mathbf{Z}_{\geq 0}$,*

$$\binom{a+b}{c} = \sum_{d=0}^{c} \binom{a}{d}\binom{b}{c-d}.$$

(7) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$,*

$$\binom{-a}{b} = (-1)^b \sum_{c=0}^{b} \binom{b-1}{b-c}\binom{a}{c}.$$

(8) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$,*

$$\sum_{c=0}^{a-1} c\binom{c}{b} = (a-1)\binom{a}{b+1} - \binom{a}{b+2}.$$

(9) *For $a_1, a_2 \in \mathbf{Z}$ and $b \in [0, \ell - 1]$ such that $a_1 \equiv a_2 \pmod{\ell}$,*

$$\binom{a_1}{b} \equiv \binom{a_2}{b} \pmod{\ell}.$$

(10) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$ such that $a \equiv 0 \pmod{\ell}$, $b \not\equiv 0 \pmod{\ell}$,*

$$\binom{a}{b} \equiv 0 \pmod{\ell}.$$

(11) *For $a \in \mathbf{Z}$ and $b \in \mathbf{Z}_{\geq 0}$,*

$$\binom{a\ell}{b\ell} \equiv \binom{a}{b} \pmod{\ell}.$$

Proof. For Lemma 4.2.4(1), use

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

For Lemma 4.2.4(2) – Lemma 4.2.4(4), use

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-(k-1))}{k!}.$$

(5) Induct on a and use Lemma 4.2.4(3).

(6) This is Vandermonde's identity for binomial coefficients, and it follows by comparing the x^c-coefficient of both sides of $(1+x)^{a+b} = (1+x)^a(1+x)^b$.

(7) Note that

$$\binom{-a}{b} = \frac{(-a)(-a-1)\cdots(-a-(b-1))}{b!} = (-1)^b\binom{a+b-1}{b},$$

so we are done by applying Lemma 4.2.4(6).

(8) We have

$$\begin{aligned}\sum_{c=0}^{a-1} c\binom{c}{b} &= \sum_{c=0}^{a-1}\left((b+1)\binom{c}{b+1} + b\binom{c}{b}\right) && \text{(by Lemma 4.2.4(4))}\\ &= (b+1)\binom{a}{b+2} + b\binom{a}{b+1} && \text{(by Lemma 4.2.4(5))}\\ &= a\binom{a}{b+1} - \left(\binom{a}{b+2} + \binom{a}{b+1}\right) && \text{(by Lemma 4.2.4(4))}\\ &= (a-1)\binom{a}{b+1} - \binom{a}{b+2}.\end{aligned}$$

(9) Consider the polynomial $q(x) := \binom{x}{b} \in \mathbf{F}_\ell[x]$. It follows from $b!p(x) = x(x-1)\cdots(x-(b-1))$ that $b!p(a_1) \equiv b!p(a_2) \pmod{\ell}$. Since $b \in [0, \ell-1]$, $b!$ is invertible modulo ℓ, so we may divide both sides by $b!$ to get $p(a_1) \equiv p(a_2) \pmod{\ell}$.

(10) For any i, note that $\binom{a}{i} \pmod{\ell}$ is the x^i-coefficient of the polynomial $p(x) := (1+x)^a \in \mathbf{F}_\ell[x]$. We have $p(x) = ((1+x)^\ell)^{a/\ell} = (1+x^\ell)^{a/\ell}$, so since $b \nmid \ell$, $\binom{a}{b} = [x^b]p(x) \equiv 0 \pmod{\ell}$.

(11) As in the previous part, define $p(x) := (1+x)^a \in \mathbf{F}_\ell[x]$. Then

$$\binom{a}{b} \equiv [x^{b\ell}]p(x^\ell) \pmod{\ell}, \tag{4.4}$$

and since $p(x^\ell) = (1+x^\ell)^a = (1+x)^{a\ell}$,

$$[x^{b\ell}]p(x^\ell) \equiv \binom{a\ell}{b\ell} \pmod{\ell}, \tag{4.5}$$

so we finish by combining (4.4) and (4.5). □

4.2.2 The index

Recall that g is a generator of the multiplicative group $\mathbf{F}_q^\times$.

Definition 4.2.5. For $x \in \mathbf{F}_q^\times$, define $\operatorname{ind}(x) \in \{0, 1, \cdots, q-2\}$ such that

$$x = g^{\operatorname{ind} x}.$$

Then by definition of $\zeta_{\ell f}$,

$$\operatorname{ind} \zeta_{\ell f} = \frac{q-1}{\ell f}. \tag{4.6}$$

Lemma 4.2.6. $\{\operatorname{ind} x : x \in \mathbf{F}_q \setminus \{0,1\}\} = \{1, 2, \ldots, q-2\}$.

Proof. This is immediate by the definition of ind since $\operatorname{ind}(1) = 0$. □

Lemma 4.2.7. *For $y, z \in \mathbf{F}_q^\times$, $\operatorname{ind}(yz) \equiv \operatorname{ind} y + \operatorname{ind} z \pmod{q-1}$.*

Proof. This follows immediately from the definition of ind. □

Lemma 4.2.8. *For $r \in [0, \ell - 1]$ and $j \in [1, f-1]$,*

$$\sum_{\substack{a \in [1, q-2] \\ a \equiv j \pmod{f} \\ a \equiv r \pmod{\ell}}} \operatorname{ind}(1 - g^a) \equiv \operatorname{ind}\left(1 - \xi_\ell^r \xi_f^j\right) \pmod{q-1}.$$

Proof. Take the equality

$$\prod_{k=0}^{\frac{q-1}{\ell f}-1} (1 - g^{k\ell f} X) = 1 - X^{\frac{q-1}{\ell f}} \qquad \text{in } \mathbf{F}_q[X]$$

and substitute $X = g^a$ to obtain

$$\begin{aligned} \prod_{k=0}^{\frac{q-1}{\ell f}-1} (1 - g^{a+k\ell f}) &= 1 - g^{a\left(\frac{q-1}{\ell f}\right)} \\ &= 1 - \zeta_{\ell f}^a \\ &= 1 - \xi_\ell^a \xi_f^a && \text{(by Lemma 4.2.1)} \\ &= 1 - \xi_\ell^r \xi_f^j, \end{aligned}$$

so we are done by taking ind of both sides and using Lemma 4.2.7. □

Definition 4.2.9. For integers a and b, define

$$\delta_{a,b} = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 4.2.10.

(1) *For $m \in [1, f-1]$,*

$$\eta_{0,m} = 1 - \xi_f^{m\ell}.$$

(2) *We have*

$$\operatorname{ind}\xi_f \equiv 0 \pmod{\ell} \tag{4.7}$$

$$\operatorname{ind}\xi_\ell \equiv \frac{q-1}{\ell f} \pmod{\ell}. \tag{4.8}$$

(3) *For $i \in [0, \ell-1]$ and $j \in [1, f-1]$,*

$$\operatorname{ind}\eta_{i,j} \equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \operatorname{ind}\left(1 - \xi_\ell^r \xi_f^j\right) \pmod{q-1}.$$

(4) *For $i \in [0, \ell-1]$ and $j \in [1, f-1]$,*

$$\begin{aligned}&\operatorname{ind}\eta_{i,f-j}\\ &\equiv -\delta_{i,\ell-1}\left(\operatorname{ind}(-1) - \left(\frac{q-1}{\ell f}\right)\right) - \delta_{i,\ell-2}\left(\frac{q-1}{\ell f}\right) + (-1)^i \sum_{k=0}^{i} \binom{i-1}{i-k} \operatorname{ind}\eta_{k,j}\\ &\quad \pmod{\ell}.\end{aligned}$$

(5) *Suppose that $i \in [1, \ell-1]$, $j \in [1, f-1]$, and $m \in [1, f-1]$ are such that $m\ell \equiv j \pmod{f}$. Then*

$$\operatorname{ind}\left(1 - \xi_\ell^i \xi_f^j\right) \equiv \operatorname{ind}\eta_{0,m} - \sum_{s=\ell-1-i}^{\ell-2} \sum_{a=0}^{s} \binom{s}{a} \operatorname{ind}\eta_{\ell-2-a,j} \pmod{\ell}.$$

(6) *For $i \in [1, \ell-1]$ and $j \in [1, f-1]$,*

$$\operatorname{ind}\left(1 - \xi_\ell^i \xi_f^j\right) \equiv \operatorname{ind}(-1) + i\left(\frac{q-1}{\ell f}\right) + \operatorname{ind}\left(1 - \xi_\ell^{\ell-i} \xi_f^{f-j}\right) \pmod{\ell}.$$

Proof.

(1) Take the equality

$$\prod_{r=0}^{\ell-1} (1 - \xi_\ell^r X) = 1 - X^\ell \qquad \text{in } \mathbf{F}_q[X]$$

and substitute $X = \xi_f^m$ to obtain

$$\begin{aligned}\eta_{0,m} &= \prod_{r=0}^{\ell-1} (1 - \xi_\ell^r \xi_f^m)\\ &= 1 - (\xi_f^m)^\ell.\end{aligned}$$

(2) Since ξ_f is an fth root of unity and $\mathbf{F}_q$ contains a primitive ℓfth root of unity, $\xi_f \in \mathbf{F}_q^{\times \ell}$; (4.7) follows. Taking ind of both sides of Lemma 4.2.1 and using Lemma 4.2.7 yields $\operatorname{ind}\zeta_{\ell f} \equiv \operatorname{ind}\xi_\ell + \operatorname{ind}\xi_f \pmod{q-1}$, so (4.8) follows from (4.6) and (4.7).

(3) Take ind of both sides of Definition 4.2.3.

(4) Modulo ℓ, we have

$$\begin{aligned}
&\operatorname{ind}\eta_{i,f-j}\\
&\equiv \sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\xi_\ell^r\xi_f^{-j}\right)\\
&\qquad\text{(by Lemma 4.2.10(3))}\\
&\equiv \sum_{r=0}^{\ell-1}\binom{r}{i}\left(\operatorname{ind}(-1)+r\operatorname{ind}\xi_\ell-j\operatorname{ind}\xi_f+\operatorname{ind}\left(1-\xi_\ell^{-r}\xi_f^{j}\right)\right)\\
&\qquad\text{(by Lemma 4.2.7)}\\
&\equiv \operatorname{ind}(-1)\left(\sum_{r=0}^{\ell-1}\binom{r}{i}\right)+\left(\frac{q-1}{\ell f}\right)\left(\sum_{r=0}^{\ell-1}r\binom{r}{i}\right)+\sum_{r=0}^{\ell-1}\operatorname{ind}\left(1-\xi_\ell^{-r}\xi_f^{j}\right)\\
&\qquad\text{(by Lemma 4.2.10(2))}\\
&\equiv \operatorname{ind}(-1)\binom{\ell}{i+1}+\left(\frac{q-1}{\ell f}\right)\left((\ell-1)\binom{\ell}{i+1}-\binom{\ell}{i+2}\right)\\
&\quad+\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\xi_\ell^{-r}\xi_f^{j}\right)\\
&\qquad\text{(by Lemma 4.2.4(5) and Lemma 4.2.4(8))}\\
&\equiv \delta_{i,\ell-1}\left(\operatorname{ind}(-1)-\left(\frac{q-1}{\ell f}\right)\right)-\delta_{i,\ell-2}\left(\frac{q-1}{\ell f}\right)+\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\xi_\ell^{-r}\xi_f^{j}\right), \qquad (4.9)
\end{aligned}$$

since $\binom{\ell}{k}$ is divisible by ℓ except when $k \in \{0,\ell\}$, in which case it equals 1 (and we assume that $i \in [0,\ell-1]$). Change variables in the last sum to $s \in [0,\ell-1]$ such that $s \equiv -r \pmod{\ell}$ (the values $\binom{r}{i}$ and ξ_ℓ^r only depend on $r \pmod{\ell}$ by Lemma 4.2.4(9) and by definition of ξ_ℓ). This yields

$$\begin{aligned}
\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\xi_\ell^{-r}\xi_f^{j}\right) &= \sum_{s=0}^{\ell-1}\binom{-s}{i}\operatorname{ind}\left(1-\xi_\ell^{s}\xi_f^{j}\right)\\
&\equiv (-1)^i\sum_{s=0}^{\ell-1}\sum_{k=0}^{i}\binom{i-1}{i-k}\binom{s}{k}\operatorname{ind}\left(1-\xi_\ell^{s}\xi_f^{j}\right)\\
&\qquad\text{(by Lemma 4.2.4(7))}\\
&\equiv (-1)^i\sum_{k=0}^{i}\binom{i-1}{i-k}\operatorname{ind}\eta_{k,j} \qquad (4.10)
\end{aligned}$$

by Lemma 4.2.10(3). We finish by combining (4.9) and (4.10).

(5) Modulo ℓ, we have

$$\begin{aligned}
&\sum_{s=\ell-1-i}^{\ell-2} \sum_{a=0}^{s} \binom{s}{a} \operatorname{ind} \eta_{\ell-2-a,j} \\
&\equiv \sum_{s=\ell-1-i}^{\ell-2} \sum_{r=0}^{\ell-1} \sum_{a=0}^{s} \binom{s}{a} \binom{r}{\ell-2-a} \operatorname{ind}\left(1-\xi_\ell^r \xi_f^j\right) && \text{(by Lemma 4.2.10(3))} \\
&= \sum_{s=\ell-1-i}^{\ell-2} \sum_{r=0}^{\ell-1} \binom{r+s}{\ell-2} \operatorname{ind}\left(1-\xi_\ell^r \xi_f^j\right) && \text{(by Lemma 4.2.4(6))} \\
&\equiv \sum_{s=\ell-1-i}^{\ell-2} \left(\operatorname{ind}\left(1-\xi_\ell^{\ell-2-s}\xi_f^j\right) - \operatorname{ind}\left(1-\xi_\ell^{\ell-1-s}\xi_f^j\right)\right) && \text{(by Lemma 4.2.4(9))} \\
&= \operatorname{ind}\left(1-\xi_f^j\right) - \operatorname{ind}\left(1-\xi_\ell^i\xi_f^j\right) && \text{(telescoping sum)} \\
&= \operatorname{ind}\eta_{0,m} - \operatorname{ind}\left(1-\xi_\ell^i\xi_f^j\right) && \text{(by Lemma 4.2.10(1)).}
\end{aligned}$$

(6) Taking ind of both sides of $1-\xi_\ell^i\xi_f^j = -\xi_\ell^i\xi_f^j\left(1-\xi_\ell^{\ell-i}\xi_f^{f-j}\right)$ and using Lemma 4.2.7 gives

$$\begin{aligned}
\operatorname{ind}\left(1-\xi_\ell^i\xi_f^j\right) &\equiv \operatorname{ind}(-1) + i \operatorname{ind}\xi_\ell + j \operatorname{ind}\xi_f + \operatorname{ind}\left(1-\xi_\ell^{\ell-i}\xi_f^{f-j}\right) \pmod{\ell} \\
&\equiv \operatorname{ind}(-1) + i\left(\frac{q-1}{\ell f}\right) + \operatorname{ind}\left(1-\xi_\ell^{\ell-i}\xi_f^{f-j}\right) \pmod{\ell}
\end{aligned}$$

by (4.8) and (4.7). □

4.2.3 Some rings

Definition 4.2.11. Define $Q := \mathbf{Z}[t]/(t^f-1)$. Define ring homomorphisms $\alpha\colon Q \to \mathcal{O}_M$ and $\beta\colon Q \to \mathbf{Z}$ by $\alpha(t) = \zeta_f$ and $\beta(t) = 1$. Define

R := $Q/\ell Q = \mathbf{Z}[t]/(\ell, t^f - 1)$

R' := the subring $\mathbf{Z}/\ell\mathbf{Z}$ of R

$\omega\colon R \to \mathcal{O}_M/\ell\mathcal{O}_M$:= the ring homomorphism induced by α; i.e., $\omega(t) = [\zeta_f]$

$\tau\colon R \to \mathbf{Z}/\ell\mathbf{Z}$:= the ring homomorphism induced by β; i.e., $\tau(t) = 1$.

Each $r \in R$ has a unique representation $r = a_0 + a_1 t + \cdots + a_{f-1}t^{f-1}$ for $a_0, a_1, \ldots, a_{f-1} \in \mathbf{Z}/\ell\mathbf{Z}$, so for $j \in [0, f-1]$, define

$$[t^j](r) := a_j$$

to be the jth coefficient of r.

Lemma 4.2.12. *The product homomorphism*

$$(\omega, \tau) : R \to (\mathcal{O}_M/\ell\mathcal{O}_M) \times (\mathbf{Z}/\ell\mathbf{Z})$$

is an isomorphism.

Proof. The ideals I_1, I_2 of R defined by

$$\begin{aligned} I_1 &:= (t^{f-1} + t^{f-2} + \cdots + 1) \\ I_2 &:= (t-1) \end{aligned}$$

are pairwise coprime because for

$$\begin{aligned} i_1 &:= t^{f-1} + t^{f-2} + \cdots + 1 && \in I_1 \\ i_2 &:= (t^{f-1} - 1) + (t^{f-2} - 1) + \cdots + (t-1) && \in I_2, \end{aligned}$$

the difference $i_1 - i_2 = f$ is a unit of R, so by the Chinese remainder theorem, the natural map

$$R \to (R/I_1) \times (R/I_2)$$

is an isomorphism. Since ω is the composite map $\omega \colon R \to R/I_1 \simeq \mathcal{O}_M/\ell\mathcal{O}_M$ and τ is the composite map $\tau \colon R \to R/I_2 \simeq \mathbf{Z}/\ell\mathbf{Z}$, we are done. □

Lemma 4.2.13. *For $r \in \ker \tau$, the following are equivalent.*

(1) $\omega(r) = 0$*;*

(2) $r = 0$*;*

(3) $r \in R'$*.*

Proof. The restriction $\tau|_{R'} : R' \to \mathbf{Z}/\ell\mathbf{Z}$ is an isomorphism, so $r \in R' \cap \ker \tau$ if and only if $r = 0$, giving Lemma 4.2.13(3) $\iff$ Lemma 4.2.13(2). By Lemma 4.2.12, $r = 0$ if and only if $\tau(r) = 0$ and $\omega(r) = 0$, giving Lemma 4.2.13(1) $\iff$ Lemma 4.2.13(2). □

Definition 4.2.14. For nonnegative integers u and v, define

$$\begin{aligned} S(u,v) &:= \sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \binom{\operatorname{ind} x}{u} \binom{\operatorname{ind}(1-x)}{v} t^{\operatorname{ind} x} && \in R \\ T(u,v) &:= \tau(S(u,v)) && \in \mathbf{Z}/\ell\mathbf{Z} \\ W(u,v) &:= \omega(S(u,v)) && \in \mathcal{O}_M/\ell\mathcal{O}_M. \end{aligned}$$

Lemma 4.2.15. *For $i \in [0, \ell-1]$,*

$$T(0,i) = \begin{cases} -1 & \text{if } i = 0 \\ 0 & \text{if } i \in [1, \ell-2] \\ \frac{q-1}{\ell} & \text{if } i = \ell - 1. \end{cases}$$

Proof. We have

$$\begin{aligned}
T(0,i) &= \tau(S(0,i)) \\
&= \tau\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{i} t^{\operatorname{ind} x}\right) \\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{i} \\
&= \sum_{k=1}^{q-2} \binom{k}{i} && \text{(by Lemma 4.2.6)} \\
&= \binom{q-1}{i+1} - \binom{0}{i} && \text{(by Lemma 4.2.4(5))},
\end{aligned}$$

and the rest follows from Lemma 4.2.4(10) and Lemma 4.2.4(11). □

Lemma 4.2.16.

(A) *For $i \in [1, \ell-2]$, the following are equivalent:*

(1) $S(0,i) \in R'$;

(2) $W(0,i) = 0$.

(B) *The following are equivalent:*

(1) $S(0,\ell-1) - \frac{q-1}{\ell f}(1+t+t^2+\cdots+t^{f-1}) \in R'$;

(2) $W(0,\ell-1) = 0$.

Proof. Lemma 4.2.15 implies that

$$\begin{aligned}
S(0,i) &\in \ker\tau \\
S(0,\ell-1) - \frac{q-1}{\ell f}(1+t+t^2+\cdots+t^{f-1}) &\in \ker\tau,
\end{aligned}$$

so we are done by applying Lemma 4.2.13(1) $\Longleftrightarrow$ Lemma 4.2.13(3) to $r = S(0,i)$ and to $r = S(0,\ell-1) - \frac{q-1}{\ell f}(1+t+t^2+\cdots+t^{f-1})$. □

4.2.4 ℓ-adic valuation of Jacobi sums

Definition 4.2.17. For integers $a, b \not\equiv 0 \pmod{\ell f}$, define

$$J(a,b) := \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_{f\ell}^{a\operatorname{ind}(x)+b\operatorname{ind}(1-x)}.$$

Lemma 4.2.18.

(A) *For $k \in [1, \ell-1]$, the following are equivalent:*

(1) $J(\ell, f) + 1 \in \pi_\ell^k \mathcal{O}_L$;

(2) $S(0,1),\ S(0,2),\ \ldots,\ S(0,k-1) \in R'$.

(B) *The following are equivalent:*

(1) $J(\ell,f)+1 \in \pi_\ell^\ell \mathcal{O}_L$;

(2) $S(0,1),\ S(0,2),\ \ldots,\ S(0,\ell-2),\ S(0,\ell-1) - \frac{q-1}{\ell f}\left(1+t+\cdots+t^{f-1}\right) \in R'$.

Proof. By definition,

$$\begin{aligned}
&J(\ell,f)\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_{f\ell}^{\ell\,\mathrm{ind}(x)+f\,\mathrm{ind}(1-x)}\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)}\zeta_\ell^{\mathrm{ind}(1-x)}\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)}(1+\pi_\ell)^{\mathrm{ind}(1-x)}\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)} \sum_{i=0}^{\mathrm{ind}(1-x)} \binom{\mathrm{ind}(1-x)}{i}\pi_\ell^i\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)} \sum_{i=0}^{q-1} \binom{\mathrm{ind}(1-x)}{i}\pi_\ell^i \qquad\qquad (\text{since } \mathrm{ind}(1-x)<q-1)\\
&= \sum_{i=0}^{q-1}\pi_\ell^i\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)\\
&\in \left(\sum_{i=0}^{\ell-1}\pi_\ell^i\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)\right)+\pi_\ell^\ell\mathcal{O}_L
\end{aligned}$$

By Lemma 4.2.6, the $i=0$ term contributes $\zeta_f^1+\cdots+\zeta_f^{q-2} = (\zeta_f^{q-1}-\zeta_f)/(\zeta_f-1) = -1$ since $q\equiv 1 \pmod{\ell f}$, so

$$J(\ell,f) \in \left(-1+\sum_{i=1}^{\ell-1}\pi_\ell^i\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)\right)+\pi_\ell^\ell\mathcal{O}_L \tag{4.11}$$

Since $v_\ell(\pi_\ell)=\frac{1}{\ell-1}$, the term $\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)$ lies in $\mathcal{O}_M$, and M is unramified at ℓ, the ith term in the sum on the right hand side of (4.11) has ℓ-adic valuation $\frac{i}{\ell-1} \pmod 1$. In particular, all the valuations are distinct, so

$$J(\ell,f)+1\in\pi_\ell^k\mathcal{O}_L$$

if and only if

$$\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)} \in \ell\mathcal{O}_M \qquad \text{for } i\in[1,k-1],$$

which is the same as

$$W(0,1),\ W(0,2),\ \cdots,\ W(0,k-1)=0,$$

so we are done by Lemma 4.2.16. □

4.2.5 The connection between $S(i,1)$ and cyclotomic units

Recall that g is a generator for $\mathbf{F}_q^\times$. We abuse notation and define $\zeta_{\ell f} := g^{\frac{q-1}{\ell f}} \in \mathbf{F}_q^\times$. Using $\zeta_{\ell f}$, define $\zeta_f, \zeta_\ell, \xi_f, \xi_\ell$ as before.

Lemma 4.2.19. *For $i \in [0,\ell-1]$ and $j \in [1, f-1]$,*

$$[t^j]S(i,1) \equiv \operatorname{ind} \eta_{i,j} \pmod{\ell}.$$

Proof. By definition of $S(i,1)$,

$$\begin{aligned}
[t^j]S(i,1) &= \sum_{\substack{a\in[1,q-2]\\ a\equiv j \pmod f}} \binom{a}{i} \operatorname{ind}(1-g^a)\\
&= \sum_{r=0}^{\ell-1} \sum_{\substack{a\in[1,q-2]\\ a\equiv j \pmod f\\ a\equiv r \pmod \ell}} \binom{a}{i} \operatorname{ind}(1-g^a)\\
&\equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \sum_{\substack{a\in[1,q-2]\\ a\equiv j \pmod f\\ a\equiv r \pmod \ell}} \operatorname{ind}(1-g^a) \pmod{\ell} && \text{(by Lemma 4.2.4(9))}\\
&\equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \operatorname{ind}\left(1-\xi_\ell^r \xi_f^j\right) \pmod{\ell} && \text{(by Lemma 4.2.8)}\\
&\equiv \operatorname{ind} \eta_{i,j} \pmod{\ell} && \text{(by Lemma 4.2.10(3)).}
\end{aligned}$$

□

Lemma 4.2.20.

(A) *For $i \in [0,\ell-3]$, the following are equivalent:*

(1) *$S(i,1) \in R'$;*

(2) *$\operatorname{ind} \eta_{i,j} \equiv 0 \pmod{\ell}$ for $j \in [1, f-1]$.*

(B) *The following are equivalent:*

(1) *$S(\ell-2,1) + \frac{q-1}{\ell f}\left(1+t+\cdots+t^{f-1}\right) \in R'$;*

(2) *$\operatorname{ind}(\eta_{\ell-2,j}) + \frac{q-1}{\ell f} \equiv 0 \pmod{\ell}$ for $j \in [1, f-1]$.*

Proof. For any $r \in R$, the condition $r \in R'$ is equivalent to $[t^j]r \equiv 0 \pmod{\ell}$ for $j \in [1, f-1]$. Apply this observation to $r \in \{S(0,1), \cdots, S(\ell-3), S(\ell-2,1) + \frac{q-1}{\ell f}\left(1+t+\cdots+t^{f-1}\right)\}$ and use Lemma 4.2.19 to finish. □

4.2.6 A recursion for $S(u, v)$

In this section, we will investigate the product of expressions of the form $S(u, v)$.

Lemma 4.2.21. *For $i \in [1, \ell - 2]$ and $s \in [1, i]$,*

$$\begin{aligned}
&(i-s+1)S(i-s+1,s) - (s+1)S(i-s,s+1) \\
&\equiv \left(\sum_{r=0}^{i-s} S(i-s-r,s)S(r,1)\right) - \left(\sum_{k=1}^{s} T(1,s-k)S(i-s,k)\right) - (i-2s)S(i-s,s) \\
&\quad \pmod{R'}.
\end{aligned}$$

Proof. By definition of $S(u, v)$,

$$\begin{aligned}
&\sum_{r=0}^{i-s} S(i-s-r,s)S(r,1) \\
&= \sum_{y,z\in \mathbf{F}_q\setminus\{0,1\}} \sum_{r=0}^{i-s} \binom{\operatorname{ind}(y)}{i-s-r}\binom{\operatorname{ind}(z)}{r}\binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(1-z) t^{\operatorname{ind} y} t^{\operatorname{ind} z} \\
&= \sum_{y,z\in \mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(y)+\operatorname{ind}(z)}{i-s}\binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(1-z) t^{\operatorname{ind} y+\operatorname{ind} z} \\
&\quad \text{(by Lemma 4.2.4(6))} \\
&= \sum_{y,z\in \mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(yz)}{i-s}\binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(1-z) t^{\operatorname{ind}(yz)} \\
&\quad \text{(by Lemma 4.2.7, Lemma 4.2.4(9), and } t^{q-1}=1\text{)} \\
&= \sum_{\substack{x\in \mathbf{F}_q\setminus\{0\} \\ y\in \mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}\left(1-\frac{x}{y}\right)\binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\quad \text{(by setting } x := yz\text{)} \\
&= \sum_{\substack{x\in \mathbf{F}_q\setminus\{0\} \\ y\in \mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} (\operatorname{ind}(y-x)-\operatorname{ind}(y))\binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\quad \text{(by Lemma 4.2.7)} \\
&\equiv \sum_{\substack{x\in \mathbf{F}_q\setminus\{0,1\} \\ y\in \mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} (\operatorname{ind}(y-x)-\operatorname{ind}(y))\binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \pmod{R'},
\end{aligned}$$

so if we define

$$\begin{aligned}
A &:= \sum_{\substack{x\in \mathbf{F}_q\setminus\{0,1\} \\ y\in \mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y-x)\binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
B &:= \sum_{\substack{x\in \mathbf{F}_q\setminus\{0,1\} \\ y\in \mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y)\binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x},
\end{aligned}$$

then

$$\sum_{r=0}^{i-s} S(i-s-r,s)S(r,1) \equiv A - B \pmod{R'}. \tag{4.12}$$

We have

$$\begin{aligned}
B &= \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y\in\mathbf{F}_q\setminus\{0,1\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\quad - \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y=x}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= \left(\sum_{y\in\mathbf{F}_q\setminus\{0,1\}} \operatorname{ind}(y) \binom{\operatorname{ind}(1-y)}{s} \right) \left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \right) \\
&\quad - \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{s} \operatorname{ind}(x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= T(1,s)S(i-s,0) \\
&\quad - \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{s} \left((i-s+1)\binom{\operatorname{ind} x}{i-s+1} + (i-s)\binom{\operatorname{ind} x}{i-s} \right) t^{\operatorname{ind} x} \\
&\qquad \text{(by definition of } T(1,s),\ S(i-s,0), \text{ and Lemma 4.2.4(4))} \\
&= T(1,s)S(i-s,0) - (i-s+1)S(i-s+1,s) - (i-s)S(i-s,s) \\
&\qquad \left(\text{by definition of } S(i-s+1,s) \text{ and } S(i-s,s)\right).
\end{aligned}$$

Since $s \geq 1$, the summand in A vanishes when $y = 0$, so we can put it back in to get

$$\begin{aligned}
A &= \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ y \in \mathbf{F}_q \setminus \{1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y-x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}((1-x)(1-w))}{s} \operatorname{ind}((1-x)w) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad \text{(by setting } w := (x-y)/(x-1)\text{)} \\
&= \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \operatorname{ind}\,(1-x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\quad + \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \operatorname{ind}\,(w) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad \text{(by Lemma 4.2.7, Lemma 4.2.4(9), and Lemma 4.2.4(6))} \\
&= \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \left((k+1) \binom{\operatorname{ind}(1-x)}{k+1} + k \binom{\operatorname{ind}(1-x)}{k} \right) \binom{\operatorname{ind}(1-w)}{s-k} \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\quad + \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \operatorname{ind}\,(w) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad \text{(by Lemma 4.2.4(4))} \\
&= \sum_{k=0}^{s} \left[\left(\sum_{w \in \mathbf{F}_q \setminus \{0,1\}} \binom{\operatorname{ind}(1-w)}{s-k} \right) \right. \\
&\quad \left. \times \left(\sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \binom{\operatorname{ind} x}{i-s} \left((k+1) \binom{\operatorname{ind}(1-x)}{k+1} + k \binom{\operatorname{ind}(1-x)}{k} \right) t^{\operatorname{ind} x} \right) \right] \\
&\quad + \sum_{k=0}^{s} \left(\sum_{w \in \mathbf{F}_q \setminus \{0,1\}} \operatorname{ind}\,(w) \binom{\operatorname{ind}(1-w)}{s-k} \right) \left(\sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \binom{\operatorname{ind} x}{i-s} \binom{\operatorname{ind}(1-x)}{k} t^{\operatorname{ind} x} \right) \\
&= \left(\sum_{k=0}^{s} T(0, s-k) \left((k+1) S(i-s, k+1) + k S(i-s, k) \right) \right) + \sum_{k=0}^{s} T(1, s-k) S(i-s, k) \\
&\qquad \text{(by definition of } S(u,v) \text{ and } T(u,v)\text{)} \\
&= -(s+1) S(i-s, s+1) - s S(i-s, s) + \sum_{k=0}^{s} T(1, s-k) S(i-s, k) \\
&\qquad \text{(by Lemma 4.2.15)} \\
&= -(s+1) S(i-s, s+1) - s S(i-s, s) + T(1, s) S(i-s, 0) + \sum_{k=1}^{s} T(1, s-k) S(i-s, k),
\end{aligned}$$

and we finish by substituting these expressions for A and B into (4.12). □

Corollary 4.2.22. *Suppose that $i \in [1, \ell - 2]$. Assume that $S(u, v) \in R'$ holds whenever $u + v \leq i$ and $v \geq 1$. Then for all $s \in [1, i]$,*

$$(i - s + 1)S(i - s + 1, s) \equiv (s + 1)S(i - s, s + 1) \pmod{R'}.$$

Proof. The assumptions imply that all the terms on the right hand side of Lemma 4.2.21 lie in R', so Lemma 4.2.21 implies the corollary. □

Corollary 4.2.23. *Suppose that $i \in [1, \ell - 2]$. Assume that $S(u, v) \in R'$ holds whenever $u + v \leq i$ and $v \geq 1$. Then if one of*

$$S(i, 1),\ S(i - 1, 2),\ \ldots,\ S(0, i + 1)$$

is in R', then they must all be in R'.

Proof. For $s \in [1, i]$, Corollary 4.2.23 implies

$$(i - s + 1)S(i - s + 1, s) \equiv (s + 1)S(i - s, s + 1) \pmod{R'},$$

so since $i - s + 1$ and $s + 1$ are invertible modulo ℓ (they lie in $[1, \ell - 1]$),

$$S(i - s + 1, s) \in R' \text{ if and only if } S(i - s, s + 1) \in R'.$$

Since this holds for all $s \in [1, i]$, we are done. □

4.2.7 Proof of main theorem

Now we combine all of our results from the previous sections in the following lemma.

Lemma 4.2.24. *For $k \in [1, \ell - 1]$, the following are equivalent:*

(1) *$S(0, 1), S(1, 1), \cdots, S(k - 2, 1)$ lie in R';*

(2) *$S(u, v)$ lies in R' for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq k - 1$;*

(3) *$S(0, 1), S(0, 2), \cdots, S(0, k - 1)$ lie in R';*

(4) *$J(\ell, f) + 1 \in \pi_\ell^k \mathcal{O}_L$.*

Proof. By Corollary 4.2.23, conditions Lemma 4.2.24(1) to Lemma 4.2.24(3) are equivalent. By Lemma 4.2.18(A), conditions Lemma 4.2.24(3) and Lemma 4.2.24(4) are equivalent. □

Theorem 4.2.25. *For $k \in [1, \ell - 1]$, the following are equivalent:*

(1) *$J(\ell, f) + 1 \in \pi_\ell^k \mathcal{O}_L$;*

(2) *$\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ for all $i \in [0, k - 2]$ and $j \in [1, f - 1]$;*

(3) *$\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ for all $i \in [0, k - 2]$ and $j \in [1, f/2]$.*

In particular, $J(\ell, f) + 1 \in \pi_\ell \mathcal{O}_L$ always holds.

Proof. Theorem 4.2.25(1) $\iff$ Theorem 4.2.25(2) follows by combining Lemma 4.2.20(A) and Lemma 4.2.24(1) $\iff$ Lemma 4.2.24(4).

Lemma 4.2.10(4) implies that for $i \in [0, \ell - 3]$ and $j \in [1, f/2]$, $\operatorname{ind} \eta_{i,f-j}$ is a linear combination of $\operatorname{ind}_{0,j}, \dots, \operatorname{ind}_{i,j}$ modulo ℓ, and this implies Theorem 4.2.25(2) $\iff$ Theorem 4.2.25(3). □

4.2.8 The case $k = \ell$

Lemma 4.2.26. *The following are equivalent.*

(1) $J(\ell, f) + 1 \in \pi_\ell^\ell \mathcal{O}_L$;

(2) $S(0,1),\ S(1,1),\ \cdots,\ S(\ell-3,1),\ S(\ell-2,1) + \dfrac{q-1}{\ell f}(1 + t + t^2 + \cdots + t^{f-1}) \in R'$.

Proof. By Lemma 4.2.18(B),

- $J(\ell, f) + 1 \in \pi_\ell^\ell \mathcal{O}_L$

is equivalent to

- $S(0,1), S(0,2), \dots, S(0, \ell-2)$ lie in R', and
- $S(0, \ell-1) - \frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by Lemma 4.2.24(3) $\iff$ Lemma 4.2.24(2), is equivalent to

- for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq \ell - 2$, $S(u,v)$ lies in R', and
- $S(0, \ell-1) - \frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by Corollary 4.2.22, is equivalent to

- for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq \ell - 2$, $S(u,v)$ lies in R',
- for all $s \in [1, \ell-2]$, $(\ell - 1 - s)S(\ell-1-s, s) \equiv (s+1)S(\ell-2-s, s+1) \pmod{R'}$, and
- $S(0, \ell-1) - \frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which is equivalent to

- for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq \ell - 2$, $S(u,v)$ lies in R',
- for all $s \in [1, \ell-2]$, $(\ell - 1 - s)S(\ell-1-s, s) \equiv (s+1)S(\ell-2-s, s+1) \pmod{R'}$, and
- $S(\ell-2, 1) - (-1)^{\ell-2}\frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by Corollary 4.2.22, is equivalent to

- for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq \ell - 2$, $S(u,v)$ lies in R',
- $S(\ell-2, 1) - (-1)^{\ell-2}\frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by Lemma 4.2.24(2) $\iff$ Lemma 4.2.24(1), is equivalent to

- $S(0,1), S(1,1), \dots, S(\ell-3, 1)$ lies in R',

- $S(\ell-2,1) - (-1)^{\ell-2}\frac{q-1}{\ell f}(1+t+\cdots+t^{f-1})$ lies in R',

and we are done by observing that $(-1)^{\ell-2} \equiv -1 \pmod{\ell}$. □

Lemma 4.2.27. *The following are equivalent:*

(1) $J(\ell,f)+1 \in \pi_\ell^\ell \mathcal{O}_L$;

(2) *All the following are divisible by* ℓ*:*

$$\begin{array}{cccc}
\operatorname{ind}(\eta_{0,1}) & \operatorname{ind}(\eta_{0,2}) & \dots & \operatorname{ind}(\eta_{0,f-1}) \\
\operatorname{ind}(\eta_{1,1}) & \operatorname{ind}(\eta_{1,2}) & \dots & \operatorname{ind}(\eta_{1,f-1}) \\
\vdots & \vdots & \ddots & \vdots \\
\operatorname{ind}(\eta_{\ell-3,1}) & \operatorname{ind}(\eta_{\ell-3,2}) & \dots & \operatorname{ind}(\eta_{\ell-3,f-1}) \\
\operatorname{ind}(\eta_{\ell-2,1}) + \frac{q-1}{\ell f} & \operatorname{ind}(\eta_{\ell-2,2}) + \frac{q-1}{\ell f} & \dots & \operatorname{ind}(\eta_{\ell-2,f-1}) + \frac{q-1}{\ell f}
\end{array}$$

Proof. Combine Lemma 4.2.20 and Lemma 4.2.26. □

Corollary 4.2.28. *The following are equivalent:*

(1) $J(\ell,f)+1 \in \pi_\ell^\ell \mathcal{O}_L$;

(2) $\frac{q-1}{\ell f} \equiv 0 \pmod{\ell}$ *and* $\operatorname{ind}(1-\xi_\ell^i \xi_f^j) \equiv 0 \pmod{\ell}$ *for all* $i \in [0,\ell-1]$ *and* $j \in [1,f-1]$;

(3) $\frac{q-1}{\ell f} \equiv 0 \pmod{\ell}$ *and* $\operatorname{ind}(1-\xi_\ell^i \xi_f^j) \equiv 0 \pmod{\ell}$ *for all for all* $i \in [0,\ell-1]$ *and* $j \in [1,f/2]$.

Proof.

(a) Corollary 4.2.28(2) $\implies$ Corollary 4.2.28(3)

This is obvious.

(b) Corollary 4.2.28(2) $\implies$ Corollary 4.2.28(1)

This follows from Lemma 4.2.10(3) and Lemma 4.2.27(2) $\implies$ Lemma 4.2.27(1).

(c) Corollary 4.2.28(3) $\implies$ Corollary 4.2.28(2)

Suppose that $i \in [0,\ell-1]$ and $j \in [f/2, f-1]$. Then

$$\begin{aligned}
&\operatorname{ind}\left(1-\xi_\ell^i \xi_f^j\right) \\
&\equiv \operatorname{ind}(-1) + i\left(\frac{q-1}{\ell f}\right) + \operatorname{ind}\left(1-\xi_\ell^{\ell-i}\xi_f^{f-j}\right) \pmod{\ell} \qquad \text{(by Lemma 4.2.10(6))} \\
&\equiv \operatorname{ind}(-1) \qquad \left(\text{since } \frac{q-1}{\ell f} \equiv 0 \pmod{\ell} \text{ and } f-j \in [1,f/2]\right). \qquad (4.13)
\end{aligned}$$

If $\ell = 2$, then $\operatorname{ind}(-1) = (q-1)/2 = (q-1)/\ell \equiv 0 \pmod{\ell}$ since $q-1 \equiv 0 \pmod{\ell^2 f}$ by assumption. If ℓ is odd, then $\operatorname{ind}(-1) = (q-1)/2 \equiv 0 \pmod{\ell}$ since $q-1 \equiv 0 \pmod{\ell}$ and 2 is coprime to ℓ. In any case, $\operatorname{ind}(-1) \equiv 0 \pmod{\ell}$ so we are done by (4.13).

(d) Corollary 4.2.28(1) $\Longrightarrow$ Corollary 4.2.28(2)

Lemma 4.2.27 implies that Lemma 4.2.27(2) holds. Substituting these congruences into Lemma 4.2.10(4) with $i = \ell - 2$ (and any value of j) yields

$$-\left(\frac{q-1}{\ell f}\right) \equiv -\left(\frac{q-1}{\ell f}\right) - (-1)^{\ell-2}\left(\frac{q-1}{\ell f}\right) \pmod{\ell},$$

which implies

$$\frac{q-1}{\ell f} \equiv 0 \pmod{\ell}.$$

Combining this with Lemma 4.2.27(2) implies that $\operatorname{ind} \eta_{k,j} \equiv 0 \pmod{\ell}$ for all $k \in [0, \ell-2]$ and $j \in [1, f-1]$, so Lemma 4.2.10(5) gives that $\operatorname{ind}\left(1 - \xi_\ell^i \xi_f^j\right) \equiv 0 \pmod{\ell}$ for all $i \in [1, \ell-1]$ and $j \in [1, f-1]$. □

Theorem 4.2.29. *The following are equivalent:*

(1) $J(\ell, f) + 1 \in \pi_\ell^\ell \mathcal{O}_L$

(2) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \xi_\ell^i \xi_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, \ell-1]$ *and* $j \in [1, f-1]$*;*

(3) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \xi_\ell^i \xi_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in [0, \ell-1]$ *and* $j \in [1, f/2]$*.*

Proof. This is a restatement of Corollary 4.2.28. □

Chapter 5

Torsion Points on Superelliptic Curves

As usual, we consider superelliptic curves $\mathcal{C}$ of the form $y^n = f(x)$ where $\deg f = d$ and $n, d \geq 2$ are coprime. The Abel–Jacobi map embeds $\mathcal{C}$ into its jacobian $\mathcal{J}$ by sending P to $[P - \infty]$. By a torsion point of $\mathcal{C}$, we mean a geometric point P of the curve such that the divisor class $[P - \infty]$ is torsion; i.e., $k[P - \infty] = 0$ for some positive integer k.

In Section 5.1, we summarize our new results and explain how they generalize previous results on torsion points in the hyperelliptic $n = 2$ case and their relationship with previous results on torsion points on Fermat curves.

In Section 5.2, we classify torsion points on the superelliptic "Catalan" curve $\mathcal{C}_{n,d}$ given by $y^n = x^d + 1$. In Section 5.3, we classify torsion points on an appropriate "generic" superelliptic curve.

The contents of this chapter are the same as that of my paper [6] on torsion points.

5.1 Summary of new results

Fix coprime integers $n, d \geq 2$. Let $\mathcal{C}_{n,d}$ be the smooth projective model of the Catalan curve

$$y^n = x^d + 1$$

in $\mathbf{A}^2_{\mathbf{C}}$. Then $\mathcal{C}_{n,d}$ has a unique point at infinity, denoted by ∞. Note that this curve is a quotient of the Fermat curve $X^{nd} + Y^{nd} + Z^{nd} = 0$.

Let $\mathcal{J}_{n,d}$ be the jacobian of $\mathcal{C}_{n,d}$. Then $\mathcal{C}_{n,d}$ naturally embeds into $\mathcal{J}_{n,d}$ via the map sending a point $P \in \mathcal{C}_{n,d}$ to the divisor class $[P - \infty] \in \mathcal{J}_{n,d}$. A point P of $\mathcal{C}_{n,d}(\mathbf{C})$ is called a torsion point if its image in $\mathcal{J}_{n,d}(\mathbf{C})$ is torsion, i.e., if there exists an integer $k \geq 1$ such that $[kP - k\infty] = 0$. We seek to classify the torsion points on $\mathcal{C}_{n,d}$.

For every $m \geq 2$, let $\zeta_m \in \mathbf{C}$ be a primitive mth root of unity. Let Z be the subgroup of $\mathrm{Aut}(\mathcal{C}_{n,d})$ generated by $(x, y) \mapsto (\zeta_d x, \zeta_n y)$. It is easy to check that any $P \in \mathcal{C}_{n,d}(\mathbf{C})$ fixed by some element of Z is a torsion point.

Definition 5.1.1. Call a torsion point of $\mathcal{C}_{n,d}$ an *exceptional* torsion point if it is not fixed by any element of Z.

Our main result is the following classification.

Theorem 5.2.73. *Suppose that n, d are coprime integers with $n, d \geq 2$.*

(1) *If* $(n,d) = (2,3)$*, then* $\mathcal{C}_{2,3}$ *is an elliptic curve, so it has infinitely many torsion points.*

(2) *If* $(n,d) = (2,5)$*, then the set of exceptional torsion points of* $\mathcal{C}_{2,5}$ *is the* Z*-orbit of* $(\sqrt[5]{4}, \sqrt{5})$*. Each has exact order* $(1-\zeta_5)^3$*; in particular, each is killed by* 5*.*

(3) *If* $(n,d) = (4,3)$*, then the set of exceptional torsion points of* $\mathcal{C}_{4,3}$ *is the* Z*-orbit of* $(2, \sqrt{3})$*. Each has exact order* $(1-\zeta_4)(1-\zeta_3)^2$*; in particular, each is killed by* 12*.*

(4) *If* $(n,d) \in \{(3,2),(5,2),(3,4)\}$*, then* $\mathcal{C}_{n,d} \simeq \mathcal{C}_{d,n}$ *via* $(x,y) \in \mathcal{C}_{n,d} \mapsto (\zeta_{2n}y, \zeta_{2d}x) \in \mathcal{C}_{d,n}$*, so the exceptional torsion points of* $\mathcal{C}_{n,d}$ *are described by one of Theorem 5.2.73(1), Theorem 5.2.73(2), Theorem 5.2.73(3).*

(5) *Otherwise,* $\mathcal{C}_{n,d}$ *has no exceptional torsion points.*

The case $(n,d) = (2,5)$ was already handled in the last two pages of [15]. The case when $n = 2$ and $d \geq 7$ is prime was already proven as Theorem 1.1 of [29].

Similar results are proven in [15, 16] for the Fermat curve F_m, which is given by the equation $X^m + Y^m + Z^m = 0$. These papers show that whenever P and Q are points of $F_m(\mathbf{C})$ such that $P - Q$ is torsion and P is a cusp (a point such that one of its coordinates is zero), then Q is also necessarily a cusp. Our result for $y^n = x^d + 1$ implies their result for F_{nd}.

The ideas in our proof of Theorem 5.2.73 are quite different from those used in [15]. The classification of torsion points on F_m in [15] uses Coleman integration, while we exploit the Galois action on torsion points. If P is a torsion point of $\mathcal{C}_{n,d}$, then so are all of its Galois conjugates. If the Galois action is large enough, there will be many relations among these torsion points, which will force low-degree maps to $\mathbf{P}^1$. Now we obtain consequences from these low-degree maps using two geometric techniques: the Castelnuovo–Severi inequality and Riemann's theorem on the sum of the Weierstrass weights on a Riemann surface. Eventually we reduce to checking finitely many points on finitely many $\mathcal{C}_{n,d}$, which we complete with the aid of a computer.

During the analysis, we work out explicitly the torsion field $\mathbf{Q}(\mathcal{J}_{p,q}[p], \mu_{pq})$ when p and q are distinct primes (see Theorem 5.2.28). The key ingredient is an understanding of the p-adic and q-adic valuation of certain Jacobi sums; this analysis is performed in Section 4.2. There is related work by Jędrzejak: in [37, 38] he studies $J(\mathbf{Q})_{\text{tors}}$ for the Jacobian J of the curve $y^q = x^p + a$, where $a \in \mathbf{Z}$.

Theorem 5.3.1 classifies the torsion points on the generic superelliptic curve $y^n = (x - a_1) \cdots (x - a_d)$ over $\mathbf{Q}(a_1, \ldots, a_d)$ in the case of coprime $n, d \geq 2$. This generalizes Theorem 7.1 of [57], which handles the $n = 2$ case. The key idea is to specialize to the curves $y^n = x^d + 1$ and $y^n = x^d + x$ and use Theorem 5.2.73.

Theorem 5.3.1. *Suppose that* $n, d \geq 2$ *are coprime and satisfy* $n + d \geq 7$*. Let* $\mathscr{C}_n$ *be the curve over* $k := \mathbf{Q}(a_1, \ldots, a_d)$ *defined by the equation*

$$y^n = \prod_{x=1}^{d} (x - a_i).$$

Suppose that $\mathscr{C}_n$ *is embedded into its jacobian* $\mathscr{J}_n$ *using the unique point* ∞ *at infinity. Points fixed by* ζ_n *are torsion points of order dividing* n*.*

(1) *If* $d \geq 3$*, there are no other torsion points defined over* $\overline{k}$*.*

(2) *If $d = 2$ and $n \neq 5$, the only other torsion points defined over $\overline{k}$ are*

$$\left\{ \left(\frac{a_1 + a_2}{2}, -\zeta_n^i \sqrt[n]{\left(\frac{a_1 - a_2}{2}\right)^2} \right) : 0 \leq i \leq n-1 \right\}.$$

(3) *If $d = 2$ and $n = 5$, the only other torsion points defined over $\overline{k}$ are*

$$\left\{ \left(\frac{a_1 + a_2}{2}, -\zeta_5^i \sqrt[5]{\left(\frac{a_1 - a_2}{2}\right)^2} \right) : 0 \leq i \leq 4 \right\} \bigcup$$
$$\left\{ \left(\frac{\pm(a_2 - a_1)\sqrt{5} + (a_1 + a_2)}{2}, \zeta_5^i \sqrt[5]{(a_2 - a_1)^2} \right) : 0 \leq i \leq 4 \right\}.$$

5.2 Torsion points on the Catalan curve $\mathcal{C}_{n,d}$

Let $\zeta_{nd} \in \overline{\mathbf{Q}}$ be a primitive ndth root of unity. Let

$$\begin{aligned} \zeta_n &:= \zeta_{nd}^d \\ \zeta_d &:= \zeta_{nd}^n \\ E &:= \mathbf{Q}(\zeta_{nd}) \\ \mathcal{O}_E &:= \mathbf{Z}[\zeta_{nd}]. \end{aligned}$$

Suppose that ξ_n and ξ_d are primitive nth and dth roots of unity respectively such that $\zeta_{nd} = \xi_n \xi_d$; then $\xi_n^d = \zeta_n$ and $\xi_d^n = \zeta_d$. We will abuse notation and define

$$\begin{aligned} \zeta_{nd} &:= \text{automorphism of } \mathcal{C}_{n,d} \text{ which sends } (x,y) \text{ to } (\xi_d x, \xi_n y) \\ \zeta_n &:= \zeta_{nd}^d, \text{ which is the automorphism of } \mathcal{C}_{n,d} \text{ which sends } (x,y) \text{ to } (x, \zeta_n y) \\ \zeta_d &:= \zeta_{nd}^n, \text{ which is the automorphism of } \mathcal{C}_{n,d} \text{ which sends } (x,y) \text{ to } (\zeta_d x, y) \\ Z &:= \text{the subgroup of } \operatorname{Aut}(\mathcal{C}_{n,d}) \text{ generated by } \zeta_{nd} \\ Z_n &:= \text{the subgroup of } Z \text{ generated by } \zeta_n \\ Z_d &:= \text{the subgroup of } Z \text{ generated by } \zeta_d. \end{aligned}$$

5.2.1 The homology of $\mathcal{C}_{n,d}$

Definition 5.2.1. Let R be the ring

$$R := \mathbf{Z}[T] / \left(1 + T^n + T^{2n} + \cdots + T^{(d-1)n}, 1 + T^d + T^{2d} + \cdots + T^{(n-1)d}\right).$$

Define

$$\varphi_{n,d}(T) := \frac{(T^{nd} - 1)(T - 1)}{(T^n - 1)(T^d - 1)} \in \mathbf{Z}[T].$$

Lemma 5.2.2. *For integers $a, b \geq 1$, define the ideal*

$$I_{a,b} := \left(1 + T + \cdots + T^{a-1}, 1 + T + \cdots + T^{b-1}\right)$$

of $\mathbf{Z}[T]$*. Then* $I_{a,b}$ *is generated by* $1+T+\cdots+T^{\gcd(a,b)-1}$.

Proof. If $a \geq b$, then

$$1+T+\cdots+T^{a-b-1} = (1+T+\cdots+T^{a-1}) - T^{a-b}(1+T+\cdots+T^{b-1})$$

implies $I_{a,b} = I_{a-b,b}$, so by the Euclidean algorithm, $I_{a,b} = T_{\gcd(a,b),0}$. □

Corollary 5.2.3.

(1) $R \simeq \mathbf{Z}[T]/(\varphi_{n,d}(T))$.

(2) $\{T^{da+nb} \colon a \in [0, d-2]$ *and* $j \in [0, n-2]\}$ *is a* $\mathbf{Z}$*-basis of* R.

Proof.

(1) Lemma 5.2.2 implies $I_{n,d}$ is the unit ideal, so

$$\begin{aligned}(\varphi_{n,d}(T)) &= \varphi_{n,d}(T)\,(I_{n,d}) \\ &= \frac{(T^{nd}-1)(T-1)}{(T^n-1)(T^d-1)}\left(\frac{T^n-1}{T-1}, \frac{T^d-1}{T-1}\right) \\ &= \left(\frac{T^{nd}-1}{T^d-1}, \frac{T^{nd}-1}{T^n-1}\right) \\ &= \left(1+T^d+T^{2d}+\cdots+T^{(n-1)d}, 1+T^n+T^{2n}+\cdots+T^{(d-1)n}\right),\end{aligned}$$

so applying this to the definition of R yields $R \simeq \mathbf{Z}[T]/(\varphi_{n,d}(T))$.

(2) For nonnegative integers u, v, define $B_{u,v} := \{T^{da+nb} \colon a \in [0,u]$ and $j \in [0,v]\}$. Since $T^{nd} = 1$ in R and the set $\{da + nb : a \in [0, n-1]$ and $b \in [0, d-1]\}$ contains every residue class modulo nd, $B_{n-1,d-1}$ must generate R as a $\mathbf{Z}$-module. Using $1+T^n+T^{2n}+\cdots+T^{(d-1)n} = 0$ and $1+T^d+T^{2d}+\cdots+T^{(n-1)d} = 0$ shows that $B_{n-2,d-2}$ generates R as a $\mathbf{Z}$-module. Corollary 5.2.3(1) implies that R is a free $\mathbf{Z}$-module of rank $\deg\varphi_{n,d} = (n-1)(d-1) = \#S_{n-2,d-2}$, so $S_{n-2,d-2}$ must be a basis. □

Proposition 5.2.4. $H_1(\mathcal{C}_{n,d}, \mathbf{Z})$ *is a free* R*-module of rank 1 for which* T *acts by* ζ_{nd}.

Proof. We apply the results of Section 2.5. Our basepoint will be $B := (0,1)$. Choose $\alpha_1 \in \mathbf{C}$ to be a root of $(-x)^d + 1 = 0$, and define $\alpha_i := \zeta_d^{i-1}\alpha_1$. Let β_1 be a loop in $\mathbf{P}^1 \setminus \{-\alpha_1, \ldots, -\alpha_d, \infty\}$ starting and ending at 0 which encircles $-\alpha_1$ positively and does not encircle any of $\{-\alpha_2, \ldots, -\alpha_d, \infty\}$. Define $\beta_i := \zeta_d^{i-1}\beta_1$. As in Definition 2.5.1, for $i \in [1,d]$ and $j \in [0, n-1]$, define $\psi_{i,j} \in H_1(\mathcal{C}_{n,d}, \mathbf{Z})$ to be the cycle $\zeta_n^j[\beta_i\beta_{i+1}^{-1}]$. Therefore,

$$\psi_{i,j} = \zeta_n^j \zeta_d^{i-1}\psi_{1,0},$$

so Proposition 2.5.4 implies that $\{\zeta_n^j\zeta_d^{i-1}\psi_{1,0} \colon i \in [1, d-1]$ and $j \in [0, n-2]\}$ is a $\mathbf{Z}$-basis for $H_1(\mathcal{C}_{n,d}, \mathbf{Z})$. Lemma 2.5.2 and Lemma 2.5.3 give the relations

$$\begin{aligned}(1+\zeta_n+\cdots+\zeta_n^{n-1})\gamma_{1,0} = 0, \\ (1+\zeta_d+\cdots+\zeta_d^{d-1})\gamma_{1,0} = 0,\end{aligned}$$

so there is an R-module map $R \to H_1(\mathcal{C}_{n,d}, \mathbf{Z})$ sending 1 to $\gamma_{1,0}$. The $\mathbf{Z}$-basis of R given in Corollary 5.2.3(2) gets mapped to the $\mathbf{Z}$-basis $\{\zeta_n^a \zeta_d^b \gamma_{1,0} \colon a \in [0, d-2] \text{ and } b \in [0, n-2]\}$ of $H_1(\mathcal{C}_{n,d}, \mathbf{Z})$, so this is an isomorphism. □

Corollary 5.2.5. *The map* $\mathbf{Z}[T] \to \operatorname{End} \mathcal{J}_{n,d}$ *sending* T *to* ζ_{nd} *has kernel* $(\varphi_{n,d}(T))$.

Proof. By Proposition 5.2.4, the composite map $\mathbf{Z}[T] \to \operatorname{End} \mathcal{J}_{n,d} \to \operatorname{End} H_1(\mathcal{J}_{n,d}, \mathbf{Z}) = \operatorname{End} H_1(\mathcal{C}_{n,d}, \mathbf{Z})$ has kernel equal to $(\varphi_{n,d}(T))$. Since the map $\operatorname{End} \mathcal{J}_{n,d} \to \operatorname{End} H_1(\mathcal{J}_{n,d}, \mathbf{Z})$ is injective, we are done. □

In view of Corollary 5.2.5, we will view R as the subring of $\operatorname{End} \mathcal{J}_{n,d}$ generated by Z.

5.2.2 The structure of $T_\ell \mathcal{J}_{n,d}$ as a Galois representation

Let ℓ be a prime and λ be a prime of E lying above ℓ. Let $r \nmid \ell nd$ be another prime and $\mathfrak{r}$ be a prime of E lying above r. Define $\mathbf{F}_\mathfrak{r}$ to be the residue field at $\mathfrak{r}$. Define $\operatorname{Frob}_\mathfrak{r} \in \operatorname{Gal}(E(\mathcal{J}_{n,d}[\ell^\infty])/E)$ to be the Frobenius automorphism for $\mathfrak{r}$; it is well-defined since the extension $E(\mathcal{J}_{n,d}[\ell^\infty])/E$ is unramified because $\mathcal{C}_{n,d}$ has good reduction at ℓ.

Define

$$\begin{aligned} T_\ell \mathcal{J}_{n,d} &:= \text{the Tate module } \varprojlim_i \mathcal{J}_{n,d}[\ell^i] \\ V_\ell \mathcal{J}_{n,d} &:= \text{the rational Tate module } (T_\ell \mathcal{J}_{n,d}) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \\ R_\ell &:= R \otimes_{\mathbf{Z}} \mathbf{Z}_\ell. \end{aligned}$$

Definition 5.2.6. Define $\operatorname{End}_{R_\ell}(T_\ell \mathcal{J}_{n,d})$ to be the ring of endomorphisms of $T_\ell \mathcal{J}_{n,d}$ that commute with ζ_{nd}.

Lemma 5.2.7. *$T_\ell \mathcal{J}_{n,d}$ is free R_ℓ-module of rank 1. Hence,*

$$\operatorname{Aut}_{R_\ell}(T_\ell \mathcal{J}_{n,d}) \simeq R_\ell^\times, \tag{5.1}$$

$$\operatorname{End}_{R_\ell}(T_\ell \mathcal{J}_{n,d}) \simeq R_\ell. \tag{5.2}$$

Proof. Proposition 5.2.4 gives that $H_1(\mathcal{C}_{n,d}, \mathbf{Z})$ is a free R-module of rank 1, so $T_\ell \mathcal{J}_{n,d} \simeq H_1(\mathcal{C}_{n,d}, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ is a free R_ℓ-module of rank 1, and this implies (5.1) and (5.2). □

Definition 5.2.8. Using (5.1), define

$$\theta_\ell \colon \operatorname{Gal}(E(\mathcal{J}_{n,d}[\ell^\infty])/E) \hookrightarrow \operatorname{Aut}_{R_\ell}(T_\ell \mathcal{J}_{n,d}) \simeq R_\ell^\times$$

to be the injective group homomorphism which sends each element of $\operatorname{Gal}(E(\mathcal{J}_{n,d}[\ell^\infty])/E)$ to its action on $T_\ell \mathcal{J}_{n,d}$. Extend θ_ℓ linearly to a ring homomorphism

$$\theta_\ell \colon \mathbf{Z}_\ell[\operatorname{Gal}(E(\mathcal{J}_{n,d}[\ell^\infty])/E)] \to \operatorname{End}_{R_\ell}(T_\ell \mathcal{J}_{n,d}) \simeq R_\ell.$$

Remark 5.2.9. When $n = p$ is prime, recall that θ_p was previously defined in Definition 2.5.9 as a map from $\mathbf{Z}_p[\operatorname{Gal}(\mathbf{Q}(\mu_p, \mathcal{J}_{p,d}[p^\infty])/\mathbf{Q}(\mu_p))]$, but we are now defining θ_p to be its restriction to the subring $\mathbf{Z}_p[\operatorname{Gal}(E(\mathcal{J}_{p,d}[p^\infty])/E)]$; this is a subring because the field of definition of $\mathcal{J}_{p,d}[p^\infty] \supseteq \mathcal{J}_{p,d}[1-\zeta_p]$ contains $\mathbf{Q}(\mu_d)$, so $\mathbf{Q}(\mu_p, \mathcal{J}[p^\infty])$ does contain E.

Lemma 5.2.10. *Suppose that $n = p$ is prime. Then $\gamma \in \mathbf{Z}_p\left[\operatorname{Gal}\left(E(\mathcal{J}_{p,d}[p^\infty])/E\right)\right]$ kills $\mathcal{J}_{p,d}[(1-\zeta_p)^i]$ if and only if*

$$\theta_p(\gamma) \in (1-\zeta_p)^i R_p.$$

Proof. Since $T_p\mathcal{J}_{p,d}$ is a free R_p-module of rank 1 by Lemma 5.2.7, this lemma is proved in the same way as Corollary 2.5.10. □

Lemma 5.2.11. *For each positive integer m, $\operatorname{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right)$ is abelian.*

Proof. Using the fact that the θ_ℓ are injective, we see that

$$\operatorname{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right) \hookrightarrow \prod_{\ell \mid m} \operatorname{Gal}\left(E(\mathcal{J}_{n,d}[\ell^\infty])/E\right) \hookrightarrow \prod_{\ell \mid m} R_\ell^\times,$$

so we are done since $R_\ell^\times$ is abelian. □

Definition 5.2.12. Suppose that $\mathbf{F}_Q$ is a finite field and that $\mathcal{S}$ is a ring. Suppose that $\chi_1, \chi_2 \colon \mathbf{F}_Q^\times \to \mathcal{S}^\times$ are nontrivial characters. For each integer $k \geq 1$, define the Jacobi sum

$$J_k(\chi_1,\chi_2) := \sum_{\alpha \in \mathbf{F}_{Q^k} \setminus \{0,1\}} \chi_1\left(\alpha^{(Q^k-1)/(Q-1)}\right) \chi_2\left((1-\alpha)^{(Q^k-1)/(Q-1)}\right).$$

Definition 5.2.13. Define natural isomorphisms

$$\kappa_{n,\mathfrak{r}} \colon \mu_n(\mathbf{F}_\mathfrak{r}) \to Z_n$$
$$\kappa_{d,\mathfrak{r}} \colon \mu_d(\mathbf{F}_\mathfrak{r}) \to Z_d.$$

Compose the "exponentiation by $(\#\mathbf{F}_\mathfrak{r} - 1)/n$" map and $\kappa_{n,\mathfrak{r}}$ to define

$$\gamma_{n,\mathfrak{r}} \colon \mathbf{F}_\mathfrak{r}^\times \to \mu_n(\mathbf{F}_\mathfrak{r}) \to Z_n.$$

In an analogous fashion, define the composite morphism

$$\gamma_{d,\mathfrak{r}} \colon \mathbf{F}_\mathfrak{r}^\times \to \mu_d(\mathbf{F}_\mathfrak{r}) \to Z_d.$$

Definition 5.2.14. For characters $\rho_n \colon Z_n \to E^\times$ and $\rho_d \colon Z_d \to E^\times$, use $(V_\ell\mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ to denote the (ρ_n,ρ_d)-isotypic component of $(V_\ell\mathcal{J}_{n,d}) \otimes_{\mathbf{Q}_\ell} E_\lambda$, i.e.,

$$(V_\ell\mathcal{J}_{n,d})^{(\rho_n,\rho_d)} := \left\{ v \in (V_\ell\mathcal{J}_{n,d}) \otimes_{\mathbf{Q}_\ell} E_\lambda : \begin{array}{l} z_n(v) = \rho_n(z_n)v \text{ for all } z_n \in Z_n \\ z_d(v) = \rho_d(z_d)v \text{ for all } z_d \in Z_d \end{array} \right\}.$$

Proposition 5.2.15.

(1) *There is a direct sum decomposition*

$$(V_\ell\mathcal{J}_{n,d}) \otimes_{\mathbf{Q}_\ell} E_\lambda \simeq \bigoplus_{\substack{\rho_n \colon Z \to E^\times \\ \rho_d \colon Z \to E^\times}} (V_\ell\mathcal{J}_{n,d})^{(\rho_n,\rho_d)}.$$

(2) *The $\mathbf{Q}_\ell$-dimension of $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ is*

$$\dim_{\mathbf{Q}_\ell} (V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)} = \begin{cases} 1 & \text{if } \rho_n \neq 1 \text{ and } \rho_d \neq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Proposition 5.2.15(1) is just representation theory (c.f. page 172 of [41]).

By Proposition 5.2.4 and Corollary 5.2.3(1), we know that the characteristic polynomial of ζ_{nd} on $H_1(\mathcal{C}_{n,d}, \mathbf{Z})$ is $\varphi_{n,d}(T)$, so the eigenvalues of ζ_{nd} on $T_\ell \mathcal{J}_{n,d} = H_1(\mathcal{C}_{n,d}, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ are $\mu_{nd}(\overline{\mathbf{Q}_\ell}) \setminus \left(\mu_n(\overline{\mathbf{Q}_\ell}) \cup \mu_d(\overline{\mathbf{Q}_\ell})\right)$; Proposition 5.2.15(2) follows. □

Proposition 5.2.16. *Suppose that $\rho_n \colon Z_n \to E^\times$ and $\rho_d \colon Z_d \to E^\times$ are nontrivial multiplicative characters.*

(1) *Let $\chi_{n,\mathfrak{r}} = \rho_n \circ \gamma_{n,\mathfrak{r}}$ and $\chi_{d,\mathfrak{r}} = \rho_d \circ \gamma_{d,\mathfrak{r}}$. Then the eigenvalue of* $\operatorname{Frob}_\mathfrak{r}$ *acting upon $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ is*
$$-\chi_{d,\mathfrak{r}}(-1) J_1(\chi_{n,\mathfrak{r}}, \chi_{d,\mathfrak{r}}).$$

(2) *Let $\gamma'_{n,\mathfrak{r}} \colon \mathbf{F}_\mathfrak{r}^\times \to R^\times$ be the composite of $\gamma_{n,\mathfrak{r}}$ with the inclusion $Z_n \subseteq R^\times$. Define $\gamma'_{d,\mathfrak{r}}$ similarly. Then*
$$\theta_\ell\left(\operatorname{Frob}_\mathfrak{r}\right) = -\gamma'_{d,\mathfrak{r}}(-1) J_1(\gamma'_{n,\mathfrak{r}}, \gamma'_{d,\mathfrak{r}}) \in R. \tag{5.3}$$

Proof. We apply the results in Section 1 of Katz [41] to the group Z acting on the curve $\mathcal{C}_{n,d,\mathfrak{r}}$, which is the reduction of $\mathcal{C}_{n,d}$ at the prime ideal $\mathfrak{r}$.

Define $\rho \colon Z \to E^\times$ to be the character that restricts to ρ_n on Z_n and to ρ_d on Z_d. As on page 172 of [41], for every integer $k \geq 1$, define $\operatorname{Fix}\left(\operatorname{Frob}_\mathfrak{r}^k z^{-1}\right)$ to be the subset of $\mathcal{C}_{n,d,\mathfrak{r}}(\overline{\mathbf{F}_\mathfrak{r}})$ fixed by $\operatorname{Frob}_\mathfrak{r}^k z^{-1}$ and

$$\begin{aligned} S(\rho, k) &:= \frac{1}{\#Z} \sum_{z \in Z} \rho(z) \# \operatorname{Fix}\left(\operatorname{Frob}_\mathfrak{r}^k z^{-1}\right) \\ &= \frac{1}{\#Z} \sum_{P \in \mathcal{C}_{n,d,\mathfrak{r}}(\overline{\mathbf{F}_\mathfrak{r}})} \sum_{\substack{z \in Z \\ \operatorname{Frob}_\mathfrak{r}^k z^{-1} P = P}} \rho(z). \end{aligned} \tag{5.4}$$

Claim. Let $Q = \#\mathbf{F}_\mathfrak{r}$. For every $k \geq 1$, we have

$$S(\rho, k) = (\chi_{d,\mathfrak{r}}(-1))^{(Q^k-1)/(Q-1)} J_k(\chi_{n,\mathfrak{r}}, \chi_{d,\mathfrak{r}}).$$

Proof of claim. Suppose that $P \in \mathcal{C}_{n,d,\mathfrak{r}}(\overline{\mathbf{F}_\mathfrak{r}})$ is fixed by Z_n. Then $\{z \in Z \colon \operatorname{Frob}_\mathfrak{r}^k z^{-1} P = P\}$ will be a union of cosets for the subgroup Z_n of Z. Since $\rho_n \neq 1$, the sum of $\rho(z)$ for any coset of Z_n is zero, and hence the inner sum of (5.4) is zero. Hence we may ignore P that are fixed by Z_n. Similarly, we may also ignore P that are fixed by Z_d. Therefore, we may restrict to the subset

$$\begin{aligned} \mathcal{C}_{n,d,\mathfrak{r}}(\overline{\mathbf{F}_Q})^* &:= \{P \in \mathcal{C}_{n,d,\mathfrak{r}}(\overline{\mathbf{F}_Q}) \colon P \text{ is not fixed by } Z_n \text{ nor by } Z_d\} \\ &= \{(x,y) \in \overline{\mathbf{F}_\mathfrak{r}}^\times \times \overline{\mathbf{F}_\mathfrak{r}}^\times \colon y^n = x^d + 1\}. \end{aligned}$$

Suppose that $P = (x,y) \in \mathcal{C}_{n,d,\mathfrak{r}}(\overline{\mathbf{F}_Q})^*$ and that $z \in Z$ satisfy $\operatorname{Frob}_\mathfrak{r}^k z^{-1} P = P$. Since $\mathbf{F}_\mathfrak{r}$ contains an ndth root of unity, $\operatorname{Frob}_\mathfrak{r}^k$ and z^{-1} commute, so this is equivalent to $\operatorname{Frob}_\mathfrak{r}^k(x,y) =$

$z(x,y)$. Since z scales the x-coordinate by a dth root of unity and scales the y-coordinate by a nth root of unity, we see that x^d, y^n are both fixed by $\mathrm{Frob}_{\mathfrak{r}}^k$. Define $\alpha := y^n = x^d + 1$, so that α is fixed by $\mathrm{Frob}_{\mathfrak{r}}^k$. Also, $\alpha \notin \{0,1\}$ since $x, y \neq 0$. Rewrite (5.4) as

$$S(\rho,k) = \frac{1}{\#Z} \sum_{\substack{\alpha \in \overline{\mathbf{F}_{\mathfrak{r}}} \setminus \{0,1\} \\ \mathrm{Frob}_{\mathfrak{r}}^k\, \alpha = \alpha}} \sum_{\substack{(x,y,z) \in \overline{\mathbf{F}_{\mathfrak{r}}}^{\times} \times \overline{\mathbf{F}_{\mathfrak{r}}}^{\times} \times Z \\ \mathrm{Frob}_{\mathfrak{r}}^k\, z^{-1}(x,y) = (x,y) \\ \alpha = y^n = x^d + 1}} \rho(z).$$

Define $z_n \in Z_n$ and $z_d \in Z_d$ such that $z = z_n z_d$. By definition of $\kappa_{n,\mathfrak{r}}$ and $\kappa_{d,\mathfrak{r}}$, we know that $z(x,y) = \left(\kappa_{d,\mathfrak{r}}^{-1}(z_d)x, \kappa_{n,\mathfrak{r}}^{-1}(z_n)y\right)$, so the condition that $\mathrm{Frob}_{\mathfrak{r}}^k(x,y) = z(x,y)$ is equivalent to the two conditions $x^{Q^k} = \kappa_{d,\mathfrak{r}}^{-1}(z_d)x$ and $y^{Q^k} = \kappa_{n,\mathfrak{r}}^{-1}(z_d)y$, which is equivalent to the two conditions $z_d = \kappa_{d,\mathfrak{r}}(x^{Q^k-1})$ and $z_n = \kappa_{n,\mathfrak{r}}(y^{Q^k-1})$, which by definition of α, is equivalent to $z_d = \kappa_{d,\mathfrak{r}}((\alpha-1)^{(Q^k-1)/d})$ and $z_n = \kappa_{n,\mathfrak{r}}(\alpha^{(Q^k-1)/n})$, which uniquely determines z. Since $\rho(z) = \rho(z_n z_d) = \rho_n(z_n)\rho_d(z_d)$, we may rewrite the sum as

$$S(\rho,k) = \frac{1}{\#Z} \sum_{\substack{\alpha \in \overline{\mathbf{F}_{\mathfrak{r}}} \setminus \{0,1\} \\ \mathrm{Frob}_{\mathfrak{r}}^k\, \alpha = \alpha}} \sum_{\substack{(x,y) \in \overline{\mathbf{F}_{\mathfrak{r}}}^{\times} \times \overline{\mathbf{F}_{\mathfrak{r}}}^{\times} \\ \alpha = y^n = x^d + 1}} \rho_n\left(\kappa_{n,\mathfrak{r}}(\alpha^{(Q^k-1)/n})\right) \rho_d\left(\kappa_{d,\mathfrak{r}}((\alpha-1)^{(Q^k-1)/d})\right).$$

For each α, there are $nd = \#Z$ pairs $(x,y) \in \overline{\mathbf{F}_{\mathfrak{r}}}^{\times} \times \overline{\mathbf{F}_{\mathfrak{r}}}^{\times}$ satisfying $y^n = x^d + 1$, so we simplify to

$$S(\rho,k) = \sum_{\substack{\alpha \in \overline{\mathbf{F}_{\mathfrak{r}}} \setminus \{0,1\} \\ \mathrm{Frob}_{\mathfrak{r}}^k\, \alpha = \alpha}} \rho_n\left(\kappa_{n,\mathfrak{r}}(\alpha^{(Q^k-1)/n})\right) \rho_d\left(\kappa_{d,\mathfrak{r}}((\alpha-1)^{(Q^k-1)/d})\right).$$

By definition of $\chi_{n,\mathfrak{r}}$, we know that $\chi_{n,\mathfrak{r}}(\alpha) = \rho_n(\gamma_{n,\mathfrak{r}}(\alpha)) = \rho_n\left(\kappa_{n,\mathfrak{r}}\left(\alpha^{(Q-1)/n}\right)\right)$. A similar statement holds for $\chi_{d,\mathfrak{r}}$, so this sum equals

$$\begin{aligned} S(\rho,k) &= \sum_{\substack{\alpha \in \overline{\mathbf{F}_{\mathfrak{r}}} \setminus \{0,1\} \\ \mathrm{Frob}_{\mathfrak{r}}^k\, \alpha = \alpha}} \chi_{n,\mathfrak{r}}\left(\alpha^{(Q^k-1)/(Q-1)}\right) \chi_{d,\mathfrak{r}}\left((\alpha-1)^{(Q^k-1)/(Q-1)}\right) \\ &= (\chi_{d,\mathfrak{r}}(-1))^{(Q^k-1)/(Q-1)} \sum_{\substack{\alpha \in \overline{\mathbf{F}_{\mathfrak{r}}} \setminus \{0,1\} \\ \mathrm{Frob}_{\mathfrak{r}}^k\, \alpha = \alpha}} \chi_{n,\mathfrak{r}}\left(\alpha^{(Q^k-1)/(Q-1)}\right) \chi_{d,\mathfrak{r}}\left((1-\alpha)^{(Q^k-1)/(Q-1)}\right) \\ &= (\chi_{d,\mathfrak{r}}(-1))^{(Q^k-1)/(Q-1)} J_k(\chi_{n,\mathfrak{r}}, \chi_{d,\mathfrak{r}}) \end{aligned}$$

by definition of the Jacobi sum (Definition 5.2.12). So **the proof of the claim is complete.**

Theorem 2.1.3(b) of [11] implies that $|J_k(\chi_n, \chi_d)| = Q^{k/2}$, so by the claim, $|S(\rho,k)| = Q^{k/2}$. Using Lemma 1.1 of [41] (3) $\iff$ (6), the eigenvalue of $\mathrm{Frob}_{\mathfrak{r}}$ on $(V_\ell \mathcal{J}_{n,d,\mathfrak{r}})^{(\rho_n,\rho_d)}$ is $-S(\rho,1) = -\chi_{d,\mathfrak{r}}(-1)J_1(\chi_{n,\mathfrak{r}}, \chi_{d,\mathfrak{r}})$, which gives Proposition 5.2.16(1).

We may check Proposition 5.2.15(2) after tensoring up to E_λ to work with $(V_\ell \mathcal{J}_{n,d}) \otimes_{\mathbf{Q}_\ell} E_\lambda$, and Proposition 5.2.15 implies that it is sufficient to check this on each $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ whenever $\rho_n, \rho_d \neq 1$. For any $z_n \in Z_n$, the eigenvalue of z_n on $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ is $\rho_n(z_n)$, so the eigenvalue of $\gamma'_{n,\mathfrak{r}}(\alpha)$ acting on $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ is $\rho_n(\gamma_{n,\mathfrak{r}}(\alpha)) = \chi_{n,\mathfrak{r}}(\alpha)$ (and similarly for

$\gamma'_{d,\mathfrak{r}}(1-\alpha))$, meaning that the right hand side of (5.3) acts on $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ by the scalar $-\chi_{n,\mathfrak{r}}(-1)J_1(\chi_{n,\mathfrak{r}},\chi_{d,\mathfrak{r}})$, so we are done by Proposition 5.2.16(1). □

Definition 5.2.17. By Galois theory, $\mathrm{Gal}(E(\mathcal{J}_{n,d}[m^\infty])/\mathbf{Q})$ acts by conjugation on the subgroup $\mathrm{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right)$. By Lemma 5.2.11, the subgroup $\mathrm{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right)$ is abelian, so this action factors through an action of $\mathrm{Gal}(E/\mathbf{Q})$ on $\mathrm{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right)$. For any $h \in \mathrm{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right)$ and $\gamma \in \mathrm{Gal}(E/\mathbf{Q})$, write ${}^\gamma h$ to denote the action of γ on h. Let $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$ be complex conjugation.

Proposition 5.2.18. *$\mathrm{Frob}_\mathfrak{r} \cdot {}^\sigma\mathrm{Frob}_\mathfrak{r}$ acts on $T_\ell \mathcal{J}_{n,d}$ as multiplication by $\#\mathbf{F}_\mathfrak{r}$.*

Proof. By Proposition 5.2.15, we may as well verify this on each eigenspace $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$. Apply σ to everything in Proposition 5.2.16 to see that $\mathrm{Frob}_{\sigma(\mathfrak{r})}$ acts on $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ as multiplication by $\chi_{d,\sigma(\mathfrak{r})}(-1)J_1\left(\chi_{n,\sigma(\mathfrak{r})},\chi_{d,\sigma(\mathfrak{r})}\right) = \sigma\left(\chi_{d,\mathfrak{r}}(-1)J_1(\chi_{n,\mathfrak{r}},\chi_{d,\mathfrak{r}})\right)$, implying that $\mathrm{Frob}_\mathfrak{r} \cdot {}^\sigma\mathrm{Frob}_\mathfrak{r} = \mathrm{Frob}_\mathfrak{r}\,\mathrm{Frob}_{\sigma(\mathfrak{r})}$ acts on $(V_\ell \mathcal{J}_{n,d})^{(\rho_n,\rho_d)}$ as multiplication by $J_1(\chi_{n,\mathfrak{r}},\chi_{d,\mathfrak{r}}) \cdot \sigma\left(J_1(\chi_{n,\mathfrak{r}},\chi_{d,\mathfrak{r}})\right)$, which equals $\#\mathbf{F}_\mathfrak{r}$ by Theorem 2.1.3(b) of [11]. □

Corollary 5.2.19. *Let m be a nonnegative integer and let $h \in \mathrm{Gal}(E(\mathcal{J}_{n,d}[m^\infty])/E)$. By the Weil pairing, $E(\mathcal{J}_{n,d}[m^\infty])$ contains $E(\mu_{m^\infty})$, so suppose that h acts on μ_{m^∞} as multiplication by c. Then $h \cdot {}^\sigma h$ acts on $\mathcal{J}[m^\infty]$ as multiplication by c.*

Proof. Frobenius elements are dense by the Chebotarev density theorem, so we reduce to checking on $h = \mathrm{Frob}_\mathfrak{r}$. By definition of Frobenius, h acts on μ_{m^∞} as multiplication by $\#\mathbf{F}_\mathfrak{r}$, so we are done by applying Proposition 5.2.18 to every prime ℓ dividing m. □

5.2.3 Bounding the order of torsion points on $\mathcal{C}_{n,d}$

Corollary 5.2.20. *Let m be a positive integer. For every prime ℓ dividing m, let $c_\ell \in \mathbf{Z}_\ell^\times$; if $\ell | nd$, assume that $c_\ell \in 1 + nd\mathbf{Z}_\ell$. Then there exists an element τ of $\mathrm{Gal}\left(E(\mathcal{J}_{n,d}[m^\infty])/E\right)$ such that for each ℓ dividing m, τ acts on $\mathcal{J}[\ell^\infty]$ as multiplication by c_ℓ.*

Proof. The assumptions on c_ℓ imply that there exists an element of $\gamma \in \mathrm{Gal}\left(E(\mu_{m^\infty})/E\right)$ such that for each prime ℓ dividing m, γ acts on μ_{ℓ^∞} as multiplication by c_ℓ. Lift γ arbitrarily to $h \in \mathrm{Gal}(E(\mathcal{J}_{n,d}[m^\infty])/E)$, define $\tau := h \cdot {}^\gamma h$, and apply Corollary 5.2.19 to finish. □

Definition 5.2.21. Let $P \in \mathcal{C}_{n,d}$ be a torsion point.

Proposition 5.2.22. *Suppose that $\mathcal{C}_{n,d}$ has genus $g > 1$ (i.e., $(n,d) \notin \{(2,3),(3,2)\}$). Let $m = \mathrm{lcm}(2, nd)$.*

(i) *If $(n,d) \notin \{(2,5),(4,5),(5,2),(5,4)\}$ then $m(P-\infty) \sim 0$.*

(ii) *If $(n,d) \in \{(2,5),(5,2),(4,5),(5,4)\}$ then $3m(P-\infty) \sim 0$.*

Proof. Without loss of generality, assume that d is odd. Choose an integer M such that $M(P-\infty) \sim 0$. Assume that M is divisible by m. Define

$$\mathcal{R} := \{\text{prime } r \colon r \nmid 2nd \text{ and } r | M\},$$
$$\mathcal{S} := \{\text{prime } s \colon s \nmid 2 \text{ and } s \mid nd\},$$

so that the set of primes dividing M is the disjoint union $\{2\} \cup \mathcal{R} \cup \mathcal{S}$. For any prime a dividing M, let e_a be the largest integer such that $a^{e_a} | nd$ and define $D_a \in \mathcal{J}_{n,d}[a^\infty]$ such that

$$[P - \infty] = \sum_{a|M} D_a.$$

By definition of m,

$$m = 2^{\max\{1,e_2\}} \left(\prod_{s \in \mathcal{S}} s^{e_s} \right). \tag{5.5}$$

Using Corollary 5.2.20, choose $\tau_1, \tau_2, \tau_3 \in \mathrm{Gal}(E(\mathcal{J}_{n,d}[M^\infty])/E)$ such that:

$$\tau_1 \text{ acts on } \begin{cases} \mathcal{J}_{n,d}[2^\infty] & \text{as multiplication by } 1 + 2^{\max\{1,e_2\}} \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } 2 \text{ for each } r \in \mathcal{R} \\ \mathcal{J}_{n,d}[s^\infty] & \text{as multiplication by } 1 + s^{e_s} \text{ for each } s \in \mathcal{S} \end{cases}$$

$$\tau_2 \text{ acts on } \begin{cases} \mathcal{J}_{n,d}[2^\infty] & \text{as multiplication by } 1 - 2^{\max\{1,e_2\}} \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } -2 \text{ for each } r \in \mathcal{R} \\ \mathcal{J}_{n,d}[s^\infty] & \text{as multiplication by } 1 - s^{e_s} \text{ for each } s \in \mathcal{S} \end{cases}$$

$$\tau_3 \text{ acts on } \begin{cases} \mathcal{J}_{n,d}[2^\infty] & \text{as multiplication by } 1 \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } -1 \text{ for all } r \in \mathcal{R} \\ \mathcal{J}_{n,d}[s^\infty] & \text{as multiplication by } 1 \text{ for all } s \in \mathcal{S} \end{cases}$$

By construction,

$$\tau_1 P + \tau_2 P \sim \tau_3 P + P \tag{5.6}$$

Case A: $\{\tau_1 P, \tau_2 P\} \neq \{\tau_3 P, P\}$

By (5.6), this means that there exists a map $\upsilon_1 \colon \mathcal{C}_{n,d} \to \mathbf{P}^1$ of degree $h \leq 2$. Since d is odd, we may apply Corollary 2.2.2 applied with υ_1 and the y-map to obtain

$$(n-1)(d-1)/2 \leq (h-1)(d-1).$$

Since $d > 1$, this implies that $n - 1 \leq 2(h-1)$. Since $h \leq 2$ and $n \geq 2$, this implies that $h = 2$ and $n \in \{2, 3\}$.

Case A1: $n = 3$ and $h = 2$

By Corollary 2.2.2 applied with υ_1 and the x-map, we obtain

$$(3-1)(d-1)/2 \leq (2-1)(3-1),$$

which forces $d \leq 3$, contradicting the assumption that n and d are coprime.

Case A2: $n = 2$ and $h = 2$

This curve is hyperelliptic of genus at least 2, so any 2-to-1 map to $\mathbf{P}^1$ must factor through the canonical map. Applying this fact to υ_1 yields $\tau_1 P + \tau_2 P \sim 2\infty$ and

$\tau_3 P + P \sim 2\infty$, so by definition of τ_3,

$$
\begin{aligned}
2D_2 &= 0 && && (5.7)\\
D_s &= 0 && \text{for all } s \in \mathcal{S}. && (5.8)
\end{aligned}
$$

Using Corollary 5.2.20, choose $\tau_4, \tau_5 \in \mathrm{Gal}(E(\mathcal{J}_{n,d}[M^\infty])/E)$ such that:

$$
\tau_4 \text{ acts on } \begin{cases} \mathcal{J}_{n,d}[2^\infty] & \text{as multiplication by } 1 \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } 1+3 \text{ for each } r \in \mathcal{R} \cap \{3\} \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } 3 \text{ for each } r \in \mathcal{R} \setminus \{3\} \end{cases}
$$

$$
\tau_5 \text{ acts on } \begin{cases} \mathcal{J}_{n,d}[2^\infty] & \text{as multiplication by } 1 \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } 1-3 \text{ for each } r \in \mathcal{R} \cap \{3\} \\ \mathcal{J}_{n,d}[r^\infty] & \text{as multiplication by } -1 \text{ for each } r \in \mathcal{R} \setminus \{3\} \end{cases}
$$

By construction,

$$\tau_4 P + \tau_5 P \sim 2P. \tag{5.9}$$

Case A2a: $\tau_4 P \neq P$

If $\tau_5 P = P$, then (5.9) would imply that $\mathcal{C}_{n,d}$ has a degree 1 map to $\mathbf{P}^1$, which contradicts the assumption that the genus of $\mathcal{C}_{n,d}$ is at least 2. Therefore, $P \notin \{\tau_4 P, \tau_5 P\}$, and (5.9) gives a 2-to-1 map to $\mathbf{P}^1$. As before, such a map must factor through the canonical map, so $\tau_4 P + \tau_5 P \sim 2P \sim 2\infty$. Hence $2[P - \infty] = 0$, so the conclusion of the proposition holds.

Case A2b: $\tau_4 P = P$

Then by definition of τ_4,

$$
\begin{aligned}
3D_3 &= 0 && \text{if } 3 \in \mathcal{R}, && (5.10)\\
D_r &= 0 && \text{for all } r \in \mathcal{R} \setminus \{3\}. && (5.11)
\end{aligned}
$$

Suppose that $3 \notin \mathcal{R}$. Then we are done because (5.7), (5.8), and (5.11) together imply that $2[P - \infty] = 0$.

Suppose that $3 \in \mathcal{R}$. Then (5.7), (5.8), (5.10), and (5.11) together imply that

$$6[P - \infty] = 0, \tag{5.12}$$

so using ι to denote the hyperelliptic involution yields

$$3P \sim 3\iota P. \tag{5.13}$$

If $P = \iota P$, then $2[P - \infty] = 0$ and the conclusion of the proposition holds. If $P \neq \iota P$, then (5.13) yields a nonconstant 3-to-1 map $\upsilon_2 : \mathcal{C}_{n,d} \to \mathbf{P}^1$, so applying Corollary 2.2.2 with υ_2 and the x-map yields $(2-1)(d-1)/2 \leq (3-1)(2-1)$, forcing $d \leq 5$, so by (5.12), the conclusion of the proposition holds.

Case B: $P = \tau_1 P$

Then by definition of τ_1,

$$\begin{aligned} 2^{\max\{1,e_2\}} D_2 &= 0, && && (5.14)\\ D_r &= 0 && \text{for all } r \in \mathcal{R}, && (5.15)\\ s^{e_s} D_s &= 0 && \text{for all } s \in \mathcal{S}, && (5.16) \end{aligned}$$

so (5.5), (5.14), (5.15), and (5.16) together imply $mD_2 = 0$, $mD_r = 0$ for all $r \in \mathcal{R}$, and $mD_s = 0$ for all $s \in \mathcal{S}$. We conclude that $m[P - \infty] = 0$.

Case C: $P = \tau_2 P$

Then by definition of τ_2,

$$\begin{aligned} 2^{\max\{1,e_2\}} D_2 &= 0, && && (5.17)\\ 3D_3 &= 0 && \text{for all } r \in \mathcal{R} \cap \{3\}, && (5.18)\\ D_r &= 0 && \text{for all } r \in \mathcal{R} \setminus \{3\}, && (5.19)\\ s^{e_s} D_s &= 0 && \text{for all } s \in \mathcal{S}. && (5.20) \end{aligned}$$

Case C1: $3 \notin \mathcal{R}$

Then (5.5), (5.17), (5.19), and (5.20) together imply $mD_2 = 0$, $mD_r = 0$ for all $r \in \mathcal{R}$, and $mD_s = 0$ for all $s \in \mathcal{S}$. We conclude that $m[P - \infty] = 0$.

Case C2: $3 \in \mathcal{R}$

Arguing similarly as in Case C1 yields

$$3m[P - \infty] = 0. \tag{5.21}$$

Using Corollary 5.2.20, choose $\tau_6 \in \mathrm{Gal}(E(\mathcal{J}_{n,d}[M^\infty])/E)$ such that:

$$\tau_6 \text{ acts on } \begin{cases} \mathcal{J}_{n,d}[(2nd)^\infty] & \text{as multiplication by } 1 \\ \mathcal{J}_{n,d}[3^\infty] & \text{as multiplication by } 2 \end{cases}$$

By definition, τ_6 fixes D_2 and D_s for all $s \in \mathcal{S}$, so by (5.18) and (5.19), τ_6 must fix $3P$, i.e.,

$$3P \sim 3\tau_6 P. \tag{5.22}$$

Case C2a: $P = \tau_6 P$

Since τ_6 acts on D_3 as multiplication by 2, this forces $D_3 = 0$. Combining this with (5.5), (5.17), (5.19), and (5.20) yields $m[P - \infty] = 0$.

Case C2b: $P \neq \tau_6 P$

Then (5.22) yields a nonconstant 3-to-1 map $\upsilon_3 \colon \mathcal{C}_{n,d} \to \mathbf{P}^1$. Then $3 \in \mathcal{R}$ implies $3 \nmid nd$, so $3 \nmid \min\{n, d\}$, meaning we may apply Corollary 2.2.2 to υ_3 and to whichever of $y \colon \mathcal{C}_{n,d} \to \mathbf{P}^1$, $x \colon \mathcal{C}_{n,d} \to \mathbf{P}^1$ has smaller degree to obtain

$$(n-1)(d-1)/2 \leq (3-1)(\min\{n, d\} - 1),$$

which forces $n, d \leq 5$. Since $3 \nmid nd$ and d is odd, this implies $(n, d) \in \{(2, 5), (4, 5)\}$, so we are done by (5.21). □

5.2.4 Computation of some torsion fields for $\mathcal{C}_{p,q}$

In this section, we use results of Section 4.2 to compute some torsion fields. Assume that p and q are distinct odd primes from now on. Then we may identify R with $\mathcal{O}_E$.

Definition 5.2.23. For nonnegative i, j, define the torsion field

$$L_{i,j} := E(\mathcal{J}_{p,q}[(1-\zeta_p)^i(1-\zeta_q)^j]).$$

Lemma 5.2.24.

(1) *Each $L_{i,j}$ is an abelian extension of E.*

(2) $L_{0,0} = L_{0,1} = L_{1,0} = L_{1,1} = E$.

(3) $L_{i,j} = L_{i,0}L_{0,j}$ *and* $E = L_{i,0} \cap L_{0,j}$.

(4) $L_{i,1} = L_{i,0} = E(\mathcal{J}_{p,q}[(1-\zeta_p)^i])$.

(5) $L_{1,j} = L_{0,j} = E(\mathcal{J}_{p,q}[(1-\zeta_q)^j])$.

(6) $L_{p-1,1} = L_{p-1,0} = E(\mathcal{J}_{p,q}[p])$.

(7) $L_{1,q-1} = L_{0,q-1} = E(\mathcal{J}_{p,q}[q])$.

(8) $L_{2,1} = E\left(\sqrt[p]{1-\zeta_q^i} : 1 \leq i \leq q-1\right)$ *and* $[L_{2,1} : E] > 1$.

(9) $L_{1,2} = E\left(\sqrt[q]{1-\zeta_p^i} : 1 \leq i \leq p-1\right)$ *and* $[L_{1,2} : E] > 1$.

(10) *$L_{p,1}/E$ is a p-Kummer extension, i.e., it is generated by pth roots of elements of E.*

(11) *$L_{1,q}/E$ is a q-Kummer extension, i.e., it is generated by qth roots of elements of E.*

Proof.

(1) Since $\mathcal{J}_{p,q}[1-\zeta_p] \subseteq \mathcal{J}_{p,q}[p]$ and $\mathcal{J}_{p,q}[1-\zeta_q] \subseteq \mathcal{J}_{p,q}[q]$, this is a special case of Lemma 5.2.11.

(2) By Proposition 2.3.1, $\mathcal{J}_{p,q}[1-\zeta_p]$ is generated by $[(-\zeta_q^i, 0) - \infty]$ and $\mathcal{J}_{p,q}[1-\zeta_q]$ is generated by $[(0, \zeta_p^j) - \infty]$, so $L_{1,1} = E$.

(3) By definition, $L_{i,j} = L_{i,0}L_{0,j}$. By Corollary 2.5.12, $[L_{i,0} : L_{0,0}]$ is a power of p and $[L_{0,j} : L_{0,0}]$ is a power of q, so $L_{i,0} \cap L_{0,j} = L_{0,0} = E$.

(4) Lemma 5.2.24(3) implies that $L_{i,1} = L_{i,0}L_{0,1}$ and Lemma 5.2.24(2) gives that $L_{0,1} = E$, so $L_{i,1} = L_{i,0}$. By definition, $L_{i,0} = E(\mathcal{J}_{p,q}[(1-\zeta_p)^i])$.

(5) Similar to the proof of Lemma 5.2.24(4).

(6) Since $(1-\zeta_p)^{p-1} \in pR^\times$, we see that $\mathcal{J}_{p,q}[(1-\zeta_p)^{p-1}] = \mathcal{J}_{p,q}[p]$, so $L_{p-1,0} = E(\mathcal{J}_{p,q}[p])$, and we are done by Lemma 5.2.24(4).

(7) Similar to the proof of Lemma 5.2.24(6).

(8) Apply Corollary 2.3.8 by using the x-coordinate map to view $\mathcal{C}_{p,q}$ as a degree p superelliptic cover of $\mathbf{P}^1$. This shows that $L_{2,1}$ is generated over E by adjoining pth roots of $\zeta_q^a - \zeta_q^b$. Since $\zeta_q^a - \zeta_q^b = \zeta_q^a(1-\zeta_q^{b-a})$ and ζ_q already has a pth root in E, we see that $L_{2,1}$ is generated over E by adjoining pth roots of $1-\zeta_q^i$.

Consider the ramification of $L_{2,1}$ and E above the prime q. The field $L_{2,1}$ contains $(1-\zeta_q)^{1/p}$, so
$$e_q(L_{2,1}/\mathbf{Q}) \geq p(q-1) > q-1 = e_q(E/\mathbf{Q}),$$
so $L_{2,1}$ has to strictly contain E.

(9) Similar to the proof of Lemma 5.2.24(8).

(10) Lemma 5.2.24(1) implies that $L_{p,1}/E$ is abelian. Since E already contains the pth roots of unity and Corollary 2.5.12 implies that the exponent of $\mathrm{Gal}(L_{p,1}/E)$ divides p, we are done by Kummer theory.

(11) Similar to the proof of Lemma 5.2.24(10). □

Definition 5.2.25. Suppose that $\mathfrak{r}$ is a prime of E lying over a prime r of $\mathbf{Q}$ such that $r \notin \{p, q\}$. Abuse notation and write $\zeta_p, \zeta_q \in \mathbf{F}_\mathfrak{r}$ to denote the images of $\zeta_p, \zeta_q \in \mathcal{O}_E$ under the reduction map $\mathcal{O}_E \to \mathbf{F}_\mathfrak{r}$.

For integers $i \in [0, p-2]$, $j \in [1, q-1]$, and $s \in [0, p-1]$, define
$$u_{s,j} := 1 - \zeta_q^j \zeta_p^s \in \mathcal{O}_E$$
$$\eta_{i,j} := \prod_{s=0}^{p-1} u_{s,j}^{\binom{s}{i}} \in \mathcal{O}_E$$
$$\eta'_{i,j} := \prod_{s=0}^{p-1} u_{s,j}^{s^i} \in \mathcal{O}_E.$$

(We adopt the convention $0^0 = 1$ here.) We will also use $u_{i,j}, \eta_{i,j}, \eta'_{i,j}$ to denote the images of the same expressions in $\mathbf{F}_\mathfrak{r}$.

Theorem 5.2.26. *Let χ_p and χ_q denote characters $\mathbf{F}_\mathfrak{r}^\times \to E^\times$ of exact order p and q, respectively. Let $k \in [1, p-1]$. Let J be the Jacobi sum $J_1(\chi_p, \chi_q)$. The following are equivalent:*

(1) *$J + 1 \in (1-\zeta_p)^k \mathcal{O}_E$;*

(2) *$\eta_{i,j} \in \mathbf{F}_\mathfrak{r}^{\times p}$ for all $i \in [0, k-2]$ and $j \in [1, q-1]$;*

(3) *$\eta_{i,j} \in \mathbf{F}_\mathfrak{r}^{\times p}$ for all $i \in [0, k-2]$ and $j \in [1, (q-1)/2]$.*

Proof. This is a special case (since q is odd) of Theorem 4.2.25. □

Corollary 5.2.27. *Let $k \in [1, p-1]$ be an integer. The following are equivalent:*

(1) *$\mathfrak{r}$ splits in the field $E(\mathcal{J}_{p,q}[(1-\zeta_p)^k])$*

(2) *$\eta_{i,j} \in \mathbf{F}_\mathfrak{r}^{\times p}$ for all $i \in [0, k-2]$ and $j \in [1, q-1]$;*

(3) *$\eta_{i,j} \in \mathbf{F}_\mathfrak{r}^{\times p}$ for all $i \in [0, k-2]$ and $j \in [1, (q-1)/2]$.*

Proof. Define characters $\gamma'_{p,\mathfrak{r}}, \gamma'_{q,\mathfrak{r}} \colon \mathbf{F}_{\mathfrak{r}}^\times \to R^\times \simeq \mathcal{O}_E^\times$ of exact orders p and q as in Proposition 5.2.16(2). Then $\mathfrak{r}$ splits in $E(\mathcal{J}_{p,q}[(1-\zeta_p)^k])$ if and only if $\mathrm{Frob}_{\mathfrak{r}} - 1$ kills $\mathcal{J}_{p,q}[(1-\zeta_p)^k]$, which by Lemma 5.2.10 is equivalent to $\theta_p(\mathrm{Frob}_{\mathfrak{r}} - 1) \in (1-\zeta_p)^k R_p$, which by Proposition 5.2.16(2) is equivalent to $-\gamma'_{q,\mathfrak{r}}(-1)J(\gamma'_{p,\mathfrak{r}}, \gamma'_{q,\mathfrak{r}}) - 1 \in (1-\zeta_p)^k R = (1-\zeta_p)^k \mathcal{O}_E$ (recall from Proposition 5.2.16(2) that $\theta_p(\mathrm{Frob}_{\mathfrak{r}})$ lies in R). Since q is odd, we know $\gamma'_{q,\mathfrak{r}}(-1) = 1$, so we are done by Theorem 5.2.26. □

Theorem 5.2.28. *Let $k \in [1, p-1]$ be an integer. Then*

$$\begin{aligned} L_{k,1} &= E\left(\sqrt[p]{\eta_{i,j}} \colon i \in [0, k-2] \text{ and } j \in [1, q-1]\right) \\ &= E\left(\sqrt[p]{\eta_{i,j}} \colon i \in [0, k-2] \text{ and } j \in [1, (q-1)/2]\right). \end{aligned}$$

Proof. Define

$$\begin{aligned} L'_{k,1} &:= E\left(\sqrt[p]{\eta_{i,j}} \colon i \in [0, k-2] \text{ and } j \in [1, q-1]\right), \\ L''_{k,1} &:= E\left(\sqrt[p]{\eta_{i,j}} \colon i \in [0, k-2] \text{ and } j \in [1, (q-1)/2]\right). \end{aligned}$$

For any extension M of E and subset S of primes of $\mathbf{Q}$, define

$$\mathrm{Spl}_S(M/E) := \left\{ \mathfrak{r} \text{ is a prime of } E \colon \begin{array}{c} \mathfrak{r} \text{ splits in } M \text{ and} \\ \mathfrak{r} \text{ does not lie above a prime in } S \end{array} \right\}.$$

Corollary 5.2.27 implies that $\mathrm{Spl}_{\{p,q\}}(L_{k,1}/E) = \mathrm{Spl}_{\{p,q\}}(L'_{k,1}/E) = \mathrm{Spl}_{\{p,q\}}(L''_{k,1}/E)$, so since $L_{k,1}$, $L'_{k,1}$, and $L''_{k,1}$ are Galois extensions of E, the Chebotarev density theorem implies that $L_{k,1} = L'_{k,1} = L''_{k,1}$. □

Lemma 5.2.29. *Suppose that $i \in [0, p-3]$ and $j \in [1, q-1]$.*

1. *The image of $\eta_{i,j}$ in $E^\times/E^{\times p}$ lies in the subgroup generated by $\eta'_{i,j}, \cdots, \eta'_{0,j}$.*

2. *The image of $\eta'_{i,j}$ in $E^\times/E^{\times p}$ lies in the subgroup generated by $\eta_{i,j}, \cdots, \eta_{0,j}$.*

Proof. Observe that there exist integers $b_{i,k} \in \mathbf{Z}$ such that for each i,

$$T^i = b_{i,i}\binom{T}{i} + b_{i,i-1}\binom{T}{i-1} + \cdots + b_{i,0}\binom{T}{0} \qquad \text{in } \mathbf{Z}[T]$$

and $b'_{i,j} \in \mathbf{Z}_{(p)}$ such that for each i,

$$\binom{T}{i} = b'_{i,i}T^i + b'_{i,i-1}T^{i-1} + \cdots + b'_{i,0}T^0 \qquad \text{in } \mathbf{Z}_{(p)}[T].$$

We are now done by using the definition of $\eta_{i,j}$ and $\eta'_{i,j}$. □

Corollary 5.2.30. *Let $k \in [1, p-1]$ be an integer. Then*

$$\begin{aligned} L_{k,1} &= E\left(\sqrt[p]{\eta'_{i,j}} \colon i \in [0, k-2] \text{ and } j \in [1, q-1]\right) \\ &= E\left(\sqrt[p]{\eta'_{i,j}} \colon i \in [0, k-2] \text{ and } j \in [1, (q-1)/2]\right). \end{aligned}$$

Proof. This follows immediately from Theorem 5.2.28 and Lemma 5.2.29. □

Definition 5.2.31. Let $\omega : \mathrm{Gal}(E/\mathbf{Q}(\mu_q)) \simeq \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \to \mathbf{Z}_p$ be the composite of the natural isomorphism $\mathrm{Gal}(E/\mathbf{Q}(\mu_q)) \simeq \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ with the Teichmüller character. If A is an abelian group which has an action of $\mathrm{Gal}(E/\mathbf{Q}(\mu_q))$ and $i \in \mathbf{Z}$, use $\varepsilon_{\omega^i} A$ to denote the subgroup of A for which $\mathrm{Gal}(E/\mathbf{Q}(\mu_q))$ acts as ω^i.

Definition 5.2.32. For each $i \in [0, p-2]$, define

$$\begin{aligned} \Delta_i &:= \text{the subgroup of } E^\times/E^{\times p} \text{ generated by } \eta'_{i,1}, \dots, \eta'_{i,(q-1)/2} \\ M_i &:= E(\sqrt[p]{\delta} : \delta \in \Delta_i). \end{aligned}$$

Lemma 5.2.33. *$\Delta_i \subseteq \varepsilon_{\omega^{-i}}(E^\times/E^{\times p})$ for each $i \in [0, p-2]$.*

Proof. This follows from a straightforward computation of the $\mathrm{Gal}(E/\mathbf{Q}(\mu_q))$-action on each $\eta'_{i,j}$. □

Lemma 5.2.34. *Let $k \in [2, p-1]$ be an integer.*

(1) *$L_{k,1}$ is the compositum of $M_0, \dots, M_{k-2}$ over E.*

(2) *The fields $M_0, \dots, M_{p-2}$ are disjoint over E.*

(3) *$[L_{k,1} : L_{k-1,1}] = [M_{k-2} : E]$.*

Proof.

(1) This follows immediately from Corollary 5.2.30 and Definition 5.2.32.

(2) By Kummer theory, we must check that if $\delta_i \in \Delta_i$ satisfy $\prod_{i=0}^{p-2} \delta_i = 1$, then $\delta_i = 1$ for all i. Lemma 5.2.33 implies that each δ_i lies in a different isotypic component for the ω-action, so they must all be 1. □

(3) This follows immediately from Lemma 5.2.34(1) and Lemma 5.2.34(2).

Corollary 5.2.35. *For each integer $k \in [2, p-1]$, there exists an integer $e(k) \in [0, (q-1)/2]$ such that*

$$[L_{k,1} : L_{k-1,1}] = p^{e(k)}.$$

Proof. This follows immediately from Lemma 5.2.34(3). □

Remark 5.2.36. For our strategy of using large Galois action to classify torsion points, we need a lower bound for $[L_{k,1} : L_{k-1,1}]$. Corollary 5.2.35 gives an upper bound, but we do not know when it is possible to attain this value. In light of Lemma 5.2.34(3), we focus our efforts on studying M_i for the rest of the section.

Corollary 5.2.37. *$[L_{2,1} : L_{1,1}] \geq p$.*

Proof. This follows immediately from Corollary 5.2.35 and Lemma 5.2.24(8). □

Definition 5.2.38. Recall the notion of a cyclotomic unit as in Section 8.1 of [64]. Define

U	to be the unit group of $\mathbf{Q}(\mu_p)$
C	to be the group of cyclotomic units of $\mathbf{Q}(\mu_p)$
$Q(\mu_p)^+$	to be the totally real subfield of $\mathbf{Q}(\mu_p)$
U^+	to be the unit group of $\mathbf{Q}(\mu_p)^+$
C^+	to be the group of cyclotomic units of $\mathbf{Q}(\mu_p)^+$
A	to be the class group of $\mathbf{Q}(\mu_p)$.

For any group B, let B_p be the p-Sylow subgroup of B.

For $i \in [0, p-3]$ and $b \in (\mathbf{Z}/p\mathbf{Z})^\times$, define

$$U_i(b) := \prod_{s=0}^{p-1} \left(\zeta_p^{(p+1)(1-b)s/2} \frac{1-\zeta_p^{bs}}{1-\zeta_p^s} \right)^{s^i} \in \mathbf{Q}(\mu_p)^+$$

($U_i(b)$ lies in $\mathbf{Q}(\mu_p)^+$ since each term $\zeta_p^{(p+1)(1-b)s/2}(1-\zeta_p^{bs})/(1-\zeta_p^s)$ is fixed by complex conjugation.)

Let $\nu \in (\mathbf{Z}/p\mathbf{Z})^\times$ be a generator and define $U_i := U_i(\nu)$.

Lemma 5.2.39. *Suppose that $i \in [0, p-3]$, $b \in (\mathbf{Z}/p\mathbf{Z})^\times$, and $b^i \not\equiv 1 \pmod{p}$.*

(1) *Then*

$$U_i(b) = \prod_{s=0}^{p-1} \left(\frac{1-\zeta_p^{bs}}{1-\zeta_p^s} \right)^{s^i}.$$

(2) *The images of U_i and $U_i(b)$ in $\mathbf{Q}(\mu_p)^{+\times}/\mathbf{Q}(\mu_p)^{+\times p}$ generate the same subgroup.*

Proof.

(1) Since $i \in [0, p-3]$,

$$\sum_{s=0}^{p-1} s^{i+1} \equiv 0 \pmod{p},$$

so

$$\prod_{s=0}^{p-1} \left(\zeta_p^{(p+1)(1-b)s/2} \right)^{s^i} = 1$$

and we are done by definition of $U_i(b)$.

(2) For notational convenience, use the shorthand $\zeta_p^{m/2}$ to mean $\zeta_p^{m(p+1)/2}$, i.e., it is a pth root of unity whose square is ζ_p^m. For any $c \in \mathbf{Z}/p\mathbf{Z}$,

$$U_i(c) = \prod_{s=0}^{p-1} \left(\frac{\zeta_p^{cs/2} - \zeta_p^{-cs/2}}{\zeta_p^{s/2} - \zeta_p^{-s/2}} \right)^{s^i},$$

so

$$\begin{aligned}
(U_i(c))^{c^i} &= \prod_{s=0}^{p-1} \left(\frac{\zeta_p^{cs/2} - \zeta_p^{-cs/2}}{\zeta_p^{s/2} - \zeta_p^{-s/2}} \right)^{(cs)^i} \\
&= \left(\prod_{s=0}^{p-1} (\zeta_p^{cs/2} - \zeta_p^{-cs/2})^{(cs)^i} \right) \left(\prod_{s=0}^{p-1} (\zeta_p^{s/2} - \zeta_p^{-s/2})^{(cs)^i} \right)^{-1} \\
&\equiv \left(\prod_{t=0}^{p-1} (\zeta_p^{t/2} - \zeta_p^{-t/2})^{t^i} \right) \left(\prod_{s=0}^{p-1} (\zeta_p^{s/2} - \zeta_p^{-s/2})^{(cs)^i} \right)^{-1} \pmod{\mathbf{Q}(\mu_p)^{+\times p}}
\end{aligned}$$

by setting $t \equiv cs \pmod p$ in the first product and observing that this change-of-variable preserves the product modulo $\mathbf{Q}(\mu_p)^{+\times p}$. Combining the products yields

$$(U_i(c))^{c^i} \equiv \left(\prod_{t=0}^{p-1} (\zeta_p^{t/2} - \zeta_p^{-t/2})^{t^i} \right)^{1-c^i} \pmod{\mathbf{Q}(\mu_p)^{+\times p}},$$

so if we define

$$U := \prod_{t=0}^{p-1} (\zeta_p^{t/2} - \zeta_p^{-t/2})^{t^i}$$

then

$$(U_i(c))^{c^i} \equiv U^{1-c^i} \pmod{\mathbf{Q}(\mu_p)^{+\times p}},$$

so

$$(U_i(b))^{b^i(1-\nu^i)} \equiv U^{(1-b^i)(1-\nu^i)} \equiv U_i^{\nu^i(1-b^i)} \pmod{\mathbf{Q}(\mu_p)^{+\times p}}.$$

Since $b^i, 1-b^i, \nu^i, 1-\nu^i$ are invertible modulo p, we are done. □

Lemma 5.2.40. *Suppose that $i \in [1, p-3]$ and $j \in [1, q-1]$.*

(1) *For each $s \in [1, p-1]$,*

$$\operatorname{Norm}_{E/\mathbf{Q}(\mu_p)} u_{s,j} = \frac{1-\zeta_p^{qs}}{1-\zeta_p^{s}}.$$

(2) *We have*

$$\operatorname{Norm}_{E/\mathbf{Q}(\mu_p)} \eta'_{i,j} = U_i(q).$$

(3) *Suppose that $q^i \not\equiv 1 \pmod p$. Then $U_i \in M_i^p$.*

Proof.

(1) This is a straightforward computation.

(2) Combine the definition of $\eta'_{i,j}$, Lemma 5.2.40(1), and Lemma 5.2.39(1).

(3) M_i is Galois over $\mathbf{Q}(\mu_p)$ and $\eta'_{i,1} \in M_i^p$, so $\operatorname{Norm}_{E/\mathbf{Q}(\mu_p)} \eta'_{i,1} \in M_i^p$, so we are done by Lemma 5.2.40(2) and Lemma 5.2.39(2). □

Corollary 5.2.41. *For any $i \in [1, p-3]$ such that $q^i \not\equiv 1 \pmod p$,*

$$[M_i : E] \geq [E(\sqrt[p]{U_i}) : E] = [\mathbf{Q}(\mu_p)^+(\sqrt[p]{U_i}) : \mathbf{Q}(\mu_p)^+].$$

Proof. Lemma 5.2.40(3) implies that $M_i \supseteq E(\sqrt[p]{U_i})$, so $[M_i : E] \geq [E(\sqrt[p]{U_i}) : E]$.

Let $F := \mathbf{Q}(\mu_p)^+(\sqrt[p]{U_i})$. Since $E/\mathbf{Q}(\mu_p)$ is totally ramified at q and $F(\mu_p)/\mathbf{Q}(\mu_p)$ is unramified at q, $E \cap F \subseteq \mathbf{Q}(\mu_p)$. Therefore,

$$\mathbf{Q}(\mu_p)^+ \subseteq E \cap F \subseteq \mathbf{Q}(\mu_p). \tag{5.23}$$

Since $[F : \mathbf{Q}(\mu_p)^+] \in \{1, p\}$ and $[F : \mathbf{Q}(\mu_p)^+]$ is divisible by $[E \cap F : \mathbf{Q}(\mu_p)^+]$, we must have $E \cap F \neq \mathbf{Q}(\mu_p)$, so (5.23) implies

$$E \cap F = \mathbf{Q}(\mu_p)^+. \tag{5.24}$$

Note that $[E(\sqrt[p]{U_i}) : E] = [EF : E] = [F : E \cap F]$ since E is Galois over $E \cap F$, so we are done by (5.24). □

Theorem 5.2.42. *For even $i \in [2, p-3]$, $\#\varepsilon_{\omega^i}(U^+/C^+)_p = 1$ if and only if $U_{p-1-i} \notin \mathbf{Q}(\mu_p)^{+\times p}$.*

Proof. This follows from Section 8.3 of [64] (Washington uses E and E^+ to denote the unit groups of $\mathbf{Q}(\mu_p)$ and $\mathbf{Q}(\mu_p)^+$, respectively); see the discussion on pages 155–156: U_{p-1-i} is a pth power if and only if Washington's $E_i^{(N)}$ is a pth power, if and only if the ω^i-isotypic component of $(U^+/C^+)_p$ is nontrivial. □

Theorem 5.2.43. *For even $i \in [2, p-3]$,*

$$\#\varepsilon_{\omega^i}(U^+/C^+)_p = \#\varepsilon_{\omega^i} A_p.$$

Proof. See Theorem 15.7 on page 342 of [64]. □

Theorem 5.2.44. *For any odd prime p, $\#\varepsilon_{\omega^{p-3}} A_p = 1$.*

Proof. This is Corollary 3.8 on page 230 of [44]. □

Corollary 5.2.45. *If $q^2 \not\equiv 1 \pmod{p}$, then $[L_{4,1} : L_{3,1}] \geq p$.*

Proof. Taking $i = p-3$ and combining Theorems 5.2.42 to 5.2.44 yields $U_2 \notin \mathbf{Q}(\mu_p)^{+\times p}$, so taking $i = 2$ in Corollary 5.2.41 yields $[M_2 : E] \geq p$, and we are done by Lemma 5.2.34(3). □

Corollary 5.2.46. *If $q^2 \not\equiv 1 \pmod{p}$, then $[L_{4,1} : E] \geq p^2$.*

Proof. This follows from Corollary 5.2.37 and Corollary 5.2.45. □

Lemma 5.2.47. *Suppose that $q = 3$ and $p \in \{5, 7, 11, 13\}$. Then $[L_{3,1} : L_{2,1}] = [L_{2,1} : E] = p$.*

Proof. By Corollary 5.2.35, it suffices to check that $L_{3,1}/L_{2,1}/E$ is a tower where each successive step is nontrivial. The bottom extension $L_{2,1}/E$ is known to be nontrivial by Lemma 5.2.24(8), so it suffices to check that $L_{3,1}/L_{2,1}$ is nontrivial. For each $p \in \{5, 7, 11, 13\}$, we find a prime r and a prime $\mathfrak{r}$ of E lying above r such that $\mathrm{Frob}_{\mathfrak{r}} - 1$ kills $\mathcal{J}_{p,q}[(1-\zeta_p)^2]$ but not $\mathcal{J}_{p,q}[(1-\zeta_p)^3]$; using Corollary 5.2.27, a computer calculation shows that we may use the prime $\mathfrak{r}$ specified by the following table.

p	5	7	11	13
$\#\mathbf{F}_{\mathfrak{r}}$	2^4	13^2	43^2	547

□

5.2.5 Galois action on the torsion of $\mathcal{J}_{p,q}$

As before, suppose that p, q are distinct odd primes.

Definition 5.2.48. Let $G_{\mathbf{Q}}$ denote the absolute Galois group of $\mathbf{Q}$.

Lemma 5.2.49. *Suppose that ℓ is a prime and that $k \geq 1$ is an integer.*

(1) *Suppose that $\ell \notin \{p, q\}$ and that $D \in \mathcal{J}_{p,q}[\ell^k] \setminus \mathcal{J}_{p,q}[\ell^{k-1}]$. Then $G_{\mathbf{Q}} Z D$ generates $\mathcal{J}_{p,q}[\ell^k]$.*

(2) *Suppose that $\ell \in \{p, q\}$ and that $D \in \mathcal{J}_{p,q}[(1-\zeta_\ell)^k] \setminus \mathcal{J}_{p,q}[(1-\zeta_\ell)^{k-1}]$. Then $G_{\mathbf{Q}} Z D$ generates $\mathcal{J}_{p,q}[(1-\zeta_\ell)^k]$.*

Proof.

(1) Suppose that $k = 1$. By linear algebra, $\mathcal{J}_{p,q}[\ell] \otimes_{\mathbf{F}_\ell} \overline{\mathbf{F}_\ell}$ breaks up into the direct sum of its eigenspaces for the ζ_{nd}-action. The action of $G_{\mathbf{Q}}$ on $\mathcal{J}_{p,q}[\ell]$ permutes the eigenspaces transitively.

We will show that $G_{\mathbf{Q}} Z D$ generates $\mathcal{J}_{p,q}[\ell] \otimes_{\mathbf{F}_\ell} \overline{\mathbf{F}_\ell}$ as an $\overline{\mathbf{F}_\ell}$-vector space. Since D is nonzero, there is some eigenspace for which its projection is nonzero, so since $\ell \nmid pq$, there exists $r \in \overline{\mathbf{F}_\ell}[Z]$ such that rD is a nonzero eigenvector. Since $G_{\mathbf{Q}}$ acts on the eigenspaces transitively, the $G_{\mathbf{Q}}$-orbit of rD hits every eigenspace; hence, $G_{\mathbf{Q}} Z D$ generates $\mathcal{J}_{p,q}[\ell] \otimes_{\mathbf{F}_\ell} \overline{\mathbf{F}_\ell}$ as a $\overline{\mathbf{F}_\ell}$-vector space. This completes the case $k = 1$.

Now suppose that $k \geq 1$. Multiplication by ℓ^{k-1} provides an isomorphism

$$\mu \colon \mathcal{J}_{p,q}[\ell^k] / \ell \mathcal{J}_{p,q}[\ell^k] \simeq \mathcal{J}_{p,q}[\ell].$$

The proof of the $k = 1$ case shows that the image of $G_{\mathbf{Q}} Z D$ under μ generates $\mathcal{J}_{p,q}[\ell]$, so $G_{\mathbf{Q}} Z D$ generates $\mathcal{J}_{p,q}[\ell^k] / \ell \mathcal{J}_{p,q}[\ell^k]$. By Nakayama's Lemma, the only subgroup of $\mathcal{J}_{p,q}[\ell^k]$ which generates $\mathcal{J}_{p,q}[\ell^k] / \ell \mathcal{J}_{p,q}[\ell^k]$ is $\mathcal{J}_{p,q}[\ell^k]$, so we are done.

(2) Without loss of generality, assume that $\ell = q$.

Suppose that $k = 1$. By Corollary 2.3.2, we may express $D = \sum_{i=0}^{p-1} a_i [(0, \zeta_p^i) - \infty]$ for $a_i \in \mathbf{Z}/q\mathbf{Z}$ such that $a_0 + \cdots + a_{p-1} = 0$. By applying an appropriate power of ζ_p to D, we may assume that $a_0 \not\equiv 0 \pmod{q}$. Let $g \in G_{\mathbf{Q}}$ restrict to a generator of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$. Then

$$\begin{aligned}(g + g^2 + \cdots + g^{p-1}) D &= (p-1) a_0 [(0,1) - \infty] + \left(\sum_{i=1}^{p-1} a_i \right) \sum_{j=1}^{p-1} [(0, \zeta_p^j) - \infty] \\ &= (p-1) a_0 [(0,1) - \infty] + (-a_0) \left(-[(0,1) - \infty] \right) \\ &= p a_0 [(0,1) - \infty]. \end{aligned} \tag{5.25}$$

Since $p a_0 \not\equiv 0 \pmod{q}$, (5.25) implies that $[(0,1) - \infty]$ lies in the subgroup generated by $G_{\mathbf{Q}} Z_p D$. Applying elements of Z_p shows that each $[(0, \zeta_p^i) - \infty]$ also lies the subgroup generated by $G_{\mathbf{Q}} Z_p D$, and these generate $\mathcal{J}_{p,q}[1 - \zeta_q]$.

The proof of the $k \geq 1$ case is similar to the one in Lemma 5.2.49(1). □

Corollary 5.2.50. *Suppose that ℓ is a prime and $k \geq 1$.*

(1) *Suppose that $\ell \notin \{p, q\}$ and $D \in \mathcal{J}_{p,q}[\ell^k] \setminus \mathcal{J}_{p,q}[\ell^{k-1}]$. Then the Galois closure of $E(D)$ over $\mathbf{Q}$ equals $E(\mathcal{J}_{p,q}[\ell^k])$.*

(2) *Suppose that $\ell \in \{p, q\}$ and $D \in \mathcal{J}_{p,q}[(1-\zeta_\ell)^k] \setminus \mathcal{J}_{p,q}[(1-\zeta_\ell)^{k-1}]$. Then the Galois closure of $E(D)$ over $\mathbf{Q}$ equals $E(\mathcal{J}_{p,q}[(1-\zeta_\ell)^k])$.*

Proof. This follows immediately from Lemma 5.2.49(1) and Lemma 5.2.49(2). □

Corollary 5.2.51. *Suppose that $p \geq 5$, $q = 3$, and $k \in [1, p-1]$. Suppose that $D \in \mathcal{J}_{p,q}[(1-\zeta_p)^k] \setminus \mathcal{J}_{p,q}[(1-\zeta_p)^{k-1}]$. Then $E(D) = L_{k,1}$.*

Proof. Induct on k. The case $k = 1$ follows since $\mathcal{J}[1-\zeta_p]$ is already defined over E.

Now suppose the assertion holds for $k-1$ and that $D \in \mathcal{J}_{p,q}[(1-\zeta_p)^k] \setminus \mathcal{J}_{p,q}[(1-\zeta_p)^{k-1}]$. By the inductive hypothesis, $L_{k-1,1} = E((1-\zeta_p)D)$, so $L_{k-1,1} = E((1-\zeta_p)D) \subseteq E(D) \subseteq L_{k,1}$. By Corollary 5.2.35, either $E(D) = L_{k,1}$ (in which case we are done) or that $E(D) = L_{k-1,1}$. If $E(D) = L_{k-1,1}$, then $E(D)$ is Galois over $\mathbf{Q}$, so Corollary 5.2.50(2) gives $E(D) = E(\mathcal{J}_{p,q}[(1-\zeta_\ell)^k]) = L_{k,1}$, so we are again done. □

Lemma 5.2.52. *Let $i \geq 0$ be an integer and $\gamma \in \mathbf{Z}_p[\mathrm{Gal}(E(\mathcal{J}[p^\infty])/E)]$. Suppose that $\gamma - 1$ kills $\mathcal{J}[(1-\zeta_p)^i]$. Then*

(1) *for any integer $k \geq 0$, $(\gamma-1)^k$ kills $\mathcal{J}_{p,q}[(1-\zeta_p)^{ik}]$;*

(2) *$\gamma^{p-1} + \gamma^{p-2} + \cdots + 1$ kills $\mathcal{J}[p] = \mathcal{J}_{p,q}[(1-\zeta_p)^{p-1}]$;*

(3) *$\gamma^p - 1$ kills $\mathcal{J}_{p,q}[(1-\zeta_p)^{p-1+i}]$.*

Proof. Since $\mathcal{J}_{p,q}[p^\infty] \supseteq \mathcal{J}[1-\zeta_p]$ and the field of definition of $\mathcal{J}_{p,q}[1-\zeta_p]$ is $\mathbf{Q}(\mu_q)$,

$$E(\mathcal{J}_{p,q}[p^\infty]) = \mathbf{Q}(\mu_p, \mathcal{J}_{p,q}[p^\infty]).$$

So now this lemma follows from Lemma 2.5.11. □

5.2.6 Classification of torsion points on $\mathcal{C}_{n,d}$

The case $\mathcal{C}_{p,q}$ for distinct odd primes p, q

As before, p and q will be distinct odd primes.

Definition 5.2.53. Suppose that $m \geq 1$ is an integer coprime to p and q and that $a, b \geq 0$ are integers. Say that $D \in \mathcal{J}_{p,q}(\mathbf{C})$ is of *exact order* $(1-\zeta_p)^a(1-\zeta_q)^b m$ if

$$\begin{aligned} &D \in \mathcal{J}_{p,q}[(1-\zeta_p)^a(1-\zeta_q)^b m] \\ &D \notin \mathcal{J}_{p,q}[(1-\zeta_p)^{a-1}(1-\zeta_q)^b m] \\ &D \notin \mathcal{J}_{p,q}[(1-\zeta_p)^a(1-\zeta_q)^{b-1} m], \end{aligned}$$

and for all $m'|m$ such that $m' \neq m$, we have

$$D \notin \mathcal{J}_{p,q}[(1-\zeta_p)^a(1-\zeta_q)^b m'].$$

Lemma 5.2.54. *Suppose that $D \in \mathcal{J}_{n,d}(\mathbf{C})$.*

(1) *Suppose that D has exact order $(1-\zeta_p)$. Then the stabilizer of D in Z is Z_p.*

(2) *Suppose that D has exact order $(1-\zeta_q)$. Then the stabilizer of D in Z is Z_q.*

(3) *Suppose that D has exact order $(1-\zeta_p)(1-\zeta_q)$. Then the stabilizer of D in Z is $\{1\}$.*

Proof.

(1) The stabilizer contains Z_p. If it were any larger, then it would be Z. That would imply that D is fixed by ζ_q, so $qD = 0$. Since D is fixed by ζ_p, we also have $pD = 0$. Together, these imply that $D = 0$, a contradiction.

(2) Similar to the proof of the previous part.

(3) The stabilizer of D is contained in the stabilizer of $(1-\zeta_p)D$ and $(1-\zeta_q)D$, so the previous two parts imply that it is contained in $Z_p \cap Z_q = \{1\}$. □

Lemma 5.2.55. *Suppose that $D \in \mathcal{J}_{p,q}[2] \setminus \{0\}$.*

(1) *The extension $E(D)/E$ is ramified at some prime above 2.*

(2) *The extension $E(D, \mathcal{J}_{p,q}[pq])/E(\mathcal{J}_{p,q}[pq])$ is nontrivial.*

Proof.

(1) Suppose for contradiction that $E(D)/E$ is unramified at every prime above 2. Since $E/\mathbf{Q}$ is also unramified at every prime above 2, we see that $E(D)/\mathbf{Q}$ is unramified at every prime above 2. Hence $E(\mathcal{J}_{p,q}[2])/\mathbf{Q}$, which is the Galois closure of $E(D)/\mathbf{Q}$ by Corollary 5.2.50(1), must also be unramified at every prime above 2, so Lemma 1.4 of [30] implies that the mod 2 reduction of $\mathcal{J}_{p,q}$ must be ordinary, which contradicts Lemma 4.2 of [37].

(2) Since $\mathcal{C}_{p,q}$ has good reduction at 2 and 2 is coprime to pq, the extension $E(\mathcal{J}_{p,q}[pq])/E$ is unramified at every prime above 2, so we are done by Lemma 5.2.55(1). □

Lemma 5.2.56. $2pq[P - \infty] = 0$.

Proof. This is a special case of Proposition 5.2.22(i). □

Definition 5.2.57. By Lemma 5.2.56, there exist $a \in [0, p-1]$, $b \in [0, q-1]$, and $c \in \{1, 2\}$ such that P has exact order $(1-\zeta_p)^a(1-\zeta_q)^b c$. Define D_p, D_q, D_2 to have exact order $(1-\zeta_p)^a$, $(1-\zeta_q)^b$, and c respectively, such that $[P - \infty] = D_p + D_q + D_2$.

Proposition 5.2.58. $pq[P - \infty] = 0$.

Proof. If not, then $D_2 \neq 0$. By Lemma 5.2.55(2), there must be some nontrivial $\tau \in \mathrm{Gal}(\overline{E}/E(\mathcal{J}_{p,q}[pq]))$ which moves D_2, and hence $\tau P \neq P$. Since τ fixes D_p and D_q, we see that $2[P - \tau P] = 2(D_2 - \tau D_2) = 0$, which violates Lemma 2.2.3. □

Lemma 5.2.59. *Suppose that $a \geq 2$. Then*

(1) $[E(D_p) : E] \geq p$*;*

(2) *if $q = 3$, then $E(D_p) = L_{a,1}$;*

(3) *if $q = 3$ and $a \geq 4$, then $[E(D_p) : E] \geq p^2$.*

Proof.

(1) Since $E(D_p)$ is a subfield of $L_{a,1}$ and Lemma 5.2.24(10) implies that $[L_{a,1} : E]$ is a power of p, $[E(D_p) : E]$ is also a power of p. If $E(D_p) = E$, then taking Galois closure of both sides (over $\mathbf{Q}$) and applying Corollary 5.2.50(2) yields $L_{a,1} = E$, which contradicts Lemma 5.2.24(8).

(2) This follows from Corollary 5.2.51.

(3) This follows from Lemma 5.2.59(2) and Corollary 5.2.46. □

Definition 5.2.60. Let G_E denote the absolute Galois group of E.

Lemma 5.2.61. *Suppose that $a, b \geq 1$.*

(1) $\#G_E ZP \geq pq[E(D_p) : E]$.

(2) $\#G_E ZP \geq pq[E(D_q) : E]$.

Proof. Both parts are similar so we prove the first. Suppose that $h \in \mathrm{Gal}(\overline{E}/E)$ and $z \in Z$ satisfy $hzP = P$. Since the action of $\mathrm{Gal}(\overline{E}/E)$ and Z commute, we must check that h fixes D_p and $z = 1$.

Then $(1-\zeta_p)^{a-1}(1-\zeta_p)^{b-1}P$ has exact order $(1-\zeta_p)(1-\zeta_q)$ and is fixed by hz. It is also fixed by h since $E = L_{1,1}$. Therefore, it is fixed by z. Lemma 5.2.54(3) implies that $z = 1$, so h fixes P, and hence h also fixes D_p. □

Lemma 5.2.62.

(1) *Suppose that $a \geq 2$. Then there exists $h \in \mathrm{Gal}\left(\overline{E}/E\right)$ which moves P such that $h-1$ kills $\mathcal{J}_{p,q}[(q(1-\zeta_p)]$.*

(2) *Suppose that $b \geq 2$. Then there exists $h \in \mathrm{Gal}\left(\overline{E}/E\right)$ which moves P such that $h-1$ kills $\mathcal{J}_{p,q}[p(1-\zeta_q)]$.*

Proof. Both parts are similar so we show the first. Since $a \geq 2$, the extension $E(D_p)/E$ is nontrivial by Lemma 5.2.59(1) and it is disjoint from $E(\mathcal{J}_{p,q}[q])/E$ by Lemma 5.2.24(3). Therefore, there exists $h \in \mathrm{Gal}(\overline{E}/E)$ which moves D_p (and hence, moves P) such that $h-1$ kills $\mathcal{J}_{p,q}[q]$. Since $E = L_{1,1}$ by Lemma 5.2.24(2), we know that $h-1$ also kills $\mathcal{J}_{p,q}[1-\zeta_p]$. □

Recall the definitions of $\mathrm{WM}(Q)$ and $\mathrm{wt}(Q)$ in Definition 2.6.1 and Definition 2.6.5.

Lemma 5.2.63.

(1) *Suppose that $a \geq 2$ and $b \geq 1$. Then for each $Q \in S_P$, we have $p-1, p \in \mathrm{WM}(Q)$.*

(2) *Suppose that $a \geq 1$ and $b \geq 2$. Then for each $Q \in S_P$, we have $q-1, q \in \mathrm{WM}(Q)$.*

Proof. Both parts are similar so we show the first. Since $\mathrm{WM}(Q) = \mathrm{WM}(P)$ for each $Q \in S_P$, we will show that $p-1, p \in \mathrm{WM}(P)$.

By Lemma 5.2.62(1), there exists $h \in \mathrm{Gal}(\overline{E}/E)$ which moves P such that $h-1$ kills $\mathcal{J}_{p,q}[q(1-\zeta_p)]$. By Lemma 5.2.52(3), $h^p - 1$ kills $\mathcal{J}_{p,q}[pq]$, so $h^p P = P$ and hence

$$h^i P \neq P \text{ for } 1 \leq i \leq p-1. \tag{5.26}$$

Since $h-1$ kills $\mathcal{J}_{p,q}[q] \ni pP$, we have $pP \sim p(hP)$, so by (5.26), $p \in \mathrm{WM}(P)$.

Since $h-1$ kills $\mathcal{J}_{p,q}[1-\zeta_p]$, Lemma 5.2.52(2) gives that $1+h+\cdots+h^{p-1}$ kills $\mathcal{J}_{p,q}[p]$, which combined with the fact that $h-1$ kills $\mathcal{J}_{p,q}[q]$ shows that $(1+h+\cdots+h^{p-1})-p$ kills $\mathcal{J}_{p,q}[pq] \ni P$, so

$$hP + h^2P + \cdots + h^{p-1}P \sim (p-1)P,$$

and hence by (5.26), $p-1 \in \mathrm{WM}(P)$. □

Lemma 5.2.64. *Suppose that $Q \in \mathcal{C}_{p,q}(\mathbf{C})$.*

(1) *If $p-1, p \in \mathrm{WM}(Q)$, then*

$$\mathrm{wt}(Q) \geq \begin{cases} 2 & \text{if } q = 3 \\ g\left(\dfrac{q-3}{2}\right) & \text{if } q \geq 5. \end{cases}$$

(2) *If $q-1, q \in \mathrm{WM}(Q)$, then*

$$\mathrm{wt}(Q) \geq \begin{cases} 2 & \text{if } p = 3 \\ g\left(\dfrac{p-3}{2}\right) & \text{if } p \geq 5. \end{cases}$$

Proof. Both parts are similar so we prove the first. Suppose that the gaps of Q are $k_1 < k_2 < \cdots < k_g$. Since $\mathrm{WM}(Q)$ is a monoid and we assume that $p-1, p \in \mathrm{WM}(Q)$,

$$\{p-1, p, 2p-2, 2p-1, 2p, 3p-3, 3p-2, 3p-1, 3p, \cdots\} \subseteq \mathrm{WM}(Q),$$

so

$$k_i - i \geq \begin{cases} 0 & \text{for } i \geq 1, \\ 2 & \text{for } i \geq p-1, \\ 5 & \text{for } i \geq 2p-4, \\ 9 & \text{for } i \geq 3p-8, \\ \vdots & \qquad \vdots \end{cases} \tag{5.27}$$

If $q = 3$, then $g = (p-1)(q-1)/2 = p-1$, so (5.27) implies

$$\mathrm{wt}(Q) = \sum_{i=1}^{g}(k_i - i) \geq 0 + 0 + \cdots + 0 + 2 = 2.$$

If $q \geq 5$, then weakening the bounds in (5.27) yields

$$k_i - i \geq \begin{cases} 0 & \text{for } i \geq 1, \\ 2 & \text{for } i \geq p, \\ 4 & \text{for } i \geq 2p-1, \\ 6 & \text{for } i \geq 3p-2, \\ \vdots & \qquad \vdots \end{cases}$$

so

$$\begin{aligned}\mathrm{wt}(Q) &= \sum_{i=1}^{g}(k_i - i)\\ &\geq 0\cdot(p-1) + 2\cdot(p-1) + \cdots + 2\left(\frac{g}{p-1}-1\right)(p-1)\\ &= g\left(\frac{g}{p-1}-1\right)\\ &= g\left(\frac{q-3}{2}\right)\end{aligned}$$

since $g = (p-1)(q-1)/2$. □

Proposition 5.2.65.

(1) *If $a \geq 2$ and $b \geq 1$, then $q = 3$ and $a \in \{2, 3\}$.*

(2) *If $a \geq 1$ and $b \geq 2$, then $p = 3$ and $b \in \{2, 3\}$.*

Proof. Both parts are similar so we prove the first. Using Theorem 2.6.6, observe that

$$\begin{aligned}g^3 - g &= \sum_{Q\in\mathcal{C}_{p,q}(\mathbf{C})} \mathrm{wt}(Q)\\ &\geq \sum_{Q\in G_E ZP} \mathrm{wt}(Q)\\ &\geq (\#G_E ZP)\left(\min_{Q\in G_E ZP}(\mathrm{wt}(Q))\right)\\ &\geq pq[E(D_p):E]\left(\min_{Q\in G_E ZP}(\mathrm{wt}(Q))\right) \qquad (5.28)\end{aligned}$$

by Lemma 5.2.61(1).

If $q = 3$ and $a \geq 4$, then $g = (p-1)(q-1)/2 = p-1$, Lemma 5.2.64(1) gives $\min_{Q\in G_E ZP}(\mathrm{wt}(Q)) \geq 2$, and Lemma 5.2.59(3) gives $[E(D_p):E] \geq p^2$, so by (5.28),

$$g^3 - g \geq 3p(p^2)(2) > 6(p-1)^3 = 6g^3,$$

which is impossible.

If $q \geq 5$, then $g = (p-1)(q-1)/2$, Lemma 5.2.64(1) gives $\min_{Q\in G_E ZP}(\mathrm{wt}(Q)) \geq g(q-3)/2$, and Lemma 5.2.59(1) gives $[E(D_p):E] \geq p$, so by (5.28),

$$g^3 - g \geq pq(p)\left(g\left(\frac{q-3}{2}\right)\right) > g(p-1)^2\left(\frac{5(q-1)^2}{16}\right) = \frac{5}{4}g^3,$$

which is impossible. □

Lemma 5.2.66. *Suppose that $Q = (x_0, y_0)$ is a torsion point on a superelliptic curve $y^n = f(x)$ where f is monic, $d := \deg(f)$ is coprime to n, and $d[Q - \infty] = 0$. Then there exists $v(x) \in \mathbf{C}[x]$ with $\deg v < d/n$ such that $\mathrm{div}(y - v(x)) = dQ - d\infty$ and $v(x)^n = f(x) - (x - x_0)^d$.*

Proof. Let $\mathcal{F}$ be the function field of the curve. Since $dQ \sim d\infty$, there exists $h \in \mathcal{F}$ such that

$$\operatorname{div}(h) = dQ - d\infty. \tag{5.29}$$

Since h only has poles at ∞, h is a polynomial in x and y. Since the pole at ∞ has order d, it follows (after scaling h by a constant) that $h = y - v(x)$ where $\deg(v) < d/n$. The x-map provides an inclusion of function fields $\mathbf{C}(x) \subseteq \mathcal{F}$, so taking the norm of both sides of (5.29) from $\mathcal{F}$ to $\mathbf{C}(x)$ yields

$$\operatorname{div}(f(x) - (v(x))^n) = d \operatorname{div}(x - x_0) = \operatorname{div}((x - x_0)^d),$$

so $f(x) - (v(x))^n$ and $(x - x_0)^d$ are the same up to a constant multiple; since f is monic and $\deg v < d/n$, they are equal. □

Proposition 5.2.67.

(1) *If* $a, b \leq 1$, *then* $(a, b) \in \{(0, 0), (0, 1), (1, 0)\}$.

(2) *If* $\min\{a, b\} = 0$, *then* $(a, b) \in \{(0, 0), (0, 1), (1, 0)\}$.

Proof.

(1) Then $(1 - \zeta_p)(1 - \zeta_q)[P - \infty] = 0$, which can be rearranged to yield $P + \zeta_p\zeta_q P \sim \zeta_p P + \zeta_q P$, so by Lemma 2.2.3, either $P = \zeta_p P$ or $P = \zeta_q P$, meaning that either a or b is 0.

(2) Without loss of generality, suppose that $a = 0$. Then $qP \sim q\infty$, so if we let c be the x-coordinate of P and define

$$L(x) := x^q + 1 - (x - c)^q, \tag{5.30}$$

then Lemma 5.2.66 shows that there exists $v \in \mathbf{C}[x]$ such that

$$L(x) = v(x)^p. \tag{5.31}$$

A calculation yields

$$\begin{aligned} 1 &= L - \left(\frac{2x - c}{q}\right) L' + \left(\frac{x(x - c)}{q(q - 1)}\right) L'' && \text{(by (5.30))} \\ &= v^{p-2} \left(v^2 - \left(\frac{p(2x - c)}{q}\right) vv' + \frac{px(x - c)}{q(q - 1)} \left((p - 1)(v')^2 + vv''\right) \right) && \text{(by (5.31))}, \end{aligned}$$

so v^{p-2} divides 1, implying v is a constant, so the terms with v' and v'' disappear and we obtain $v^p = 1$, so (5.31) gives $L(x) = 1$, and then (5.30) yields $c = 0$. Hence $[P - \infty] \in \mathcal{J}_{p,q}[1 - \zeta_q]$, so $b \leq 1$. □

Theorem 5.2.68. *P is not an exceptional torsion point; i.e.,* $(a, b) \in \{(0, 0), (0, 1), (1, 0)\}$.

Proof. If $\min\{a, b\} = 0$, then we are done by Proposition 5.2.67(2).

Case A: $\min\{a, b\} \geq 2$

Then Proposition 5.2.65(1) implies $q = 3$ and Proposition 5.2.65(2) implies $p = 3$, which is impossible since p and q are distinct odd primes.

Case B: $\min\{a,b\} = 1$

Without loss of generality, assume that $b = 1$ and $a \geq 1$. Then Proposition 5.2.67(1) implies that $a \geq 2$, so by Proposition 5.2.65(1), $q = 3$ and $a \in \{2, 3\}$. Then $(1 - \zeta_p)^3(1 - \zeta_3)[P - \infty] = 0$, which we can rewrite as

$$\zeta_p^3\zeta_3 P + 3\zeta_p^2 P + 3\zeta_p\zeta_3 P + P \sim \zeta_p^3 P + 3\zeta_p^2\zeta_3 P + 3\zeta_p P + \zeta_3 P \tag{5.32}$$

Case B1: $\{\zeta_p^3\zeta_3 P, \zeta_p^2 P, \zeta_p\zeta_3 P, P\} \cap \{\zeta_p^3 P, \zeta_p^2\zeta_3 P, \zeta_p P, \zeta_3 P\} \neq \emptyset$

Then P is fixed by some $z \in Z \setminus \{1\}$, so it is fixed by either ζ_p or ζ_3, which implies that $(a, b) \in \{(0, 0), (0, 1), (1, 0)\}$.

Case B2: $\{\zeta_p^3\zeta_3 P, \zeta_p^2 P, \zeta_p\zeta_3 P, P\} \cap \{\zeta_p^3 P, \zeta_p^2\zeta_3 P, \zeta_p P, \zeta_3 P\} = \emptyset$

Then (5.32) gives a degree 8 map $\upsilon \colon \mathcal{C}_{p,q} \to \mathbf{P}^1$, so applying Corollary 2.2.2 with υ and the y-map yields

$$(3 - 1)(p - 1)/2 \leq (3 - 1)(8 - 1),$$

so $p \leq 15$; thus, $p \in \{5, 7, 11, 13\}$. By Lemma 5.2.47, there exists a nontrivial $\gamma \in \operatorname{Gal}(L_{a,1}/L_{a-1,1})$. Lemma 5.2.59(2) gives $L_{a,1} = E(D_p)$, so γ moves D_p and hence γ moves P. Since $\gamma - 1$ kills $\mathcal{J}[(1 - \zeta_p)^{a-1}]$, Lemma 5.2.52(1) gives that $(\gamma - 1)^2$ kills $\mathcal{J}[(1 - \zeta_p)^{2(a-1)}]$. Also, $\gamma - 1$ kills $\mathcal{J}[1 - \zeta_q]$, so $(\gamma - 1)^2$ also kills $\mathcal{J}[1 - \zeta_q]$. Hence $(\gamma - 1)^2$ kills $\mathcal{J}[(1 - \zeta_p)^{2(a-1)}(1 - \zeta_q)]$, and since $2(a - 1) \geq a$, it kills P. Therefore,

$$\gamma^2 P + P \sim 2\gamma P,$$

so Lemma 2.2.3 implies $P = \gamma P$, contradicting the fact that γ moves P. □

The hyperelliptic case

Theorem 5.2.69 ([15]). *The set of exceptional torsion points of $\mathcal{C}_{2,5}$ is the Z-orbit of $(\sqrt[5]{4}, \sqrt{5})$. Each has exact order $(1 - \zeta_5)^3$; in particular, each is killed by 5.*

Proof. On pages 206–207 of [15], Coleman computes the torsion points of the curve $w^5 = u(1 - u)$, which is isomorphic to $\mathcal{C}_{2,5}$. See also [54]. □

Theorem 5.2.70. *When $q \geq 7$ is prime, $\mathcal{C}_{2,q}$ has no exceptional torsion points.*

Proof. This is Theorem 1.1 of [29], which classifies torsion points on the isomorphic curve $x^q = y(1 - y)$. □

Some remaining curves

Proposition 5.2.71.

(1) *For $(n, d) \in \{(2, 9), (8, 3), (2, 15), (2, 25), (4, 5)\}$, $\mathcal{C}_{n,d}$ has no exceptional torsion points.*

(2) *The set of exceptional torsion points of $\mathcal{C}_{4,3}$ is the Z-orbit of $(2, \sqrt{3})$. Each has exact order $(1 - \zeta_4)(1 - \zeta_3)^2$; in particular, each is killed by 12.*

Proof. A computation with `Magma` yields

$$\begin{aligned}
&\operatorname{div}\left(\zeta_{12}^3+2\zeta_{12}^2-2\zeta_{12}-1-6\left(\frac{x^2-(-2\zeta_{12}^2+1)xy-x-3y^2-(4\zeta_{12}^2-2)y+1}{y^3+(6\zeta_{12}^2-3)y^2-9y-6\zeta_{12}^2+3}\right)\right)\\
&=(1-\zeta_4)(1-\zeta_3)^2(2,\sqrt{3}),\\
&\operatorname{div}((12-4\sqrt{3}y)x^2+(18y^2-8\sqrt{3}y-6)x+y^4-12\sqrt{3}y^3+18y^2-4\sqrt{3}y+9)\\
&=12(2,\sqrt{3})-12\infty,
\end{aligned}$$

so this shows that the point $(2,\sqrt{3})$ is a torsion point of $\mathcal{C}_{4,3}$; hence, its Z-orbit will also consist of torsion points of the same order.

Suppose for contradiction that P were an exceptional torsion point of $\mathcal{C}_{n,d}$ and that P does not lie in the Z-orbit of $(2,\sqrt{3})$ when $(n,d)=(4,3)$.

Case A: $(n,d)\in\{(2,9),(4,3),(8,3)\}$

Let $\varphi_{n,d}\colon\mathcal{C}_{n,d}\to\mathcal{C}_{2,3}$ be defined by $\varphi_{n,d}(x,y)=(x^{d/3},y^{n/2})$. Define $S_0\subseteq\mathcal{C}_{2,3}(\overline{\mathbf{Q}})$ as follows: for $(n,d)\in\{(2,9),(8,3)\}$, S_0 is the union of the Z-orbit of $\{\infty,(0,1),(-1,0)\}$; for $(n,d)=(4,3)$, S_0 is the union of the Z-orbit of $\{\infty,(0,1),(-1,0),(2,3)\}$. Our assumptions on P imply $\varphi_{n,d}(P)\notin S_0$. Proposition 5.2.22(i) gives $nd[P-\infty]=0$, so $\varphi_{n,d}(P)\in C_{2,3}[nd]$ and hence P must lie in the finite set $S_{n,d}:=\varphi_{n,d}^{-1}(\mathcal{C}_{2,3}[nd]\setminus S_0)$.

Since $\mathcal{C}_{n,d}$ has good reduction at 71, let $\mathcal{C}_{n,d,71}$ be the reduced curve over $\mathbf{F}_{71}$, let $P_{71}\in\mathcal{C}_{n,d,71}(\overline{\mathbf{F}_{71}})$ be the reduction of P, and let $S_{n,d,71}\subseteq\mathcal{C}_{n,d,71}(\overline{\mathbf{F}_{71}})$ be the reduction of $S_{n,d}$, so $P_{71}\in S_{n,d,71}$ is such that $ndP_{71}-nd\infty$ is a principal divisor. Using division polynomials, we use `Magma` to compute $S_{n,d,71}$ explicitly and find that $S_{n,d,71}\subseteq\mathcal{C}_{n,d,71}(\mathbf{F}_{71^{24}})$. We use the `IsPrincipal` feature of `Magma` over $\mathbf{F}_{71^{24}}$ to find that there are no $Q\in S_{n,d,71}$ such that $ndQ-nd\infty$ is a principal divisor, so P_{71}, and hence P, cannot exist.

Case B: $(n,d)\in(2,15),(2,25),(4,5)\}$

Let $N_{n,d}=nd$ if $(n,d)\in\{(2,15),(2,25)\}$ and let $N_{n,d}=3nd$ if $(n,d)\in\{4,5\}$. By Proposition 5.2.22(ii), $N_{n,d}[P-\infty]=0$. Let $\varphi_{n,d}\colon\mathcal{C}_{n,d}\to\mathcal{C}_{2,5}$ be defined by $\varphi_{n,d}(x,y)=(x^{d/5},y^{n/2})$ and $\mathcal{T}_{2,5}$ be the exceptional torsion points of $\mathcal{C}_{2,5}$ listed in Theorem 5.2.69. As in Case A, we see that P lies in the finite set $S_{n,d}:=\varphi_{n,d}^{-1}(\mathcal{T}_{2,5})$. Since $\mathcal{C}_{n,d}$ has good reduction at 54001, we can define the reduced curve $\mathcal{C}_{n,d,54001}$ and the reductions P_{54001}, $S_{n,d,54001}$ of P, $S_{n,d}$ respectively. We use `Magma` to compute $S_{n,d,54001}$ explicitly and find that $S_{n,d,54001}\subseteq\mathcal{C}_{n,d,54001}(\mathbf{F}_{54001})$. We use the `IsPrincipal` feature of `Magma` over $\mathbf{F}_{54001}$ to find that there are no $Q\in S_{n,d,54001}$ such that $N_{n,d}Q-N_{n,d}\infty$ is a principal divisor, so P_{54001}, and hence P, cannot exist. □

Main Theorem

Lemma 5.2.72. *Suppose that n',d' are integers such that $n'|n$ and $d'|d$. If $\mathcal{C}_{n',d'}$ has no exceptional torsion points, then neither does $\mathcal{C}_{n,d}$.*

Proof. The map $\mathcal{C}_{n,d}\to\mathcal{C}_{n',d'}$ given by $(x,y)\mapsto(x^{d/d'},y^{n/n'})$ sends exceptional torsion points to exceptional torsion points. □

Theorem 5.2.73. *Suppose that n, d are coprime integers with $n, d \geq 2$.*

(1) *If $(n, d) = (2, 3)$, then $\mathcal{C}_{2,3}$ is an elliptic curve, so it has infinitely many torsion points.*

(2) *If $(n, d) = (2, 5)$, then the set of exceptional torsion points of $\mathcal{C}_{2,5}$ is the Z-orbit of $(\sqrt[5]{4}, \sqrt{5})$. Each has exact order $(1 - \zeta_5)^3$; in particular, each is killed by 5.*

(3) *If $(n, d) = (4, 3)$, then the set of exceptional torsion points of $\mathcal{C}_{4,3}$ is the Z-orbit of $(2, \sqrt{3})$. Each has exact order $(1 - \zeta_4)(1 - \zeta_3)^2$; in particular, each is killed by 12.*

(4) *If $(n, d) \in \{(3, 2), (5, 2), (3, 4)\}$, then $\mathcal{C}_{n,d} \simeq \mathcal{C}_{d,n}$ via $(x, y) \in \mathcal{C}_{n,d} \mapsto (\zeta_{2n} y, \zeta_{2d} x) \in \mathcal{C}_{d,n}$, so the exceptional torsion points of $\mathcal{C}_{n,d}$ are described by one of Theorem 5.2.73(1), Theorem 5.2.73(2), Theorem 5.2.73(3).*

(5) *Otherwise, $\mathcal{C}_{n,d}$ has no exceptional torsion points.*

Proof. Without loss of generality, suppose that d is odd.

Suppose that n is divisible by an odd prime p. Let q be an odd prime dividing d. By Theorem 5.2.68, $\mathcal{C}_{p,q}$ has no exceptional torsion points, so Lemma 5.2.72 implies that $\mathcal{C}_{n,d}$ has no exceptional torsion points.

So we may assume that that $n = 2^i$ for an integer $i \geq 1$. If d has a prime factor $q \geq 7$, then Theorem 5.2.70 implies that $\mathcal{C}_{2,q}$ has no exceptional torsion points, so Lemma 5.2.72 implies that $\mathcal{C}_{n,d}$ has no exceptional torsion points.

So we may assume that there exist integers $j, k \geq 0$ such that $d = 3^j 5^k$ and $(j, k) \neq (0, 0)$.

Case A: $j + k \geq 2$

Then n is divisible by 2 and d is divisible by either 9, 15, or 25, so we are done by Proposition 5.2.71(1) and Lemma 5.2.72.

Case B: $(j, k) = (1, 0)$

If $i \geq 3$, then n is divisible by 8. Since $d = 3$, we are done by Proposition 5.2.71(1) and Lemma 5.2.72. The case $(n, d) = (4, 3)$ is handled by Proposition 5.2.71(2). The case $(n, d) = (2, 3)$ is Theorem 5.2.73(1).

Case C: $(j, k) = (0, 1)$

If $i \geq 2$, then n is divisible by 4. Since $d = 5$, we are done by Proposition 5.2.71(1) and Lemma 5.2.72. The case $(n, d) = (2, 5)$ is handled by Theorem 5.2.69. □

5.3 Torsion points on a generic superelliptic curve

As usual, for any superelliptic curve $y^n = (x - a_1) \cdots (x - a_d)$, the automorphism ζ_n refers to the map given by$(x, y) \mapsto (x, \zeta_n y)$. The points fixed by ζ_n are $\{(a_1, 0), \ldots, (a_d, 0), \infty\}$, and they are torsion points whose order divides n.

The aim of this section is to prove the following result.

Theorem 5.3.1. *Suppose that $n, d \geq 2$ are coprime and satisfy $n + d \geq 7$. Let $\mathscr{C}_n$ be the curve over $k := \mathbf{Q}(a_1, \ldots, a_d)$ defined by the equation*

$$y^n = \prod_{x=1}^{d} (x - a_i).$$

Suppose that $\mathscr{C}_n$ is embedded into its jacobian $\mathscr{J}_n$ using the unique point ∞ at infinity. Points fixed by ζ_n are torsion points of order dividing n.

(1) *If $d \geq 3$, there are no other torsion points defined over $\overline{k}$.*

(2) *If $d = 2$ and $n \neq 5$, the only other torsion points defined over $\overline{k}$ are*

$$\left\{ \left(\frac{a_1 + a_2}{2}, -\zeta_n^i \sqrt[n]{\left(\frac{a_1 - a_2}{2}\right)^2} \right) : 0 \leq i \leq n-1 \right\}.$$

(3) *If $d = 2$ and $n = 5$, the only other torsion points defined over $\overline{k}$ are*

$$\left\{ \left(\frac{a_1 + a_2}{2}, -\zeta_5^i \sqrt[5]{\left(\frac{a_1 - a_2}{2}\right)^2} \right) : 0 \leq i \leq 4 \right\} \bigcup$$
$$\left\{ \left(\frac{\pm(a_2 - a_1)\sqrt{5} + (a_1 + a_2)}{2}, \zeta_5^i \sqrt[5]{(a_2 - a_1)^2} \right) : 0 \leq i \leq 4 \right\}.$$

This extends Theorem 7.1 of [57] from $n = 2$ to all n. To prove Theorem 5.3.1, we need a few more results about torsion points on certain curves.

5.3.1 The curves $y^n = x^d + x$

Proposition 5.3.2. *Suppose that $n, d \geq 2$ are coprime, P is a torsion point of $y^n = x^d + x$ whose order divides d, and $P \neq \infty$. Then $d = 2$ or $(n, d) = (2, 3)$.*

Proof. Let the x-coordinate of P be c. By Lemma 5.2.66, there exists $v \in \mathbf{C}[x]$ with $\deg v < d/n$ such that

$$v(x)^n = x^d + x - (x - c)^d. \tag{5.33}$$

Let $x' := x - c/2$ and define $u(x) := v(x + c/2)$. Using (5.33) with x and $c - x$, a computation yields

$$u(x')^n + (-1)^d u(-x')^n = \left(1 - (-1)^d\right) x' + \left(1 + (-1)^d\right) \frac{c}{2}. \tag{5.34}$$

Case A: d is even

Suppose for contradiction that $d > 2$. Factoring the left hand side of (5.34) yields

$$\prod_{i=0}^{n-1} (u(x') + \zeta_n^i \cdot \zeta_{2n} u(-x')) = c.$$

In particular, $u(x') + \zeta_{2n} u(-x')$ and $u(x') + \zeta_{2n} \cdot \zeta_n u(-x')$ are forced to be constants, so $u(x')$ and $u(-x')$ are constants, so $v(x)$ is constant, so by (5.33),

$$x^d + x - (x - c)^d \text{ is constant.} \tag{5.35}$$

Since $d > 2$, the x^{d-1}-coefficient of $x^d + x - (x - c)^d$ is dc, so (5.35) implies $c = 0$, so $x^d + x - (x - c)^d = x$, but this contradicts (5.35).

Case B: d is odd

Factoring the left hand side of (5.34) yields

$$\prod_{i=0}^{n-1}(u(x') - \zeta_n^i u(-x')) = 2x'. \tag{5.36}$$

Case B1: $n \geq 3$

Considering the degree of each factor in (5.36) shows that at least two of them must be constants, which will force $u(x')$ and $u(-x')$ to be constant, and we can repeat the same argument as in Case A to get a contradiction.

Case B2: $n = 2$

Then (5.36) becomes

$$(u(x') + u(-x'))(u(x') - u(-x')) = 2x'. \tag{5.37}$$

Since $u(x')+u(-x')$ is an even polynomial and $u(x')-u(-x')$ is an odd polynomial, (5.37) forces $u(x') + u(-x')$ to be constant and $u(x') - u(-x')$ to be a multiple of x'. Then $\deg u = 1$, so $\deg v = 1$. Let $v(x) = ax + b$, so (5.33) gives

$$(ax + b)^2 = x^d + x - (x - c)^d. \tag{5.38}$$

Considering the coefficient of x^{d-1}, we conclude that either $c = 0$ or $d = 3$. If $c = 0$, then (5.38) implies that $x = (ax+b)^2$, which is impossible. So we conclude that $(n, d) = (2, 3)$. □

5.3.2 Two curves for which $n + d = 7$

Proposition 5.3.3.

(1) *If P is a torsion point on $y^3 = x^4 + x^2 + 1$ with $12[P - \infty] = 0$, then P is fixed by ζ_3.*

(2) *If P is a torsion point on $y^4 = x^3 + x^2 + 1$ with $12[P - \infty] = 0$, then P is fixed by ζ_4.*

Proof. Let $\mathcal{C}$ be the curve $y^3 = x^4 + x^2 + 1$, let E be the elliptic curve $y^3 = x^2 + x + 1$, let $\varphi\colon \mathcal{C} \to E$ be the 2-to-1 map $(x, y) \mapsto (x^2, y)$, let S_0 be the points of E fixed by ζ_3, and suppose for contradiction that P is a torsion point of $\mathcal{C}$ with $12[P - \infty] = 0$ such that P is not fixed by ζ_3. Then $\varphi(P) \in E[12]$, so P lies in the finite set $S := \varphi^{-1}(E[12] \setminus S_0)$.

Since $\mathcal{C}$ has good reduction at 47, let $\mathcal{C}_{47}$ be the reduced curve over $\mathbf{F}_{47}$, let $P_{47} \in \mathcal{C}_{47}(\overline{\mathbf{F}_{47}})$ be the reduction of P, and let $S_{47} \subseteq \mathcal{C}_{47}(\overline{\mathbf{F}_{47}})$ be the reduction of S, so $P_{47} \in S_{47}$ is such that $12P_{47} - 12\infty$ is a principal divisor. Using division polynomials, we use `Magma` to compute S_{47} explicitly and find that $S_{47} \subseteq \mathcal{C}_{47}(\mathbf{F}_{47^4})$. We use the `IsPrincipal` feature of `Magma` over $\mathbf{F}_{47^4}$ to find that there are no $Q \in S_{47}$ such that $12Q - 12\infty$ is a principal divisor, so P_{47}, and hence P, cannot exist.

The curve $y^4 = x^3 + x + 1$ is a 2-to-1 cover of the elliptic curve $y^2 = x^3 + x + 1$ and the same technique happens to work over $\mathbf{F}_{47^4}$ again. □

5.3.3 Proof of Theorem 5.3.1

Case A: $d = 2$

$\mathcal{C}_{2,n}$ is isomorphic over k to $y^n = (x-a_1)(x-a_2)$ via the isomorphism

$$(x,y) \in \mathcal{C}_{2,n} \mapsto \left(\frac{(a_2-a_1)y + (a_1+a_2)}{2}, \sqrt[n]{\frac{(a_2-a_1)^2}{4}x} \right) \in \mathscr{C}_n,$$

so Theorem 5.2.73 gives Theorem 5.3.1(2) and Theorem 5.3.1(3).

Case B: $d \geq 3$

Suppose that P is a torsion point of $\mathscr{C}_n$ of order m. Let $M = \operatorname{lcm}(m, nd)$. Since $\mathscr{J}_n[M]$ is a finite étale cover of $\operatorname{Spec} k$, every specialization map will induce an isomorphism on the M-torsion of the jacobian.

Case B1: $(n,d) \notin \{(3,4),(4,3)\}$

Specializing to $\mathcal{C}_{n,d}$ and using Theorem 5.2.73 gives $(1-\zeta_n)[P-\infty] = 0$ or $d[P-\infty] = 0$. If $d[P-\infty]=0$, then specializing to $y^n = x^d + x$ and using Proposition 5.3.2 gives $P = \infty$.

Case B2: $(n,d) = (3,4)$

Specializing to $\mathcal{C}_{n,d}$ and using Theorem 5.2.73 gives $nd[P-\infty]=0$. Specializing to $y^3 = x^4 + x^2 + 1$ and using Proposition 5.3.3(1) gives $(1-\zeta_3)[P-\infty]=0$.

Case B3: $(n,d) = (4,3)$

Specializing to $\mathcal{C}_{n,d}$ and using Theorem 5.2.73 gives $nd[P-\infty]=0$. Specializing to $y^4 = x^3 + x + 1$ and using Proposition 5.3.3(2) gives $(1-\zeta_4)[P-\infty]=0$.

Bibliography

[1] G Anderson and Yasutaka Ihara. “Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units. Part 2”. In: *Int’l Math. J* 1 (1990), pp. 119–148 (cit. on p. 13).

[2] Greg Anderson and Yasutaka Ihara. “Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units”. In: *Ann. of Math.* (1988), pp. 271–293 (cit. on p. 13).

[3] Enrico Arbarello et al. *Geometry of Algebraic Curves, Volume I.* Springer, 1985 (cit. on p. 53).

[4] Vishal Arul. “Division by $1 - \zeta$ on superelliptic curves and jacobians”. In: *arXiv preprint arXiv:1810.07299* (2019) (cit. on p. 27).

[5] Vishal Arul. “On the ℓ-adic valuation of certain Jacobi sums”. In: *arXiv preprint arXiv:1910.14249* (2019) (cit. on p. 59).

[6] Vishal Arul. “Torsion points on Fermat quotients of the form $y^n = x^d + 1$”. In: *arXiv preprint arXiv:1910.14251* (2019) (cit. on p. 81).

[7] Vishal Arul et al. “Computing zeta functions of cyclic covers in large characteristic”. In: *The Open Book Series* 2.1 (2019), pp. 37–53 (cit. on pp. 9, 61).

[8] Matthew H Baker and Kenneth A Ribet. “Galois theory and torsion points on curves”. In: *J. Théor. Nombres Bordeaux* 15.1 (2003), pp. 11–32 (cit. on p. 11).

[9] Jennifer S Balakrishnan, Robert W Bradshaw, and Kiran S Kedlaya. “Explicit Coleman integration for hyperelliptic curves”. In: *International Algorithmic Number Theory Symposium.* Springer. 2010, pp. 16–31 (cit. on p. 9).

[10] Leonard D Baumert. *Cyclic difference sets.* Vol. 182. Springer, 2006 (cit. on p. 59).

[11] Bruce C Berndt, Kenneth S Williams, and Ronald J Evans. *Gauss and Jacobi sums.* Wiley, 1998 (cit. on pp. 59, 88, 89).

[12] Michael Victor Berry and Sz Klein. “Integer, fractional and fractal Talbot effects”. In: *J. Modern Opt.* 43.10 (1996), pp. 2139–2164 (cit. on p. 59).

[13] Alex Best. *Square root time Coleman integration on superelliptic curves.* Preprint, `https://alexjbest.github.io/papers/coleman-superelliptic.pdf` (cit. on p. 9).

[14] Christina Birkenhake and Herbert Lange. *Complex abelian varieties.* Vol. 302. Springer Science & Business Media, 2004 (cit. on p. 52).

[15] Robert F. Coleman. “Torsion points on Fermat curves”. In: *Compos. Math.* 58.2 (1986), pp. 191–208 (cit. on pp. 3, 11, 82, 107).

[16] Robert F. Coleman, P. Tzermias, and A. Tamagawa. “The cuspidal torsion packet on the Fermat curve”. In: *J. Reine Angew. Math.* 496 (1998), pp. 73–81 (cit. on p. 82).

[17] Keith Conrad. “Jacobi sums and Stickelberger’s congruence”. In: *Enseign. Math.* 41 (1995), pp. 141–141 (cit. on p. 62).

[18] Tim Dokchitser. “Models of curves over DVRs”. In: *arXiv preprint arXiv:1807.00025* (2018) (cit. on p. 54).

[19] Bernard Dwork. “On the rationality of the zeta function of an algebraic variety”. In: *American Journal of Mathematics* 82.3 (1960), pp. 631–648 (cit. on p. 60).

[20] Ronald Evans. “Congruences for Jacobi sums”. In: *J. Number Theory* 71.1 (1998), pp. 109–120 (cit. on pp. 12, 62).

[21] Hershel M. Farkas and Irwin Kra. *Riemann surfaces.* Springer, 1992, pp. 9–31 (cit. on pp. 26, 44).

[22] Carla Farsi and Neil Watling. “Cubic algebras”. In: *J. Operator Theory* (1993), pp. 243–266 (cit. on p. 59).

[23] Carla Farsi and Neil Watling. “Quartic algebras”. In: *Canad. J. Math.* 44.6 (1992), pp. 1167–1191 (cit. on p. 59).

[24] John David Fay. *Theta functions on Riemann surfaces.* Vol. 352. Springer, 2006 (cit. on p. 56).

[25] William Fulton. *Algebraic curves: an introduction to algebraic geometry.* Addison-Wesley, 1989 (cit. on p. 15).

[26] Steven Galbraith, Sachar Paulus, and Nigel Smart. “Arithmetic on superelliptic curves”. In: *Math. Comp.* 71.237 (2002), pp. 393–405 (cit. on pp. 9, 28).

[27] Pierrick Gaudry and Nicolas Gürel. “An extension of Kedlaya’s point-counting algorithm to superelliptic curves”. In: *International Conference on the Theory and Application of Cryptology and Information Security.* Springer. 2001, pp. 480–494 (cit. on p. 9).

[28] Cécile Gonçalves. “A point counting algorithm for cyclic covers of the projective line”. In: *Algorithmic arithmetic, geometry, and coding theory* 637 (2015), pp. 145–172 (cit. on pp. 9, 61).

[29] David Grant and Delphy Shaulis. “The cuspidal torsion packet on hyperelliptic Fermat quotients”. In: *J. Théor. Nombres Bordeaux* 16.3 (2004), pp. 577–585 (cit. on pp. 3, 10, 11, 13, 82, 107).

[30] Benedict H. Gross and David E. Rohrlich. “Some results on the Mordell-Weil group of the jacobian of the Fermat curve”. In: *Invent. Math.* 44.3 (1978), pp. 201–224 (cit. on p. 102).

[31] Alexander Grothendieck. “Formule de Lefschetz et rationalité des fonctions L”. In: *Séminaire Bourbaki* 9 (1964), pp. 41–55 (cit. on p. 60).

[32] Alexandre Grothendieck. “Revêtement étales et groupe fondamental (SGA1)”. In: *Lecture Notes in Math.* 224 (1971) (cit. on p. 44).

[33] JH Hannay and Michael V Berry. “Quantization of linear maps on a torus-Fresnel diffraction by a periodic grating”. In: *Phys. D* 1.3 (1980), pp. 267–290 (cit. on p. 59).

[34] Yasutaka Ihara. “Profinite braid groups, Galois representations and complex multiplications”. In: *Ann. of Math.* 123.1 (1986), pp. 43–106 (cit. on pp. 12, 62).

[35] Haruo Ishibashi. "The Terwilliger algebras of certain association schemes over the Galois rings of characteristic 4". In: *Graphs Combin.* 12.1 (1996), pp. 39–54 (cit. on p. 59).

[36] K Iwasawa. "A note on Jacobi sums". In: *Symposia Math.* Vol. 15. 1975, pp. 447–459 (cit. on pp. 12, 62).

[37] Tomasz Jędrzejak. "A note on the torsion of the jacobians of superelliptic curves $y^q = x^p + a$". In: *Banach Center Publ.* 108.1 (2016), pp. 143–149 (cit. on pp. 60, 82, 102).

[38] Tomasz Jędrzejak. "On the torsion of the jacobians of superelliptic curves $y^q = x^p + a$". In: *J. Number Theory* 145 (2014), pp. 402–425 (cit. on pp. 60, 82).

[39] Dieter Jungnickel. "Difference sets". In: *Contemporary design theory: A collection of surveys* (1992), pp. 241–324 (cit. on p. 59).

[40] Dieter Jungnickel. "Finite fields". In: *Structure and Arithmetics, Wissenshaftsverlag, Mannheim* (1993) (cit. on p. 59).

[41] Nicholas M. Katz. "Crystalline cohomology, Dieudonné modules, and Jacobi sums". In: *Automorphic forms, representation theory and arithmetic.* Springer, 1981, pp. 165–246 (cit. on pp. 60, 87, 88).

[42] KS Kedlaya. "Counting points on hyperelliptic curves using Monsky-Washinitzer cohomology". In: *J. Ramanujan Math. Soc.* 16.4 (2001), pp. 323–338 (cit. on p. 9).

[43] Neal Koblitz. "Jacobi sums, irreducible zeta-polynomials, and cryptography". In: *Can. Math. Bull* 34.2 (1991), pp. 229–235 (cit. on p. 59).

[44] Masato Kurihara. "Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$". In: *Compos. Math.* 81.2 (1992), pp. 223–236 (cit. on p. 99).

[45] Philippe Langevin. "Some sequences with good autocorrelation properties". In: *Contemp. Math.* 168 (1994), pp. 213–213 (cit. on p. 59).

[46] JS Lomont. "A generalization and refinement of Madivanane's theorem on general involutional transformations". In: *J. Math. Phys.* 26.9 (1985), pp. 2087–2091 (cit. on p. 59).

[47] Robert J McEliece and Howard Rumsey Jr. "Euler products, cyclotomy, and coding". In: *J. Number Theory* 4.3 (1972), pp. 302–311 (cit. on p. 59).

[48] Hiroo Miki. "On the l-adic expansion of certain Gauss sums and its applications". In: *Galois Representations and Arithmetic Algebraic Geometry.* Mathematical Society of Japan. 1987, pp. 87–118 (cit. on pp. 12, 62).

[49] Moritz Minzlaff. "Computing zeta functions of superelliptic curves in larger characteristic". In: *Mathematics in Computer Science* 3.2 (2010), pp. 209–224 (cit. on pp. 9, 61).

[50] Rick Miranda. *Algebraic curves and Riemann surfaces.* Vol. 5. American Mathematical Soc., 1995 (cit. on p. 44).

[51] Pascal Molin and Christian Neurohr. "Computing period matrices and the Abel-Jacobi map of superelliptic curves". In: *Mathematics of Computation* (2019) (cit. on pp. 23, 24).

[52] David Mumford. "Tata lectures on theta II". In: *Progr. Math.* 43 (1984) (cit. on p. 27).

[53] Atsushi Nakayashiki. “Tau Function Approach to Theta Functions”. In: *Int. Math. Res. Not. IMRN* 2016.17 (2015), pp. 5202–5248 (cit. on pp. 25, 26, 44, 56).

[54] Bjorn Poonen. “Computing torsion points on curves”. In: *Exp. Math.* 10.3 (2001), pp. 449–466 (cit. on p. 107).

[55] Bjorn Poonen. “Explicit descent for Jacobians of cyclic covers of the projective line”. In: *J. Reine Angew. Math.* 488 (1997), pp. 141–188 (cit. on p. 16).

[56] Bjorn Poonen. *Lectures on rational points on curves.* https://math.mit.edu/~poonen/papers/curves.pdf. Mar. 2006 (cit. on pp. 15–17, 20).

[57] Bjorn Poonen and Michael Stoll. “Most odd degree hyperelliptic curves have only one rational point”. In: *Ann. of Math.* 180.3 (2014), pp. 1137–1166 (cit. on pp. 3, 10, 11, 13, 82, 110).

[58] Viktor Prasolov. *Problems and theorems in linear algebra.* Vol. 134. American Mathematical Society, 1994 (cit. on p. 33).

[59] Edward F Schaefer. “Computing a Selmer group of a Jacobian using functions on the curve”. In: *Math. Ann* 310 (1998), pp. 447–471 (cit. on pp. 16, 17, 21).

[60] Jean-Pierre Serre. *Local fields.* Vol. 67. Springer Science & Business Media, 2013 (cit. on p. 20).

[61] Vyacheslav Spiridonov and Alexei Zhedanov. “Zeros and orthogonality of the Askey-Wilson polynomials for q a root of unity”. In: *Duke Math. J.* 89.2 (1997), pp. 283–305 (cit. on p. 59).

[62] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Vol. 254. Springer Science & Business Media, 2009 (cit. on p. 16).

[63] Tsuyoshi Uehara. “On a congruence relation between Jacobi sums and cyclotomic units”. In: *J. Reine Angew. Math* 382 (1987), pp. 199–214 (cit. on pp. 3, 12, 62).

[64] Lawrence C. Washington. *Introduction to cyclotomic fields.* Vol. 83. Springer Science & Business Media, 1997 (cit. on pp. 97, 99).

[65] André Weil et al. “Numbers of solutions of equations in finite fields”. In: *Bull. Amer. Math. Soc* 55.5 (1949), pp. 497–508 (cit. on p. 60).

[66] Mieko Yamada. “Distance-regular digraphs of girth 4 over an extension ring of $\mathbf{Z}/4\mathbf{Z}$”. In: *Graphs Combin.* 6.4 (1990), pp. 381–394 (cit. on p. 59).

[67] Mieko Yamada. “Hadamard matrices generated by an adaptation of generalized quaternion type array”. In: *Graphs Combin.* 2.1 (1986), pp. 179–187 (cit. on p. 59).

[68] Yuri G Zarhin. “Division by 2 on odd degree hyperelliptic curves and their jacobians”. In: *Izv. Math.* 83.3 (2019), pp. 501–520 (cit. on pp. 3, 10, 13, 27, 39).

[69] Yuri G Zarhin. “Halves of points of an odd degree hyperelliptic curve in its jacobian”. In: *Integrable Systems and Algebraic Geometry* 2 (2020), pp. 102–118 (cit. on p. 43).

[70] AS Zhedanov. “Gauss sums and orthogonal polynomials”. In: *Internat. J. Modern Phys. A* 12.01 (1997), pp. 289–294 (cit. on p. 59).