Distribution Agreement

In presenting this thesis or dissertation as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis or dissertation in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this thesis or dissertation. I retain all ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Signature:

_____ _____

Christopher Keyes Date

Topics in arithmetic statistics

By

Christopher Keyes
Doctor of Philosophy

Mathematics

David Zureick-Brown, Ph.D.
Advisor

Raman Parimala, Ph.D.
Committee Member

Brooke Ullery, Ph.D.
Committee Member

Accepted:

Kimberly Jacob Arriola, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

Topics in arithmetic statistics

By

Christopher Keyes
B.S., Tufts University, MA, 2018
M.S., Emory University, GA, 2021

Advisor: David Zureick-Brown, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2023

Abstract

Topics in arithmetic statistics
By Christopher Keyes

Arithmetic statistics encompasses a broad class of questions in number theory and arithmetic geometry of a distinctly quantitative flavor. In this thesis the author addresses three such questions, the first two of which are related to superelliptic curves, which are given by an equation of the form $C_f \colon y^m = f(x, z)$. For a fixed such curve defined over the rational numbers $\mathbb{Q}$ and an appropriately chosen degree n, we give an asymptotic lower bound on the number of finite extensions $K/\mathbb{Q}$ of degree n arising as the minimal field of definition for an algebraic point on C_f, counted by absolute discriminant. Rather than fixing the curve, we could instead ask how often a family of superelliptic curves has certain arithmetic properties. In particular, we study how often such curves are everywhere locally soluble, computing exactly the density of f such that C_f has points everywhere locally. Finally, we interpret the Mertens' classical product theorem as a statement about the density of integers lacking small prime factors. We then prove a generalization to Chebotarev sets of prime ideals in Galois extensions of number fields.

Topics in arithmetic statistics

By

Christopher Keyes
B.S., Tufts University, MA, 2018
M.S., Emory University, GA, 2021

Advisor: David Zureick-Brown, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2023

Acknowledgments

This thesis and the work that went into it would not have been possible without the generous support of my many mentors, colleagues, family, and friends. There are many more of you than I can mention here, so if you are not listed below, please know that I value your contributions.

To my PhD advisor, Professor David Zureick-Brown, thank you for your patient guidance in all matters professional and mathematical.

To my many mentors to whom I have turned for advice, especially Robert Lemke Oliver, Lea Beneish, Jackson Morrow, and Daniel Keliher, thank you for helping me to join and feel at home in the mathematical community.

To my collaborators, past and present, Lea Beneish, Daniel Keliher, Santiago Arango-Piñeros, and Tomer Reiter, thank you for your sustained effort in our projects. I feel fortunate to have co-authors with whom working brings joy.

To my Emory cohort, including (but not limited to) Kavinda, Kelvin, Irving, Marcelo, Diane, and Jack, thank you for making my time in Atlanta fun and memorable.

To my family, Laura, Phil, and Tor, thank you for always backing my ambitions, and in particular for putting up with me studying for my qualifying exams during a family vacation.

And to Becky, thank you for your unwavering love and kindness. It is truly an eternal inspiration.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Arithmetic statistics encompasses a broad class of quantitative questions involving objects and properties of interest to number theorists and arithmetic geometers. Examples of these objects are number fields, solutions to polynomial equations, and of course, prime numbers. In this dissertation, we address arithmetic statistical topics relating to these three objects. To set the stage, we introduce each object, and state our main results.

1.1 Counting number fields

Fix an integer $n \geq 2$ and consider the following question.

Question 1.1.1. *How many number fields $K/\mathbb{Q}$ of degree n are there?*

Since there are infinitely many such extensions, we make this precise by considering the asymptotic behavior of

$$N_n(X) = \#\left\{K/\mathbb{Q} \mid [K:\mathbb{Q}] = n,\ |\mathrm{Disc}\, K/\mathbb{Q}| \leq X\right\}.$$

Note that while we have chosen to count by discriminant, counting by other invariants is also of interest; see e.g. [ASVW21, ST22].

Let $\widetilde{K}$ be the Galois closure of $K/\mathbb{Q}$, that is the minimal field extension of K such that $\widetilde{K}/\mathbb{Q}$ is Galois. If f is a minimal polynomial for a primitive element of K, then the Galois group $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ acts transitively on the n roots of f.

Suppose G is a transitive permutation subgroup of the symmetric group S_n. We can also look to count extensions whose Galois closure has group isomorphic to G by studying

$$N_n(X, G) = \#\left\{K/\mathbb{Q} \mid [K:\mathbb{Q}] = n,\ |\mathrm{Disc}\, K/\mathbb{Q}| \leq X,\ \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G\right\}.$$

Conjecture 1.1.2 (folklore)**.** *Fix $n \geq 2$. Then we have $N_n(X, S_n) \sim C_n X$ for some constant C_n.*

Conjecture 1.1.2 is known to hold for $n \leq 5$. The $n = 2$ case is classical, with $C_2 = \frac{6}{\pi^2}$, which essentially follws from the computation of the density of squarefree integers and the classification of discriminants of quadratic fields. The $n = 3$ case is due to Davenport and Heilbronn [DH71], with improved error terms given by Bhargava, Shankar, and Tsimerman [BST13], while the $n = 4, 5$ cases are due to Bhargava [Bha05, Bha10].

For Galois groups $G \subseteq S_n$ more generally, *Malle's conjecture* and its various refinements provide predictions for the asymptotics of $N_n(X, G)$. For a more detailed summary of the conjecture and known special cases, see [Alb21].

For $N_n(X)$, relatively little is known for $n \geq 6$. The best currently known asymptotic upper bound takes the form

$$N_n(X) \ll X^{c(\log n)^2},$$

due to Lemke Oliver and Thorne [LT22], with improvements for $6 \leq n \leq 94$ given in [AGH+22, BSW22].

We can reinterpret the problem of counting number fields to counting those fields which are generated by algebraic points on the projective line, $\mathbb{P}^1$. Given some number field $K = \mathbb{Q}(\alpha)$, we can think of α as a geometric point on the $\mathbb{P}^1$, whose minimal field of definition is K. Suppose now that C is an algebraic curve defined over $\mathbb{Q}$ and define

$$N_{n,C}(X) = \#\left\{K/\mathbb{Q} \mid K = \mathbb{Q}(P),\ [K:\mathbb{Q}] = n,\ |\mathrm{Disc}\, K/\mathbb{Q}| \leq X\right\}$$

which counts fields which arise as the minimal field of definition for a degree n point $P \in C(\overline{\mathbb{Q}})$. We may similarly define $N_{n,C}(X, G)$ for a transitive subgroup $G \subseteq S_n$, and ask how these functions and their asymptotics depend on the geometry of the underlying curve C.

We present our main results in this direction below.

Theorem 1.1.3 (K.–Beneish)**.** *Let $m \geq 2$ and $C: y^m = f(x)$ be a superelliptic curve over $\mathbb{Q}$. Then for n sufficiently large and divisible by m, we have*

$$N_{n,C}(X) \gg X^{\delta_n}$$

for an explicit constant δ_n given explicitly in (3.5.1).

In the case when $m = 2$, i.e. C is a hyperelliptic curve, we can count fields with Galois group S_n.

Theorem 1.1.4 (K.)**.** *Let $C: y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$. Then for n sufficiently large and divisible by $\gcd(2, \deg f)$ we have*

$$N_{n,C}(X, S_n) \gg X^{\delta_n}.$$

The results in the hyperelliptic case appeared in [Key22], while the superelliptic case is joint with Lea Beneish [BK21a][1]. In Chapter 2 we give some more detailed background on Newton polygons and generating the symmetric group S_n. Then in Chapter 3, we prove Theorems 1.1.3 and 1.1.4, synthesizing the exposition in [Key22, BK21a] to give an account of the general strategy of counting polynomials and then adjusting for multiplicity. We also discuss geometric sources of higher degree points and prove the following.

Proposition 1.1.5 (K.–Beneish)**.** *Suppose m, d positive integers and q is an odd prime satisfying*

(i) $4 \mid m \mid d$,

(ii) $m \leq q$,

(iii) $n = 2q < \frac{d}{2} - 1$.

Then for a positive proportion of squarefree degree d polynomials f, ordered by height, the superelliptic curve $y^m = f(x)$ has finitely many points of degree n.

[1]The March 2021 preprint version contains errors, many of which are corrected in this dissertation.

1.2 Solubility for families of curves

Consider a collection of curves defined over $\mathbb{Q}$. Before making precise what we mean, we are motivated by the following question.

Question 1.2.1. *How often does a curve in this collection have a rational point?*

Note that throughout, one could more generally consider higher-dimensional varieties over fixed global field, but we content ourselves with curves over $\mathbb{Q}$.

Even for a fixed curve $C/\mathbb{Q}$, searching for rational solutions can prove challenging and time consuming. It is thus often useful to consider obstructions to the existence of rational points, the simplest of which are local obstructions.

The curve C is said to be locally soluble at a prime p if the set of p-adic points $C(\mathbb{Q}_p)$ is nonempty, and locally soluble at the infinite place if $C(\mathbb{R}) \neq \emptyset$. If C is locally soluble at all places, we say it is everywhere locally soluble. Since $\mathbb{Q}$ embeds into $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p, we have that everywhere local solubility is a necessary condition for C to have a rational point. Moreover, it is generally straightforward to determine whether or not C is everywhere locally soluble in finite time.

When everywhere local solubility is a sufficient condition, we say C satisfies the *Hasse principle*. The classical Hasse–Minkowski theorem implies that the Hasse principle holds when C has genus 0. However, this turns out not to be the case for higher genus curves.

To give only one example, and an answer to Question 1.2.1 for a specific case, consider hyperelliptic curves of the form

$$C_f \colon y^2 = f(x, z),$$

where here f is an integral binary form of degree $2g + 2$. Ordering by the height of their coefficients, we can ask about the natural density of polynomials f for which C_f has points everywhere locally, or rational points.

Poonen and Stoll showed that a positive proportion of hyperelliptics C_f are everywhere locally soluble [PS99b], with Bhargava, Cremona, and Fisher pinning this proportion down to about 76% in the $g = 1$ case [BCF21]. A landmark result of Bhargava, Gross, and Wang then states that a positive proportion of everywhere locally soluble hyperelliptic curves C_f

fail to have points of any odd degree [BGW17]. In particular, they lack rational points and thus fail the Hasse principle.

Motivated by these results, we consider the collection of superelliptic curves

$$C_f\colon y^m = f(x,z),$$

where $m \geq 2$ and f is an integral binary form of degree d divisible by m. As a first step to understanding how often such curves have (or lack) rational points or points of certain higher degrees, we study how often they are everywhere locally soluble.

Writing $f(x,z) = c_d x^d + \cdots + c_0 z^d$, we set

$$\rho_{m,d} = \lim_{B\to\infty} \frac{\#\left\{(c_0,\dots,c_d) \in (\mathbb{Z}\cap[-B,B])^{d+1} \mid C_f \text{ is everywhere locally soluble}\right\}}{(2B+1)^{d+1}},$$

if the limit exists. In joint work with Lea Beneish, appearing in [BK23] and reproduced in Chapter 4, we prove the following results.

Theorem 1.2.2 (Beneish–K.)**.** *Fix $(m,d) \neq (2,2)$. Then $\rho_{m,d}$ exists, $0 < \rho_{m,d} < 1$, and $\rho_{m,d}$ factors into a product of local densities,*

$$\rho_{m,d} = \rho_{m,d}(\infty)\prod_p \rho_{m,d}(p).$$

These local densities are made precise in (4.1.5) and (4.1.6). They may be thought of as the probability of C_f having a p-adic (resp. real) point. Thus Theorem 1.2.2 may be thought of as stating that these local probabilities look independent of one another. To deduce the result, we realize our family as coming from the fibers of a certain morphism of varieties and apply a result of Bright, Browning, and Loughran [BBL16, Theorem 1.4].

The utility of Theorem 1.2.2 is that the local factors may then be estimated, yielding estimates for $\rho_{m,d}$. This amounts to counting the residue classes of degree d forms f for which we can guarantee (or rule out) the existence of $\mathbb{F}_p$-points on the reduction $\overline{C_f}(\mathbb{F}_p)$ which lift to $\mathbb{Q}_p$-points on C_f.

With some effort, this approach can be used to give exact computations of the local

factors in certain cases.

Theorem 1.2.3 (Beneish–K.)**.** *For superelliptic curves $C_f = y^m = f(x,z)$ with $m = 3$ and $d = 6$, the exact value of $\rho_{3,6}$ is about 0.9694.*

More precisely, the local densities are given by one of two explicit rational functions when p is sufficiently large. We write $\rho_{3,6}(p) = R_i(p)$ where $p \equiv i \pmod 3$. The explicit formulae are given in (4.8.1), while the asymptotic behavior as $p \to \infty$ are described by

$$1 - R_1(t) \sim \frac{2}{3}t^{-4},$$
$$1 - R_2(t) \sim \frac{53}{144}t^{-7}.$$

For the eight primes $p = 2, 3, 7, 13, 19, 31, 37, 43$ for which $\rho_{3,6}(p)$ is not given by one of these rational functions, we are still able to compute $\rho_{3,6}(p)$ exactly, with the help of a computer, in order to give the exact value in Theorem 1.2.3.

1.3 Mertens' theorem

Let $\pi(x)$ denote the counting function of prime numbers $p \leq x$. The prime number theorem famously states

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1,$$

which we write as

$$\pi(x) \sim \frac{x}{\log x}.$$

As a consequence, the natural density of the primes is 0, but approaches it rather slowly at the rate $\frac{1}{\log x}$.

Suppose now, without knowing the prime number theorem, we were to try to estimate the density of the primes in the interval $(\sqrt{x}, x]$. An integer n in this range is prime if and only if it is not divisible by p for all primes $p \leq x$. The natural density of integers indivisible by all such p is given by the product

$$\prod_{p\leq\sqrt{x}} \left(1 - \frac{1}{p}\right),$$

so making the naïve assumption that this is the same as the density of primes in $(\sqrt{x}, x]$ (as x goes to infinity), one would guess that the asymptotic density of the primes is equal to the limit of the product above.

Enter a result of Mertens, proved before the prime number theorem was known [Mer74], which states that as $x \to \infty$ we have

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}.$$

Here γ denotes the Euler–Mascheroni constant.

Therefore using our naïve assumption above, we would obtain that the asymptotic prime density is $\frac{2e^{-\gamma}}{\log x}$. Note that $2e^{-\gamma} \approx 1.123$, so this differs from the true density of $\frac{1}{\log x}$ as given by the prime number theorem. Thus Mertens' theorem is capturing that for an integer $n \in (\sqrt{x}, x]$, failing to be divisible by distinct primes $p, p' \leq \sqrt{x}$ are not independent conditions.

Mertens theorem has since been extended in different directions. Almost a century later, Williams [Wil74] showed that for a coprime to b we have

$$\prod_{\substack{p \leq x \\ p \equiv a \pmod{b}}} \left(1 - \frac{1}{p}\right) \sim \left(\frac{e^{-\gamma(a,b)}}{\log x}\right)^{1/\varphi(b)},$$

where $\varphi(b)$ is Euler's totient function. The constant, which we denote by $e^{-\gamma(a,b)}$ to draw a parallel to the shape of Mertens' theorem, is described explicitly in Williams' paper.

For an extension of number fields $E/\mathbb{Q}$, Rosen [Ros99] gave a Mertens-type formula for prime ideals in the ring of integers $\mathcal{O}_E$ of bounded absolute norm $N(P)$,

$$\prod_{N(P) \leq x} \left(1 - \frac{1}{N(P)}\right) \sim \frac{e^{-\gamma_E}}{\log x}.$$

Here the generalized Euler constant γ_E is equal to $\gamma + \varkappa_E$, where $\varkappa_E$ is the residue of the Dedekind zeta function $\zeta_E(s)$ at $s = 1$.

In [APnKK22], joint with Santiago Arango-Piñeros and Daniel Keliher, we generalize to the setting of Chebotarev sets of primes in a Galois extension E/F of number fields,

unifying the results of both Williams and Rosen.

Theorem 1.3.1 (Arango-Piñeros–Keliher–K.). *Let E/F be a Galois extension of number fields with $G = \mathrm{Gal}(E/F)$. For a conjugacy class $C \subset G$, let $\mathcal{C}(x)$ denote the unramified primes P in $\mathcal{O}_F$ with Artin symbol $\mathrm{Frob}_P = \left(\frac{E/F}{P}\right) = C$ and bounded absolute norm $N(P) \leq x$. Then as $x \to \infty$ we have*

$$\prod_{P \in \mathcal{C}(x)} \left(1 - \frac{1}{N(P)}\right) \sim \left(\frac{e^{-\gamma(E/F,C)}}{\log x}\right)^{|C|/|G|}.$$

The proof, found in Chapter 5, follows a similar argument to that of Williams, using character orthogonality and several Euler products. Some additional care must be taken when G has representations of dimension greater than one.

We give explicit descriptions of the constants when E/F is quadratic, abelian, or an S_3 sextic, as well as an application to primes represented by quadratic forms, which we highlight here.

Corollary 1.3.2 (Arango-Piñeros–Keliher–K.). *Let Q be a primitive, irreducible, positive definite, integral binary quadratic form with discriminant D. Let E be the ring class field of the order of D. Denote by $\mathcal{Q}(x)$ the set of primes $p \leq x$ represented by Q. Then as $x \to \infty$ we have*

$$\prod_{P \in \mathcal{Q}(x)} \left(1 - \frac{1}{p}\right) \sim \left(\frac{e^{-\gamma(E/\mathbb{Q},C)}}{\log x}\right)^{\frac{|C|}{2h(D)}} \prod_{\substack{p \mid \Delta_E \\ p \in \mathcal{Q}}} \left(1 - \frac{1}{p}\right),$$

where $C \subset \mathrm{Gal}(E/\mathbb{Q})$ is the conjugacy class corresponding to $\mathcal{Q}$ via class field theory and $h(D)$ is the class number of forms of discriminant D.

Chapter 2

Preliminaries

2.1 Local fields and Newton polygons

2.1.1 Local fields

In this section, we briefly recall classical facts about local fields complete with respect to a discrete valuation. The prototypical examples are the p-adic fields $\mathbb{Q}_p$ and finite extensions thereof. We omit much explanation and most proofs, instead referring the reader to standard texts, e.g. [Lan94, Neu99, Gui18, Mil20], for the details.

Definition 2.1.1 (p-adic valuation)**.** For a nonzero integer n, the ***p*-adic valuation** of n is the largest positive integer k such that $p^k \mid n$.

This is naturally extended to a function $v_p \colon \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ by

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

and satisfies the usual properties of a discrete valuation (see e.g. [Neu99, §II.3]):

(i) $v_p(x) = \infty$ if and only if $x = 0$,

(ii) $v_p(xy) = v_p(x) + v_p(y)$ for all x, y, and

(iii) $v_p(x + y) \geq \min\left(v_p(x), v_p(y)\right)$ and equality holds if $v_p(x) \neq v_p(y)$.

Property (iii) above is known as the **nonarchimedean property**.

Definition 2.1.2 (p-adic absolute value)**.** The ***p*-adic absolute value**, denoted $|\cdot|_p$, is given by

$$|x|_p = p^{-v_p(x)}.$$

Here $|0|_p = 0$ by convention.

Definition 2.1.3 (p-adic field)**.** The ***p*-adic field** $\mathbb{Q}_p$ is constructed as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. That is, $\mathbb{Q}_p$ consists of sequences of rational numbers which are Cauchy with respect to $|\cdot|_p$, up to equivalence.

Definition 2.1.4 (p-adic numbers)**.** The ***p*-adic numbers** $\mathbb{Z}_p$ are defined to be the inverse limit

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

with the natural reduction maps $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ and their compositions.

These analytic and algebraic definitions coincide when we take the valuation ring.

Proposition 2.1.5. *The subring of $\mathbb{Q}_p$ with nonnegative valuation coincides with $\mathbb{Z}_p$.*

Moving forward, let K be a field, complete with respect to the absolute value given by a nonarchimedean discrete valuation v. We recall a number of basic facts.

Proposition 2.1.6 (See e.g. [Gui18, Proposition 2.17])**.** *With notation as above, we have the following basic facts, generalizing the case of $K = \mathbb{Q}_p$.*

(a) $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ *is a subring called the valuation ring of K.*

(b) $\mathcal{O}^\times = \{x \in \mathcal{O} \mid v(x) = 0\}$.

(c) $\mathfrak{m} = \{x \in \mathcal{O} \mid v(x) > 0\} \subset \mathcal{O}$ *is the unique maximal ideal of $\mathcal{O}$, i.e. $\mathcal{O}$ is a local ring.*

(d) $\mathfrak{m} = (\pi)$ *is a principal ideal. In fact, all ideals of $\mathcal{O}$ take the form (π^k).*

(e) $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ *is known as the residue field; Whenever $K/\mathbb{Q}_p$ is a finite extension, $\mathbb{F}$ is a finite field of characteristic p.*

Perhaps the most important result in the theory of local fields, and one that we will use later, is Hensel's lemma. It allows us to lift factorizations of polynomials, hence also their roots, from the residue $\mathbb{F}$ back to the valuation ring $\mathcal{O}$.

Theorem 2.1.7 (Hensel's lemma)**.** *With notation as above, let $f(t) \in \mathcal{O}[t]$ and denote by $\overline{f}(t)$ the image in $\mathbb{F}[t]$. Suppose in the residue field $\overline{f} \neq 0$ and we have a factorization*

$$\overline{f} = \overline{g}\overline{h} \in \mathbb{F}[t],$$

such that $\overline{g}, \overline{h}$ are relatively prime. Then there exist $g, h \in \mathcal{O}[t]$ with $\deg g = \deg \overline{g}$ such that

$$f = gh, \quad g \equiv \overline{g} \pmod{\mathfrak{m}}, \quad \text{and} \quad h \equiv \overline{h} \pmod{\mathfrak{m}}.$$

Proof. See e.g. [Neu99, II.4.6] or [Gui18, Theorem 2.21]. □

Corollary 2.1.8. *Let $f(t) \in \mathcal{O}[t]$ and suppose its reduction $\overline{f}(t)$ is nonzero with a root $\overline{\alpha}$ such that the derivative $\overline{f}'(\overline{\alpha}) \neq 0$. Then there exists $\alpha \in \mathcal{O}$ with*

$$f(\alpha) = 0 \quad \text{and} \quad \alpha \equiv \overline{\alpha} \pmod{m}.$$

Proof. The existence of a root implies $\overline{f} = (t - \overline{\alpha})\overline{h}$ for some $\overline{h} \in \mathbb{F}[t]$. Set $\overline{g} = t - \alpha$ with the coprimality of $\overline{g}, \overline{h}$ following from the fact that $\overline{f}'(\overline{\alpha}) \neq 0$. Now we apply Theorem 2.1.7 to lift to a linear polynomial $g = t - \alpha$ in the factorization of f. Since $g \equiv \overline{g} \pmod{\mathfrak{m}}$, we have $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{m}}$. □

A refinement of the proof of Theorem 2.1.7 gives a well known strengthening of Corollary 2.1.8.

Theorem 2.1.9. *Let $f(t) \in \mathcal{O}[t]$ and suppose there exists $\alpha_0 \in \mathcal{O}$ such that*

$$v(f(\alpha_0)) > 2v(f'(\alpha_0)).$$

Then the sequence

$$\alpha_i = \alpha_{i-1} - \frac{f(\alpha_{i-1})}{f'(\alpha_{i-1})}$$

for $i \geq 1$ converges to $\alpha \in \mathcal{O}$ with

$$f(\alpha) = 0 \quad \textit{and} \quad \alpha \equiv \alpha_0 \pmod{\mathfrak{m}}.$$

Proof. See e.g. [Lan94, §II.2, Proposition 2]. □

We now give several useful properties of extensions of local fields.

Proposition 2.1.10 ([Neu99, Theorem II.4.8])**.** *Let K be a field complete with respect to the discrete valuation v. If L/K is a finite extension, there is a unique extension of the valuation v to L, with respect to which L is complete.*

In light of Proposition 2.1.10, we abuse notation by also writing v for the valuation extended to L. Note that if v was normalized on K, i.e. $v(\pi) = 1$, then it need not be normalized on L; in fact, this will often fail to be the case.

Remark 2.1.11. Proposition 2.1.10 allows us to make sense of the valuations of the roots of a polynomial f over $\mathbb{Q}_p$, by uniquely extending v to a valuation on the splitting field of f over $\mathbb{Q}_p$.

2.1.2 Ramification

For the remainder of the section, let K, v be as above with p the characteristic of the residue field. Let L/K denote a finite extension with v extended to L by Proposition 2.1.10. We use subscripts to denote the valuation rings and residue fields of the respective fields.

Definition 2.1.12 (ramification index)**.** The **ramification index** of L/K is

$$e = e(L/K) = [v(L^\times) : v(K^\times)].$$

We say L/K is **unramified** if $e = 1$ and **totally ramified** if $e = [L : K]$. We say L/K is **tamely ramified** if $p \nmid e$ and **wildly ramified** otherwise.

Definition 2.1.13 (inertia degree)**.** Let L/K be a finite extension and $\mathbb{F}_L/\mathbb{F}_K$ the associ-

ated extension of residue fields. The **inertia degree** of L/K is

$$f = f(L/K) = [\mathbb{F}_L : \mathbb{F}_K].$$

Proposition 2.1.14 (fundamental identity, see e.g. [Neu99, Proposition II.6.8])**.** *Let L/K be a finite separable extension. Then $[L : K] = ef$, the product of the ramification index and inertia degree. If T/K is the maximal abelian subextension contained in L, this is visualized in the diagram below.*

$$\begin{array}{ccc} L & & \mathbb{F}_L \\ {\scriptstyle e}\big| & & \big| \\ T & & \mathbb{F}_T = \mathbb{F}_L \\ {\scriptstyle f}\big| & & {\scriptstyle f}\big| \\ K & & \mathbb{F}_K \end{array}$$

Proposition 2.1.15 (see e.g. [Neu99, Proposition II.9.9])**.** *Let L/K be a finite Galois extension. Then we have an exact sequence of finite groups*

$$0 \to I(L/K) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K) \to 0,$$

where $I(L/K) = \mathrm{Gal}(L/T)$ is the inertia subgroup.

Remark 2.1.16. The residue field $\mathbb{F}_K = \mathbb{F}_q$ is finite of order $q = p^k$, so $\mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$ is a cyclic group generated by the Frobenius automorphism $x \mapsto x^q$.

Remark 2.1.17. If L/K is unramified, then L/K is Galois and $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$, as each automorphism of the residue extension lifts to L/K.

Totally tamely ramified extensions are nicely characterized as radical extensions, with cyclic Galois group. This will come in handy later.

Lemma 2.1.18 (see e.g. [Sut, Theorem 11.8])**.** *Let L/K be a finite separable extension. L/K is totally tamely ramified, i.e. $p \nmid e = [L : K]$, if and only if*

$$L = K(\pi^{1/e})$$

for a uniformizer π of K.

Moreover, if L/K is finite Galois and totally tamely ramified, then $\mathrm{Gal}(L/K)$ *is cyclic.*

Proof. The characterization of tamely ramified extensions as radical extensions is useful in classifying finite extensions of local fields. For a proof of the first equivalence, see e.g. [Sut, Theorem 11.8].

The second statement follows from the fact that in the tamely ramified case, we have an injective group homomorphism $I(L/K) \to \mathbb{F}_L^\times$; see [Mil20, Corollary 7.59]. Since $\mathbb{F}_L^\times$ is cyclic and $I(L/K) = \mathrm{Gal}(L/K)$ by totally ramified, we are done. □

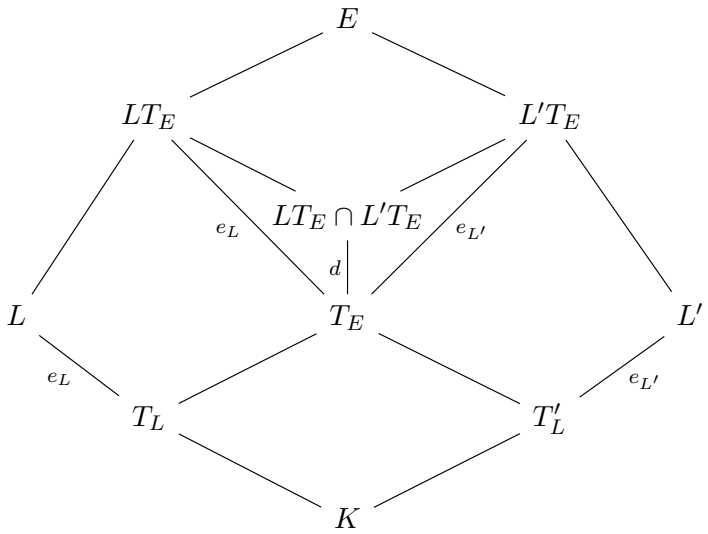
Note that if L/K is tamely ramified, but not necessarily totally ramified, we have a cyclic subgroup of order e, $\mathrm{Gal}(L/T) \subseteq \mathrm{Gal}(L/K)$, for the maximal unramified intermediate extension T/K.

We conclude with a few elementary intermediate results that will be useful to us later.

Lemma 2.1.19. *Let L/K, L'/K be finite extensions and set $E = LL'$ to be their compositum. The ramification index $e(E/K)$ divides the product of those of L and L',*

$$e(E/K) \mid e(L/K)e(L'/K).$$

Proof. For brevity, let $e_L, e_{L'}, e_E$ denote the ramification indices. Let T_L denote the maximal unramified extension of L/K, so $[L : T_L] = e_L$ (and similarly for L', E). Then we have the diagram below, with certain degrees marked.



Note that $L \cap T_E = T_L$, since L/T_L is totally ramified and T_E/T_L is unramified (and similarly for L').

From the diagram, we now see that the degree d divides both e_L and $e_{L'}$, hence $d \mid \gcd(e_L, e_{L'})$. Moreover,

$$e_E = d[E : LT_E \cap L'T_E] = d \cdot \frac{e_L}{d}\frac{e_{L'}}{d} = \frac{e_L e_{L'}}{d}.$$

This completes the proof. □

Remark 2.1.20. The proof of Lemma 2.1.19 shows that if e_L and $e_{L'}$ are coprime, then $d = 1$. In this case the ramification index is multiplicative, $e(E/K) = e(L/K)e(L'/K)$.

Similar techniques reveal that if $\gcd(e_L, e_{L'}) = 1$ then $L \cap L'$ is unramified and equal to $T_L \cap T_{L'}$.

Lemma 2.1.21. *Let L/K, L'/K be finite extensions and set $E = LL'$ to be their compositum. Set T_E/K to be the maximal unramified subextension of E/K. If the ramification indices $e(L/K)$ and $e(L'/K)$ are coprime, then*

$$LT_E \cap L'T_E = T_E.$$

Moreover, if L, L', E are Galois over K, this implies that we have identifications

$$\mathrm{Gal}(L/T_L) \simeq \mathrm{Gal}(LT_E/T_E) \simeq \mathrm{Gal}(E/L'T_E).$$

Proof. We have that $L \cap T_E = T_L$, since any subextension of T_E is unramified over K, so $L \cap T_E$ is unramified and thus contained in T_L. This and the identical argument for L' implies

$$[LT_E : T_E] = [L : T_L] = e_L, \quad [L'T_E : T_E] = [L' : T_{L'}] = e_{L'}.$$

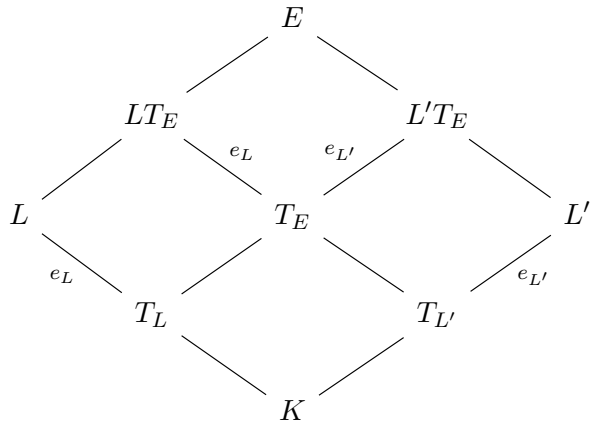
If L is Galois (T_L is unramified and thus Galois) then from standard Galois theory we have

$$\mathrm{Gal}(LT_E/T_L) = \mathrm{Gal}(LT_E/L \cap T_E) \simeq \mathrm{Gal}(L/T_L) \times \mathrm{Gal}(T_E/T_L).$$

In particular, we make the identification

$$\mathrm{Gal}(L/T_L) \simeq \mathrm{Gal}(LT_E/T_E).$$

By a similar argument for the L' side, we produce the diagram below.



By the hypothesis that $\gcd(e_L, e_{L'}) = 1$, we find $LT_E \cap L'T_E = T_E$. Repeating our previous argument, we have $\mathrm{Gal}(LT_E/T_E) \simeq \mathrm{Gal}(E/L'T_E)$ as desired. □

2.1.3 Newton polygons

We now recall the theory of Newton polygons of polynomials; see [Neu99, §II.6] for more.

Definition 2.1.22 (Newton polygon)**.** Let $f(t) = \sum_{i=0}^{d} a_i t^i \in \mathbb{Q}_p[t]$ be a polynomial. The ***p*-adic Newton polygon of *f*** is the lower convex hull in $\mathbb{R}^2$ of the points $(i, v(a_i))$ for $0 \leq i \leq d$,

$$\mathrm{NP}_{\mathbb{Q}_p}(f) = \mathrm{conv}\left\{(i, v(a_i)) \mid 0 \leq i \leq d\right\}.$$

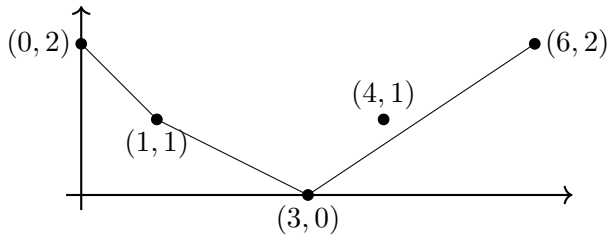
Note that we assume $a_0 a_d \neq 0$ and interpret $a_i = 0$ and the corresponding point (i, ∞) as having no contribution. When the prime p is understood, we will simply refer to this as the **Newton polygon** of f, denoted $\mathrm{NP}(f)$.

Example 2.1.23. Consider the sextic polynomial

$$f(t) = p^2 t^6 + pt^4 + t^3 + pt + p^2.$$

The points $(i, v(a_i))$ and Newton polygon $\mathrm{NP}(f)$ are drawn below.

Figure 2.1.1: An example Newton polygon for a sextic polynomial



The Newton polygon $\mathrm{NP}(f)$ encodes information about the valuations of the roots of f. Note that the valuation of a root is well defined in this context by Proposition 2.1.10; see Remark 2.1.11. To make this precise, we define the notion of a segment of $\mathrm{NP}(f)$.

Definition 2.1.24 (segment)**.** Let $f(t) = \sum_{i=0}^{d} a_i t^i \in \mathbb{Q}_p[t]$ be a polynomial and assume $a_0 a_d \neq 0$. A Newton polygon is a finite union of line segments, each with distinct slope, referred to as a **segment** of $\mathrm{NP}(f)$.

A segment with endpoints $(i, v(a_i))$ and $(j, v(a_j))$ is said to have **length** $\ell = j - i$.

We will call a segment **reduced** if it passes through no lattice points other than its endpoints. Equivalently, its length ℓ is coprime to $v(a_j) - v(a_i)$.

Theorem 2.1.25 (Fundamental theorem of Newton polygons)**.** *Suppose* $\mathrm{NP}(f)$ *has a segment of length* ℓ *and slope* s*. Then* f *has precisely* ℓ *roots of valuation* $-s$*.*

Proof. See [Neu99, Proposition II.6.3]. □

An immediate consequence is that Newton polygons have the potential to reveal information about the factorization of f over $\mathbb{Q}_p$.

Lemma 2.1.26. *Suppose* $\mathrm{NP}(f)$ *has a segment of length* ℓ *and slope* s*. Then* f *factors as* $f = f_0 f_1$ *over* $\mathbb{Q}_p$*, such that* $\deg f_0 = \ell$ *and the roots of* f_0 *have valuation* $-s$*.*

Moreover, if $s = r/\ell$ *has reduced fraction form* r'/ℓ' *then all irreducible factors of* f_0 *over* $\mathbb{Q}_p$ *have degree divisible by* ℓ'*.*

In particular, if the segment is reduced, then the f_0 *produced above is irreducible over* $\mathbb{Q}_p$*.*

Proof. The action of the Galois group $\mathrm{Gal}(f/\mathbb{Q}_p)$ on the roots of f preserves their valuations. To see why, suppose $\sigma \in \mathrm{Gal}(f/\mathbb{Q}_p)$ is an automorphism of the splitting field $E = \mathrm{Spl}_{\mathbb{Q}_p} f$. We have that v extends uniquely to a valuation of E, and one can check that $v \circ \sigma$ is another valuation of E, so by the uniqueness [Neu99, Theorem II.6.2] of the lift of v to E, we have that Galois conjugates of a root have the same valuation.

Thus for an irreducible polynomial over $\mathbb{Q}_p$, all roots must have the same valuation since they are Galois conjugate to one another. Therefore, we can decompose f into irreducible factors and group together those whose roots have valuation $-s$ into f_0. This must have degree ℓ, since f has exactly ℓ roots with valuation $-s$ by Theorem 2.1.25.

For the second statement, we use the same observation above to recognize that the Newton polygon of an irreducible polynomial has exactly one segment. Let g be an irreducible polynomial over $\mathbb{Q}_p$ dividing f_0. Then $\mathrm{NP}(g)$ has one segment of slope $s = r_g/\deg g$. Since reducing this fraction also produces r'/ℓ', we must have $\ell' \mid \deg g$. □

We caution that while the p-adic Newton polygon of a polynomial reveals some information about its factorization over $\mathbb{Q}_p$, it need not determine it exactly, as in the following example.

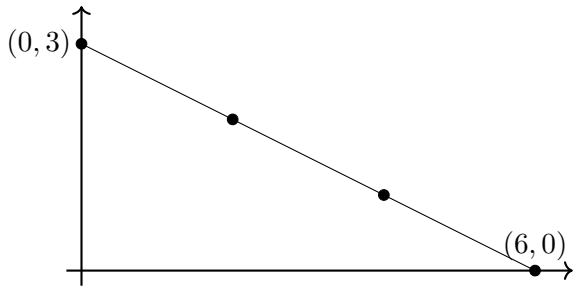
Example 2.1.27. Suppose $p > 2$ for convenience and let f denote the monic minimal polynomial over $\mathbb{Q}_p$ of $\alpha = p^{1/2} + p^{2/3}$. We compute $\deg f = 6$ by considering all possible conjugates of α.

On the other hand, suppose g is the product of the monic minimal polynomials of $\beta = p^{1/2}$ and $\gamma = p^{1/2} + p^{3/4}$, giving the factorization

$$g(t) = (t^2 - p)(t^4 - 2pt^2 + p^2 - p^3).$$

Note that $v(\alpha) = v(\beta) = v(\gamma) = 1/2$, so f and g have identical Newton polygons by Theorem 2.1.25, shown below. This illustrates a limitation of Lemma 2.1.26; if we knew only that a polynomial had the Newton polygon above, we could conclude that its irreducible factors must all have even degree, but this is not enough to decide whether or not it is irreducible.

Figure 2.1.2: Newton polygon for f and g



In certain cases, the Newton polygon may be used to deduce the cycle structure of the Galois group $\mathrm{Gal}(f/\mathbb{Q}_p)$ acting on the roots of f.

Proposition 2.1.28. *Suppose* $\mathrm{NP}(f)$ *has a reduced segment of length* ℓ*, i.e. a segment of slope* $s = r/\ell$ *with* $\gcd(r, \ell) = 1$*. By Lemma 2.1.26, f has an irreducible factor f_0 such that the roots of f with valuation $-s$ are precisely the roots of f_0.*

Suppose $p > \deg f$ *and that all other irreducible factors of f have degree coprime to* $\deg f_0 = \ell$*. Then* $\mathrm{Gal}(f/\mathbb{Q}_p)$ *contains an ℓ-cycle permuting the roots of f_0.*

Proof. We begin by factoring $f = f_0 f_1$. Let E, E_0, E_1 denote the splitting fields over $\mathbb{Q}_p$ of f, f_0, f_1 respectively, obtained by adjoining roots. Let T, T_0, T_1 denote the maximal unramified subextensions of E, E_0, E_1 over $\mathbb{Q}_p$.

Our goal is to find an ℓ-cycle in $\mathrm{Gal}(E_0/T_0)$ then make identifications

$$\mathrm{Gal}(E_0/T_0) \simeq \mathrm{Gal}(E_0T_0T_1/T_0T_1) \simeq \mathrm{Gal}(E/E_1T_0T_1) \subseteq \mathrm{Gal}(E/\mathbb{Q}_p). \tag{2.1.1}$$

Interpreting this ℓ-cycle as permuting the roots of f in E, that it fixes $E_1T_0T_1$ implies that it fixes the roots of f_1, giving the result.

Let $L = \mathbb{Q}_p[t]/(f_0(t))$ be a degree ℓ extension of $\mathbb{Q}_p$ obtained by adjoining a root of f_0. Since roots of f_0 have valuation r/ℓ, we have $\frac{r}{\ell} \in v(L^\times)$ (here we abuse notation by writing v for the unique extension of v_p to L). By the reducedness hypothesis, $\frac{1}{\ell}\mathbb{Z} \subseteq v(L^\times)$ or equivalently the ramification index of L is divisible by ℓ. Since $[L : \mathbb{Q}_p] = \ell$, we have that L is in fact totally ramified, and tamely ramified since $p \nmid \ell$.

By Lemma 2.1.18, $L = \mathbb{Q}_p(\pi^{1/\ell})$ for a uniformizer π of $\mathbb{Q}_p$. The Galois closure of L

is E_0, which we identify with $\mathbb{Q}_p(\pi^{1/\ell}, \zeta)$ for a primitive ℓ-th root of unity, ζ. Thus we find an element of order ℓ in $\mathrm{Gal}(E_0/T_0)$, coming from the root of unity, which necessarily permutes the roots of f_0 in a cyclic fashion. The first identification in (2.1.1) then follows from elementary Galois theory, since $E_0 \cap T_0T_1 = T_0$.

For the second identification, suppose $f_1 = \prod g_i$ is the irreducible factorization over $\mathbb{Q}_p$, with the degrees $\deg g_i$ coprime to ℓ by hypothesis. Denote by $E_{g_i}, T_{g_i}, e_{g_i}$ the splitting field of each g_i over $\mathbb{Q}_p$, its maximal unramified subextension, and the ramification index $[E_{g_i} : T_{g_i}]$. Arguing as above, we see that $e_{g_i} \mid \deg g_i$.

Note that E_1 is the compositum of the E_{g_i}. By Lemma 2.1.19 we have

$$[E_1T_0T_1 : T_0T_1] = [E_1 : T_1] = e(E_1/\mathbb{Q}_p) \,\Big|\, \prod e_{g_i} \,\Big|\, \prod \deg g_i,$$

which is again coprime to ℓ by our hypothesis. Thus $E_0T_0T_1 \cap E_1T_0T_1 = T_0T_1$, and elementary Galois theory again provides the second identification of (2.1.1), since $E = E_0E_1T_0T_1$.

To conclude, we recognize that lifting our ℓ-cycle from $\mathrm{Gal}(E_0/T_0)$ a priori only produces an element of order ℓ in $\mathrm{Gal}(E/E_1T_0T_1) \subseteq \mathrm{Gal}(f/\mathbb{Q}_p)$. However, it fixes E_1, i.e. the roots of f_1, and cyclically permutes those of f_0, as seen by its restriction to E_0. □

Remark 2.1.29. Again, we may not necessarily be able to read off enough factorization information from $\mathrm{NP}(f)$ directly to satisfy the hypotheses of Proposition 2.1.28; recall Example 2.1.27. In some cases though, we can; see Examples 2.1.30 and 2.1.33 below.

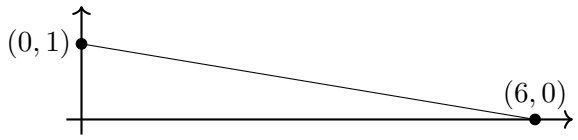
Example 2.1.30. Let $p \neq 2, 3$. Consider the sextic polynomial

$$f(t) = t^6 - p.$$

with Newton polygon $\mathrm{NP}(f)$ drawn below. This polygon has one reduced segment, so Lemma 2.1.26 reveals that f is irreducible. Moreover, by Proposition 2.1.28 $\mathrm{Gal}(f/\mathbb{Q}_p)$ contains a 6-cycle.

This is not terribly surprising considering that the splitting field of f is $\mathbb{Q}_p(p^{1/6}, \zeta)$, where ζ is a primitive 6-th root of unity. We see that the map $p^{1/6} \mapsto \zeta p^{1/6}$ extends to an automorphism of order 6 of $\mathbb{Q}_p(p^{1/6}, \zeta)/\mathbb{Q}_p(\zeta)$.

Figure 2.1.3: p-adic Newton polygon for $f = t^6 - p$



Remark 2.1.31. Those familiar with tropical geometry may recognize the Newton polygon, though we point out that it differs from the Newton polytope as defined in [MS15, Definition 2.3.4]. What we call the Newton polygon is in fact the lower faces of the Newton polytope when lifted to $\mathbb{R}^2$ using the valuations of the coefficients. We will not make use of this perspective, but if you are interested you may find some wisdom in studying [MS15, Proposition 3.1.6].

Remark 2.1.32. Suppose $f(t) \in \mathbb{Q}[t]$ is a separable polynomial of degree n. A well used strategy to show irreducibility is to argue over $\mathbb{Q}_p$. We can do the same with Galois groups. The embedding $\mathbb{Q} \to \mathbb{Q}_p$ induces a natural inclusion $\mathrm{Gal}(f/\mathbb{Q}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q})$ as permutation subgroups of the symmetric group S_n acting on the n roots of f.

This suggests the following strategy to show $\mathrm{Gal}(f/\mathbb{Q}) = S_n$: for different primes p, compute the Newton polygon $\mathrm{NP}_{\mathbb{Q}_p}(f)$ and use Proposition 2.1.28 to produce cycles in $\mathrm{Gal}(f/\mathbb{Q})$. Then, argue that these elements suffice to generate the full symmetric group S_n. We will adopt this strategy in Chapter 3 to show that many degree n points on hyperelliptic curves are defined over S_n-fields.

Example 2.1.33. Returning to the sextic polynomial f defined in Example 2.1.23,

$$f(t) = p^2t^6 + pt^4 + t^3 + pt + p^2.$$

Lemma 2.1.26 reveals that f has irreducible factors of degrees 1, 2, and 3 over $\mathbb{Q}_p$, each of which has roots of valuation 1, $1/2$, and $-2/3$, respectively.

Proposition 2.1.28 shows that $\mathrm{Gal}(f/\mathbb{Q}_p)$ contains a 3-cycle and 2-cycle, each of which cyclically permutes the roots of one irreducible factor while fixing the others.

Example 2.1.34. Taking the previous example a step further and illustrating the strategy

outlined in Remark 2.1.32, suppose we have

$$f(t) = p^2qt^6 + pqt^4 + q^2t^3 + pt + p^2$$

for a prime q distinct from p.

The q-adic Newton polygon has a reduced segment of length 5, therefore by Lemma 2.1.26, f has irreducible factors of degrees 5 and 1 over $\mathbb{Q}_q$, and by Lemma 2.1.21, there is a 5-cycle in $\mathrm{Gal}(f/\mathbb{Q}_q) \subseteq \mathrm{Gal}(f/\mathbb{Q})$.

By the rational root theorem, any rational roots lie in the set

$$\left\{\pm 1, \pm p, \pm p^2, \pm\frac{1}{q}, \pm\frac{p}{q}, \pm\frac{p^2}{q}\right\}.$$

A straightforward computation confirms none of these are roots of f, so f has no linear factors. Thus f is irreducible over $\mathbb{Q}$, in light of its factorization over $\mathbb{Q}_q$, and $\mathrm{Gal}(f/\mathbb{Q}) \subseteq S_6$ is a transitive subgroup. The presence of a transposition and a 5-cycle suffices to give equality; this will be proven shortly in Proposition 2.2.18.

While neither the p-adic nor q-adic information alone was enough to conclude f is irreducible over $\mathbb{Q}$ or deduce its Galois group, combining the local information at these places was sufficient.

2.2 Generating symmetric groups

In this section we collect some facts about permutation groups. In particular, we study generating sets of the symmetric group.

Definition 2.2.1 (S_n)**.** The **symmetric group on n letters**, denoted S_n, is defined to be the collection of permutations of the set $\{1, \ldots, n\}$. Equivalently, it is the group of automorphisms of $\{1, \ldots, n\}$ in the category of sets (i.e. bijections).

Definition 2.2.2 (permutation group)**.** A subgroup G of the symmetric group S_n is known as a **permutation group**.

2.2.1 Cycle notation

To describe elements of permutation groups compactly, we use cycle notation; see e.g. [DF04, §1.3]. As a first example, we denote by $\sigma = (1\ 2\ \ldots\ \ell)$ the permutation that sends

$$\sigma(x) = \begin{cases} x+1 & 1 \leq x < \ell, \\ 1 & x = \ell. \end{cases}$$

We generalize this as follows.

Definition 2.2.3 (cycle)**.** Let $\ell \leq n$. We denote by $\sigma = (a_1\ \ldots\ a_\ell)$ the cyclic permutation

$$\sigma(x) = \begin{cases} a_{i+1} & x = a_i \text{ for } 1 \leq i < \ell, \\ a_1 & x = a_\ell, \\ x & x \neq a_i \text{ for } 1 \leq i \leq \ell. \end{cases}$$

Such a σ is known as an **ℓ-cycle**.

Definition 2.2.4 (disjointness)**.** Two cycles $\sigma = (a_1\ \ldots\ a_\ell)$, $\sigma' = (a'_1\ \ldots\ a'_{\ell'}) \in S_n$ are said to be **disjoint** if

$$\{a_1, \ldots, a_\ell\} \cap \{a'_1, \ldots, a'_{\ell'}\} = \emptyset.$$

That is, there is no element $x \in \{1, \ldots, n\}$ on which both σ and σ' act nontrivially. This can be extended to larger collections of cycles.

One can check that disjoint cycles commute with one another; in the definition above, we have $\sigma\sigma' = \sigma'\sigma$.

Proposition 2.2.5 (cycle decomposition)**.** *Every permutation has a unique decomposition as a product of disjoint cycles (up to reordering of the factors).*

Proof. This is a straightforward exercise. See e.g. [DF04, §1.3]. □

An important fact that we will make use of is that conjugation in permutation groups corresponds to renumbering.

Proposition 2.2.6. *Let $\sigma = (a_1 \ \dots \ a_\ell) \in S_n$ be an ℓ-cycle and $\rho \in S_n$ any permutation. Then conjugating σ by ρ produces the ℓ-cycle*

$$\rho\sigma\rho^{-1} = (\rho(a_1) \ \dots \ \rho(a_\ell)).$$

Proof. We need only check what $\rho\sigma\rho^{-1}$ does to elements $\{1, \dots, n\}$. Consider the action on $\rho(a_i)$ for $1 \leq i < \ell$. We have

$$(\rho\sigma\rho^{-1}) \cdot \rho(a_i) = \rho(a_1 \ \dots \ a_\ell) \cdot a_i = \rho \cdot a_{i+1} = \rho(a_{i+1}) = (\rho(a_1) \ \dots \ \rho(a_\ell)) \cdot \rho(a_i).$$

Similarly, $(\rho\sigma\rho^{-1}) \cdot \rho(a_\ell) = \rho(a_1)$, as desired. Finally, if $x \neq \rho(a_i)$ for any i, we have that $\rho^{-1}(x) \neq a_i$ for any i, so

$$(\rho\sigma\rho^{-1}) \cdot x = \rho \cdot \rho^{-1}(x) = x,$$

and $\rho\sigma\rho^{-1}$ acts trivially outside of $\{\rho(a_i)\}$, and we are done. □

Corollary 2.2.7. *Suppose $\sigma_i = (a_{i1} \ \dots \ a_{i\ell_i}) \in S_n$ is a collection of ℓ_i-cycles for $1 \leq i \leq k$. Let $\rho \in S_n$ be any permutation. Then*

$$\rho\sigma_1 \cdots \sigma_k\rho^{-1} = (\rho(a_{11}) \ \dots \ \rho(a_{1\ell_1})) \cdots (\rho(a_{k1}) \ \dots \ \rho(a_{k\ell_k})).$$

Thus the conjugate of a product of cycles is itself a product of cycles of the same lengths, suitably renumbered.

Proof. Inserting copies of $\rho^{-1}\rho$, we have

$$\rho\sigma_1 \cdots \sigma_k\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1}) \cdots (\rho\sigma_k\rho^{-1}).$$

Then apply Proposition 2.2.6. □

Definition 2.2.8. If $\sigma_1, \dots, \sigma_k$ are disjoint cycles and σ_i has length ℓ_i, then we say the product $\sigma_1\sigma_2 \cdots \sigma_k$ has **cycle type** $(\ell_1, \ell_2, \dots, \ell_k)$, or is an $(\ell_1, \ell_2, \dots, \ell_k)$**-cycle**.

Remark 2.2.9. Corollary 2.2.7 implies that cycle type is a conjugacy class invariant. In fact, the conjugacy classes in S_n are precisely the cycle types. This can be seen by first

proving all ℓ-cycles are conjugate to $(1\ \dots\ \ell)$. Then one just has to conjugate each cyclic factor in the decomposition appropriately to some chosen ℓ_i-cycle, disjoint from the others.

We now pose the central question of this section.

Question 2.2.10. *How can we tell if $G = S_n$? What combination of properties or known elements or cycle types in G imply that it must be the full symmetric group?*

Depending on the setting from which our subgroup G arises, certain conditions may be easier than others to satisfy, if we want to prove $G = S_n$.

2.2.2 Generating sets of transpositions

Definition 2.2.11 (transposition)**.** A 2-cycle $(a\ b) \in S_n$ is also known as a **transposition**, since it transposes a and b.

Lemma 2.2.12. *An ℓ-cycle σ may be written as the product of $\ell - 1$ transpositions.*

Proof. By Corollary 2.2.7, it suffices to prove the statement for $\sigma = (1\ \dots\ \ell)$. We claim that

$$(1\ \dots\ \ell) = (2\ 3)\cdots(\ell - 1\ \ell)(1\ \ell),$$

which may be verified by direct computation. Counting the transpositions on the right, there are $\ell - 2$ of the form $(i\ i+1)$ for $2 \leq i \leq \ell - 1$, along with the rightmost factor $(1\ \ell)$. □

Proposition 2.2.13. *The set of all transpositions generates the symmetric group,*

$$\langle \{(a\ b) \mid 1 \leq a < b \leq n\} \rangle = S_n.$$

Proof. Every permutation has a unique cycle decomposition by Proposition 2.2.5. Lemma 2.2.12 states that each cyclic factor can be written as the product of transpositions. Hence a permutation is the product of transpositions. □

Remark 2.2.14. We note here that the factorization in Lemma 2.2.12 is not unique, and neither is a transposition decomposition for a general permutation. It does however have

unique parity, i.e. for a given $\phi \in S_n$, either all way of writing ϕ as a product of transpositions use an even number of them, or all of them use an odd number.

More careful study of this phenomenon leads to the alternating group, A_n, the normal subgroup of S_n consisting of permutations that can be written as the product of an even number of transpositions. In fact, A_n is generated by the 3-cycles, in analogy to Proposition 2.2.13. The proof follows from showing that any pair of distinct transpositions may be written as the product of 3-cycles:

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(a\ d) = (a\ c\ b)(a\ c\ d).$$

Note that we may assume above that all entries are distinct, except possibly $b = d$.

Notice that the generating set in Proposition 2.2.13 contains $\binom{n}{2} = \frac{n(n+1)}{2}$ transpositions. Can we make do with fewer? The answer turns out to be yes.

Proposition 2.2.15. *The sets of $n-1$ transpositions*

$$T_1 = \{(i\ i+1) \mid 1 \leq i \leq n-1\}$$
$$T_2 = \{(1\ i) \mid 2 \leq i \leq n\}$$

are both generating sets for S_n.

Proof. By Proposition 2.2.13, it suffices to show that these transpositions are enough to generate all transpositions. Given $1 \leq a < b \leq n$, let's consider the transposition $(a\ b)$ and proceed by induction on $b - a$ to show T_1 is a generating set.

If $b-a = 1$ then $b = a+1$ and $(a\ a+1)$ is already in our generating set. If not, then our inductive hypothesis is that $(a\ b-1)$ is generated by the transpositions of the form $(i\ i+1)$. Then we have

$$(a\ b) = (a\ b-1)(b-1\ b)(a\ b-1)$$

and $(a\ b)$ is also generated by transpositions of the form $(i\ i+1)$.

For T_2, we directly compute

$$(a\ b) = (1\ a)(1\ b)(1\ a)$$

for any distinct $a, b \neq 1$. □

2.2.3 Transitive subgroups

Definition 2.2.16 (transitive)**.** A permutation subgroup $G \subseteq S_n$ is **transitive** if for all $a, b \in \{1, \ldots, n\}$ there exists a permutation $\rho \in G$ such that $\rho(a) = b$.

This definition can be extended to any group G acting on a set S. The action is said to be **transitive** if for all $s, t \in S$ there exists $g \in G$ such that $g \cdot s = t$.

Many familiar groups are transitive; The symmetric group S_n, alternating group A_n, dihedral group D_n, and cyclic group C_n all act transitively on $\{1, \ldots, n\}$. Note that we are using the usual action here; the isomorphism class of G alone does not in fact tell us if its action is transitive or not, as in the following example.

Example 2.2.17. The group $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has a natural action on $\{1, 2, 3, 4\}$ when we identify

$$V_4 \simeq \langle (1\ 2), (3\ 4) \rangle \subset S_4.$$

Under this isomorphism, there is no element which sends $1 \mapsto 3$, for instance, so the action by V_4 is not transitive.

However, consider another permutation group, which is also isomorphic to V_4 as an abstract group:

$$V_4 \simeq \langle (1\ 3)(2\ 4), (1\ 4)(2\ 3) \rangle.$$

The isomorphism is given by

$$(1, 0) \mapsto (1\ 3)(2\ 4),$$

$$(0, 1) \mapsto (1\ 4)(2\ 3),$$

$$(1, 1) \mapsto (1\ 2)(3\ 4).$$

The action of this group on $\{1, 2, 3, 4\}$ is transitive; for example, 1 is sent to 2, 3, and 4 by (the images of) $(1, 1)$, $(1, 0)$, and $(0, 1)$ respectively.

If we know that a subgroup $G \subseteq S_n$ is transitive, we can get away with very small generating sets. In the following, assume $n \geq 3$ since the $n = 1, 2$ cases are trivial.

Proposition 2.2.18. *Let $G \subseteq S_n$ be a transitive subgroup containing an $(n-1)$-cycle and a transposition. Then $G = S_n$.*

Proof. Choose a numbering on $\{1, \ldots, n\}$ such that the $(n-1)$-cycle is written $\sigma = (1\ 2\ \ldots\ n-1)$. The transposition is of the form $\tau = (a\ b)$. By transitivity, there exists $\rho \in G$ such that $\rho(b) = n$, so we have

$$\tau' = \rho\tau\rho^{-1} = (\rho(a)\ n) \in G$$

by Proposition 2.2.6.

In particular, $\rho(a) \neq n$, so we have

$$\sigma = \left(\rho(a)\ \sigma(\rho(a))\ \ldots\ \sigma^{n-2}(\rho(a))\right).$$

After renumbering only $\{1, \ldots, n-1\}$, we can assume $\tau' = (1\ n)$ and $\sigma = (1\ 2\ \ldots\ n-1)$. Conjugating τ by σ^k for $k \leq n-2$ we have

$$\sigma^k\tau\sigma^{-k} = (k+1\ n) \in G.$$

This is a relabeling of the generating set T_2 from Proposition 2.2.15, hence $G = S_n$. □

Proposition 2.2.19. *Let $G \subseteq S_n$ be a transitive subgroup containing a p-cycle for some prime $p > n/2$ and a transposition. Then $G = S_n$.*

Proof. When $n = 3$, this is trivial, so assume $n \geq 4$, which implies $p > 2$. Let our p-cycle be of the form $\sigma = (1\ \ldots\ p)$. By transitivity, we may assume that the transposition acts nontrivially on 1, i.e. is given by $\tau = (1\ a)$ for some a. By Proposition 2.2.15, it suffices to see we have transpositions $(1\ x) \in G$ for all $2 \leq x \leq n$.

If $a \leq p$ then since $p = 2$, some power σ^k for $k < p$ puts a adjacent to 1. The primality of p ensures σ^k is still a p-cycle. All of this allows us to assume $a = 2$ for convenience, in which case

$$H = \langle \sigma, \tau \rangle \simeq S_p$$

with the action restricted to $\{1, \ldots, p\}$. We see this by conjugating τ by σ repeatedly to generate transpositions and appealing to the generating set T_1 from Proposition 2.2.15.

If instead $a > p$, then we set $H = \langle \sigma, \tau \rangle$, viewed as a permutation group on $\{1, \ldots, p, a\}$ and use Proposition 2.2.18 to see that $H \simeq S_{p+1}$.

In either case, we have a permutation subgroup $H \subseteq G$ containing *at least* the $p - 1$ transpositions of the form $(1\ b)$, where $b \leq p$. Let $x > p$ and use the transitivity of G to find $\rho \in G$ such that $\rho(1) = x$. Then for each b we have

$$\rho(1\ b)\rho^{-1} = (x\ \rho(b)) \in G.$$

Since $p - 1 > n - p - 1$, by the pigeonhole principle we have that for at least one b we have $\rho(b) \leq p$, which implies for this such b that

$$(1\ \rho(b))(x\ \rho(b))(1\ \rho(b)) = (1\ x) \in G.$$

Hence by Proposition 2.2.15, we are done. □

We conclude this section with examples that illustrate how things can go wrong if the hypotheses of the various propositions are not met.

Example 2.2.20. Suppose $G \subseteq S_n$ contains the n-cycle $\sigma = (1\ \ldots\ n)$ and a transposition. Note that this implies G is transitive. Suppose further that n is even and the transposition takes the form $\tau = (1\ a)$ for an odd number a. Then G is *not* necessarily the full symmetric group S_n.

For concreteness, we can take

$$G = \langle (1\ 3), (1\ 2\ 3\ 4) \rangle \subset S_4,$$

which we recognize as the dihedral group D_4. In any case, explicit computation shows that e.g. $(1\ 2) \notin G$, so $G \neq S_n$.

Note that if either of n or $a-1$ is odd, then $G = \langle \sigma, \tau \rangle = S_n$.

Remark 2.2.21. Let n be an even integer and consider the wreath product $G = S_2 \wr S_{n/2} \subset S_n$. We can realize G as two copies of $S_{n/2}$ acting on $\{1, \ldots, n/2\}$ and $\{n/2+1, \ldots, n\}$, respectively, along with an element τ of order two which swaps a with $a + n/2$ for all $1 \leq a \leq n/2$. This group is not equal to S_n, but contains $n/2$-cycles (in fact it contains k-cycles for all $k \leq n/2$), showing that Proposition 2.2.19 is sharp.

G also contains an n-cycle, constructed as follows. Let $\sigma = (1\ \ldots\ n/2)$ and τ as defined above. Then

$$\sigma\tau = \left(1\ (\frac{n}{2}+1)\ 2\ (\frac{n}{2}+2)\ \ldots\ \frac{n}{2}\ n\right)$$

is an n-cycle. Note that elements of $\{1, \ldots, n/2\}$ (respectively $\{n/2+2, \ldots, n\}$) are separated by an even number of entries.

If a permutation group H contained $G = S_2 \wr S_{n/2}$, as well as a transposition swapping elements across the two $S_{n/2}$ factors, then H would in fact be the full symmetric group.

To explore this further, we begin by generalizing an idea in the proof of Proposition 2.2.19, when we used the fact that a subgroup $H \subseteq G$ such that $H \simeq S_p$ or S_{p+1} to argue that $G = S_n$.

Lemma 2.2.22. *Let $G \subseteq S_n$ be a transitive subgroup. Suppose there exists a subgroup $H \subseteq G$ which is isomorphic as a permutation subgroup to S_k for some $k > n/2$, when considering the action on a k-element subset of $\{1, \ldots, n\}$. Then $G \simeq S_n$.*

Proof. The proof is by induction on k, with trivial base case $k = n$. Assume $n/2 < k < n$ and that the statement holds for $k+1$. Renumber so that $H \subseteq G$ fixes $\{k+1, \ldots, n\}$ and H is identified with S_k. Our goal is to add elements to H to generate a subgroup $H' \simeq S_{k+1}$, then apply the inductive hypothesis to see $G = S_n$.

Since $H \simeq S_k$, we have that H (and thus G) contains the transpositions of the form $(1\ a)$ for $2 \leq a \leq k$. By transitivity of G, there exists $\rho \in G$ such that $\rho(1) = k+1$.

Conjugating by ρ, we produce $k-1$ transpositions

$$\rho(1\ a)\rho^{-1} = (k+1\ \rho(a)) \in G.$$

As a ranges over the $k-1$ values $2 \leq a \leq k$, $\rho(a)$ takes $k-1$ distinct values also. There are only $n-k-2$ integers between $k+2$ and n, and our hypothesis that $k > n/2$ implies that

$$n-k-2 < k-2,$$

so at least one of our $\rho(a)$ values falls between 1 and k.

Letting a be such that $1 \leq \rho(a) = x \leq k$, we have produced a transposition $(x\ k{+}1) \in G$. Setting $H' = \langle H, (x\ k+1)\rangle \subseteq G$ and viewing this as a permutation subgroup of S_n on the set $\{1, \ldots, k+1\}$, we see that

$$\{(x\ i) \mid 1 \leq i \leq k+1,\ i \neq x\} \subset H'.$$

By Proposition 2.2.15 this is a generating set for S_{k+1}, so $H \simeq S_{k+1}$. Applying the inductive hypothesis, we conclude $G = S_n$. □

The idea of Lemma 2.2.22 is that transitive subgroups cannot become too big — or perhaps too interconnected — before they are forced to be the full symmetric group S_n. Using this principle, we identify other collections of elements with specified cycle type that force a transitive subgroup to be the full symmetric group.

Proposition 2.2.23. *Fix an integer $m \geq 2$. Suppose $n > m$ and $G \subseteq S_n$ is a transitive subgroup containing the following elements:*

(i) an ℓ-cycle σ with $n - m \leq \ell < n$,

(ii) a transposition τ, and

(iii) a q-cycle θ for a prime $q > m$.

Then $G = S_n$.

Proof. When $m \geq n/2$, (ii) and (iii) ensure that G satisfies the hypotheses of Proposition 2.2.19 and we have $G = S_n$. Hence, let us assume that $n > 2m$.

Assume for concreteness that $\ell = n - m$, so choosing a suitable numbering we have $\sigma = (1 \ \dots \ n-m)$. The following argument will still work the same way if $n - m < \ell < n$. By the transitivity of G, we may further assume $\tau = (1 \ a)$ and that $\theta = (1 \ b_2 \dots \ b_q)$.

Suppose first that $a > n - m$ and consider the subgroup $H = \langle \theta, \tau \rangle \subseteq G$. We can view H as a permutation subgroup on $\{1, \dots, n-m, a\}$, i.e. as a subgroup of S_{n-m+1}. In fact, the action of H on this set is transitive; elements between 1 and $n - m$ can be interchanged by repeated applications of the cycle σ, while a can be reached by using τ to move $a \mapsto 1$. Therefore, H is a transitive subgroup of S_{n-m+1} containing an $(n-m)$-cycle and a transposition, so by Proposition 2.2.18 we have $H = S_{n-m+1}$.

The hypothesis that $n > 2m$ implies that $n - m + 1 > n/2$, so applying Lemma 2.2.22 reveals that $G = S_n$ in this case.

On the other hand, suppose $a \leq n - m$. Now it is not sufficient to package τ and σ together and get a subgroup isomorphic to a large symmetric group (recall Examples 2.2.20 and Remark 2.2.21).

Instead, let $H' = \langle \tau, \theta \rangle \subseteq G$ and view H' as acting on $\{1, a, b_2, \dots, b_q\}$. This set contains either q or $q + 1$ many elements, depending on whether $a = b_i$ for some i, but in either case we have that H' is the full symmetric group acting on this set. In particular, we have $S_q \subseteq H' \subseteq G$.

This buys us *at least* $q - 1 \geq m$ distinct transpositions of the form $(1 \ c_i)$ in G (where the elements c_i are either b_j for $2 \leq j \leq q$ or $c_i = a$). By the transitivity of G, there exists $\rho \in G$ such that $\rho(1) = n - m + 1$ and conjugating our transpositions gives

$$\rho(1 \ c_i)\rho^{-1} = (n - m + 1 \ \rho(c_i)) \in G.$$

There are only $m-1$ integers between $n-m+1$ and n, but we have at least m transpositions, and hence images $\rho(c_i)$, so at least one of them satisfies $1 \leq \rho(c_i) \leq n - m$.

After a renumbering sending $\rho(c_i) \mapsto 1$ and leaving $n - m + 1$ alone, we have the transposition $(1 \ n - m + 1) \in G$, putting us back in the earlier case of $a > n - m$. Hence

we conclude that $G = S_n$. □

Remark 2.2.24. The hypotheses of Proposition 2.2.23 are somewhat contrived. They were originally intended to be combined with the theory of Newton polygons to show that the Galois group of a degree n polynomial over $\mathbb{Q}$ may be identified with S_n, where the transitivity hypothesis is equivalent to the irreducibility of the polynomial.

For polynomials arising from higher degree points on hyperelliptic and superelliptic curves as discussed in Chapter 3, Proposition 2.1.28 seems too inflexible to produce (i), (ii), and (iii), as it is difficult to come up with cycles of the desired lengths using only Newton polygons. In the hyperelliptic case (see §3.3) Propositions 2.2.18 and 2.2.19 turn out to be sufficient to show many such polynomials have symmetric Galois group. We include Proposition 2.2.23 in hopes that it, or potential generalizations, becomes useful in this regard or is of of independent interest.

2.3 Chebotarev's density theorem

Let E/F be a Galois extension of number fields with $G = \mathrm{Gal}(E/F)$. In this section, we recall the statement of the classical density theorem due to Chebotarev, and record some useful elementary consequences. For more, see e.g. [Lan94, Chapter VIII, §4] or [Neu99, Chapter VII, §13].

We begin with some standard notation and definitions. We denote by $\mathcal{O}_F$ the ring of integers of F and use P to denote maximal ideal of $\mathcal{O}_F$ with residue field $\mathbb{F}_P = \mathcal{O}_F/P$. We simply refer to such P as a prime of F.

Definition 2.3.1 (norm)**.** Given a nonzero prime P of F, the **absolute norm** of P is the size of the residue field,

$$N_F(P) = \#\left(\mathcal{O}_F/P\right) = \#\mathbb{F}_P.$$

This norm gives us a way to count primes and measure subsets of primes.

Definition 2.3.2 (natural density)**.** Let S be a subset of the set of primes of F. If it exists, the limit

$$\delta(S) = \lim_{x\to\infty} \frac{\#\left\{P \in S \mid N_F(P) \leq x\right\}}{\#\left\{P \mid N_F(P) \leq x\right\}}$$

is known as the **natural density** of S.

In the case $F = \mathbb{Q}$, we have $N_{\mathbb{Q}}(p) = p$ for a prime p (or rather the ideal $(p) \subset \mathbb{Z}$). We then have well known statements such as the density of rational primes p in a given congruence class mod N.

Theorem 2.3.3 (Dirichlet)**.** *Fix a natural number $N \geq 1$ and an integer n such that $\gcd(n, N) = 1$. Suppose S is the set of primes $p \equiv n \pmod{N}$. Then*

$$\delta(S) = \frac{1}{\varphi(N)}$$

where φ is Euler's totient function, or equivalently $\varphi(N) = \#\left(\mathbb{Z}/N\mathbb{Z}\right)^{\times}$.

Dirichlet's theorem is special abelian case of Chebotarev's theorem. To state the more general version, we recall some definitions.

Definition 2.3.4 (decomposition and inertia groups)**.** Let P be a prime of F and Q a prime of E above P. The **decomposition group of Q** is

$$D_Q = \{\sigma \in G \mid \sigma(Q) = Q\}.$$

Elements of σ fix Q, and thus give well defined automorphisms of the residue field $\mathbb{F}_Q$, allowing us to define define a subgroup

$$I_Q = \{\sigma \in D_Q \mid \sigma|_{\mathbb{F}_Q} = \mathrm{id}_{\mathbb{F}_Q}\}$$

known as the **inertia group of Q**.

We have a natural exact sequence of groups

$$0 \to I_Q \to D_Q \to \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P) \to 0 \tag{2.3.1}$$

where exactness on the right is proven in [Neu99, Proposition I.9.4], while the rest follows from the definition. We remark on the similarity of (2.3.1) with Proposition 2.1.15. This is no coincidence, as D_Q may be identified with the Galois group of the extension of local

fields obtained by completing E and F at the primes Q and P, respectively; see [Neu99, Proposition II.9.6]

Definition 2.3.5 (Frobenius)**.** Let Q be a prime of E above P and $\mathbb{F}_Q/\mathbb{F}_P$ the associated extension of residue fields. A **Frobenius element** $\mathrm{Frob}_Q \in D_Q$ is a preimage of the cyclic generator under the map $D_Q \to \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$. If Q is unramified, then Frob_Q is unique.

For an unramified prime P, Frob_P is the conjugacy class in G of Frobenius elements Frob_Q for a prime Q above P.

For any Q, Q' above an unramified prime P, Frob_Q and $\mathrm{Frob}_{Q'}$ are conjugate. Moreover, any conjugate of Frob_Q is a Frobenius element for a prime Q' above P, since G permutes the primes above P transitively. Thus Frob_P is well defined as a conjugacy class of G.

Theorem 2.3.6 (Chebotarev, see e.g. [Lan94, Ch. VIII, §4, Theorem 10])**.** *Fix a subset $C \subseteq G$ invariant under conjugation. Let S be the subset of primes of E with $\mathrm{Frob}_P \subseteq C$. Then the natural density of S exists and $\delta(S) = \frac{\#C}{\#G}$.*

Example 2.3.7 (cyclotomic extensions and Dirichlet's theorem)**.** Fix N and let $E = \mathbb{Q}(\zeta_N)$ for ζ_N a primitive N-th root of unity. Set $F = \mathbb{Q}$, so we have $G = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. This is abelian, so each conjugacy class is a single element.

Let $n \in (\mathbb{Z}/N\mathbb{Z})^\times$. What does it mean for Frob_p to correspond to n for a prime $p \nmid N$? It means precisely that $p \equiv n \pmod N$. To see why, consider the automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ given by $\sigma_p \colon \zeta_N \mapsto \zeta_N^p$. It is straightforward to compute that this induces the p-th power map on $\mathbb{F}_Q = \mathbb{Z}[\zeta_N]/Q$, which is precisely Frob_Q.

But σ is determined by the residue class of p modulo N, with $\sigma_p = \sigma_n$ for $p \equiv n \pmod N$. Thus $\mathrm{Frob}_Q = \mathrm{Frob}_P = \sigma_n$. Chebotarev's theorem then tells us that the density of primes $p \equiv n \pmod N$ is $\frac{1}{\varphi(N)}$, which is precisely the statement of Dirichlet's theorem.

Example 2.3.8 (Legendre symbols)**.** Fix an integer n not a perfect square. Recall for a prime $p \nmid n$, the Legendre symbol $\left(\frac{n}{p}\right) = \pm 1$, taking the value $+1$ when n is a quadratic residue modulo p and -1 if it is a nonresidue. Equivalently, in the extension $E = \mathbb{Q}(\sqrt{n})$ over $\mathbb{Q}$, $\left(\frac{n}{p}\right)$ detects whether p splits or remains inert.

If p splits in E and Q is a prime above p, then we have $\mathbb{F}_Q = \mathbb{F}_p$, in which case $\mathrm{Frob}_Q = \mathrm{Frob}_p$ is the identity element of $\mathbb{Z}/2\mathbb{Z} = \mathrm{Gal}(E/\mathbb{Q})$. Theorem 2.3.6 then asserts

that 50% of primes p split in E, i.e. for half of primes p we have that n is a quadratic residue, and vice-versa.

Example 2.3.9 (splitting)**.** Examples 2.3.7 and 2.3.8 involve abelian (in fact cyclic and quadratic) extensions $E/\mathbb{Q}$. More generally, for arbitrary (and perhaps nonabelian) extensions E/F with Galois group G, the set of primes P of F with Frob_P corresponding to the trivial conjugacy class has density $\frac{1}{\#G}$ by Theorem 2.3.6.

If Frob_P is trivial, then Frob_Q is trivial for all primes Q above P. In this case we have $\mathbb{F}_Q = \mathbb{F}_P$, so the prime P is (totally) split in E.

2.3.1 Useful consequences of the density theorem

Some useful facts about polynomials — many of which can be proved without appealing to Chebotarev's result — follow from Theorem 2.3.6 together with the observations made in Example 2.3.9. Namely, if $f \in \mathcal{O}_F[x]$ is an irreducible polynomial, $K = F[x]/(f)$, and P is a prime of F, then the factorization of f modulo P is related to how P splits in K. While we will not need to use it, a theorem of Dedekind makes this precise; see e.g. [Con].

We state and later use these results in the $F = \mathbb{Q}$ case, but note that they extend to arbitrary base fields.

Lemma 2.3.10. *Let $f(x) \in \mathbb{Z}[x]$. There exist infinitely many primes p such that we can find $x_0 \in \mathbb{Z}$ for which $f(x_0) \equiv 0 \pmod{p}$.*

Moreover, if $f(x)$ is squarefree then there exist infinitely many such p and $x_0 \in \mathbb{Z}$ with $p \mid\mid f(x_0)$.

Proof. If f is not squarefree, then we may replace it by the polynomial obtained by removing all repeated factors. Thus it suffices to prove the claims for f squarefree. If

Let E be the Galois extension obtained by adjoining all roots of f to $\mathbb{Q}$. It follows from Chebotarev's theorem that the density of primes p splitting completely in E is positive, equal to $\frac{1}{\#\mathrm{Gal}(E/\mathbb{Q})}$. In particular, there are infinitely many such primes p. Fix one of them, sufficiently large so that $p \nmid \mathrm{Disc}\, f$, in which case $\overline{f}(x) \in \mathbb{F}_p[x]$ is also squarefree.

Since p splits completely in E, it must split completely in the subextension $K = \mathbb{Q}[x]/f_0(x) \subset E$ obtained by adjoining the root of some irreducible factor f_0 of f. From this

it follows that the reduction of $f(x)$ modulo p splits completely into linear factors, distinct by the fact that $p \nmid \operatorname{Disc} f$.

Let $(x - \alpha) \mid \overline{f}(x)$ be such a linear factor and take x_0 an integer such that $x_0 \equiv \alpha \pmod{p}$. Then $\overline{f}(x_0) = 0$ and equivalently $p \mid f(x_0)$, proving the first statement.

For the second statement, suppose $p^2 \mid f(x_0)$. We evaluate $f(x_0 + p)$ using a Taylor expansion:

$$f(x_0 + p) = f(x_0) + pf'(x_0) + O(p^2).$$

Since $p \nmid \operatorname{Disc} f$, the root of $\overline{f}$ at x_0 is not a multiple root, and thus we know $p \nmid f'(x_0)$. Then by the above, $p^2 \nmid f(x_0 + p)$ and we are done. □

When f is not squarefree, it will be convenient to have an analogue of the "moreover" statement in Lemma 2.3.10.

Corollary 2.3.11. *Let $f(x) \in \mathbb{Z}[x]$ and suppose f has an irreducible factor f_0 appearing with multiplicity $e \geq 1$ in its factorization. Then there exist infinitely many primes p such that there exists $x_0 \in \mathbb{Z}$ for which $p^e \mid\mid f(x_0)$.*

Proof. Write the irreducible factorization $f = \prod_{i \geq 0} f_i^{e_i}$ and let $g = \prod_{i \geq 0} f_i$. Applying Lemma 2.3.10 to f_0, we find infinitely many primes $p > \operatorname{Disc} g$ for which there exists $x_0 \in \mathbb{Z}$ such that $p \mid\mid f_0(x_0)$. Clearly we have $p \mid g(x_0)$. Since the roots of g are distinct modulo p, $p \nmid \prod_{i>0} f_i(x_0)$, so we have $p \mid\mid g(x_0)$. Returning to f, we have $p^e \mid\mid f_0(x_0)^e$ and $p \nmid f_i(x_0)^{e_i}$, so $p^e \mid\mid f(x_0)$. □

Chapter 3

Fields generated by points on curves

3.1 Introduction

Let K be a number field, and let C/K be a smooth curve of genus g. Faltings [Fal83] proved that when $g \geq 2$, the set of K-rational points on C, $C(K)$, is finite. It is natural to ask if similar finiteness results hold for the higher degree points of C. We say the degree of an algebraic point $P \in C(\overline{K})$ is the degree $[K(P) : K]$, where $K(P)$ is the minimal field of definition for P. While in fact a curve of genus $g \geq 2$ may have infinitely many points of some degree $n > 1$, it is still an interesting problem to characterize when this occurs and prove finiteness results for "sporadic" points. There have been several recent works related to the study of higher degree points on families of hyperelliptic curves (see [BGW17, GM19]) and on various modular curves (see [BEL$^+$19, Box21, BGRW20, BN15, DEvH$^+$21, OS19]).

Instead of studying the points of C, one can take the perspective of studying the set of field extensions $K(P)/K$ generated by algebraic points $P \in C(\overline{K})$. This idea was suggested by Mazur and Rubin [MR18] in their program for Diophantine stability, where a variety over K is said to be Diophantine stable for L/K if its K-rational points and L-rational points coincide. A natural first question is to ask how many extensions generated by an algebraic point exist for a fixed degree when ordered by discriminant, following the discussion in §1.1.

Fixing the base field $K = \mathbb{Q}$, we recall the following functions for counting number fields by discriminant. Let

$$N_n(X) = \#\left\{K/\mathbb{Q} \mid [K:\mathbb{Q}] = n,\ |\mathrm{Disc}\, K/\mathbb{Q}| \le X\right\},$$

where $X > 0$ is a real number and $n \ge 1$ is any positive integer. For a fixed curve $C/\mathbb{Q}$, we define the counting function for extensions generated by an algebraic point of C to be

$$N_{n,C}(X) = \#\left\{\mathbb{Q}(P)/\mathbb{Q} \mid P \in C(\overline{\mathbb{Q}}),\ [\mathbb{Q}(P):\mathbb{Q}] = n,\ |\mathrm{Disc}\, \mathbb{Q}(P)/\mathbb{Q}| \le X\right\}.$$

We further define

$$N_{n,C}(X, G) = \#\Big\{\mathbb{Q}(P)/\mathbb{Q} \mid P \in C(\overline{\mathbb{Q}}),\ [\mathbb{Q}(P):\mathbb{Q}] = n, \\ |\mathrm{Disc}\, \mathbb{Q}(P)/\mathbb{Q}| \le X,\ \mathrm{Gal}(\widetilde{\mathbb{Q}(P)}/\mathbb{Q}) \simeq G\Big\}$$

where G is a transitive permutation subgroup of the symmetric group S_n and $\widetilde{\mathbb{Q}(P)}$ denotes the Galois closure of $\mathbb{Q}(P)/\mathbb{Q}$.

When E is an elliptic curve over $\mathbb{Q}$, Lemke Oliver and Thorne [LT21] show for a positive constant δ_n approaching $1/4$ from below as $n \to \infty$, we have $N_{n,E}(X, S_n) \gg X^{\delta_n - \epsilon}$. Conditionally, this exponent can be improved to approach $1/4$ from above. In fact, they show something stronger, namely that $X^{\delta_n - \epsilon}$ is an asymptotic lower bound on degree n extensions for which the Mordell–Weil ranks satisfy $\mathrm{rk}\, E(K) > \mathrm{rk}\, E(\mathbb{Q})$, with specified root number.

We first extend this approach to hyperelliptic curves.

Definition 3.1.1 (hyperelliptic curve)**.** A **hyperelliptic curve** $C/\mathbb{Q}$ is an algebraic curve given by the affine equation

$$C\colon y^2 = f(x) = \sum_{i=0}^{d} c_i x^i, \tag{3.1.1}$$

where $f(x) \in \mathbb{Z}[x]$ is a squarefree polynomial of degree $d \ge 3$. The genus g of C is related to the degree d by $g = \left\lfloor \frac{d-1}{2} \right\rfloor$.

The main results of [Key22] are an asymptotic lower bound for $N_{n,C}(X, S_n)$ when n is

large relative to d, generalizing that of Lemke Oliver and Thorne and recovering their bound when $g = 1$. We treat the cases of d odd and even separately in Theorems 3.1.2 and 3.1.3 below. In both cases, the implied constants depend on the degree n and the polynomial f, and we are able to improve the result somewhat when n is sufficiently large.

Theorem 3.1.2 (K. [Key22, Theorem 1.1]). *Let C be a hyperelliptic curve with genus $g \geq 1$ and degree $d = 2g + 1$. If $n \geq d$, then*

$$N_{n,C}(X, S_n) \gg X^{\delta_n}$$

where

$$\delta_n = \frac{1}{4} - \frac{gn^2 - (g^2 - 2g - 3)n - 2g^2}{2n^2(n-1)}.$$

Moreover, if n is sufficiently large, we have the improvement

$$\delta_n = \frac{1}{4} - \frac{gn + g^2 - 2g}{2n(n-1)}.$$

The case that d is odd coincides with an appropriate projectivization of C having a rational Weierstrass point at infinity. In the general case where d is even, we restrict our attention to even n. This turns out to be a necessary restriction in light of the fact that a positive proportion of hyperelliptic curves over $\mathbb{Q}$ have no points over any odd degree extensions [BGW17]. After making this restriction, we obtain a similar asymptotic lower bound to Theorem 3.1.2.

Theorem 3.1.3 (K. [Key22, Theorem 1.2]). *Let C be a hyperelliptic curve with genus $g \geq 1$ and degree $d = 2g + 2$. If $n \geq d + 2$ is even, then*

$$N_{n,C}(X, S_n) \gg X^{\delta_n}$$

where

$$\delta_n = \frac{1}{4} - \frac{(1 + 2g)n^2 - (2g^2 - 2g - 8)n - (4g^2 + 4g)}{4n^2(n-1)}.$$

Moreover, when n is sufficiently large, we have the improvement

$$\delta_n = \frac{1}{4} - \frac{(1+2g)n - 2g^2 + 2g + 2}{4n(n-1)}.$$

We continue this program of studying the the set of fields generated by points on curves defined over $\mathbb{Q}$ in the case of superelliptic curves.

Definition 3.1.4 (superelliptic curve)**.** Fix a positive integer $m \geq 2$. A **superelliptic curve** $C/\mathbb{Q}$ of exponent m is an algebraic curve given by the affine equation

$$C\colon y^m = f(x) = \sum_{i=0}^{d} c_i x^i, \tag{3.1.2}$$

where $f(x) \in \mathbb{Z}[x]$ is an m-th power free polynomial of degree d, and moreover not an e-th power for any nontrivial divisor $e \mid m$.

Such a curve possesses a degree m map to the line $\mathbb{A}^1$ defined over $\mathbb{Q}$, sending a point $(x, y) \mapsto x$. The condition on f not being an e-th power is equivalent to asking for C to be geometrically irreducible; see Lemma 4.2.3. Here we restrict further to the case where $m \mid d$, or equivalently that the superelliptic map is unramified at infinity. When n is a sufficiently large multiple of m, we have the following asymptotic lower bound for $N_{n,C}(X)$.

Theorem 3.1.5 (Beneish–K. [BK21a])**.** *Let C be a superelliptic curve with equation (3.1.2) with $m \mid d$ and suppose n is a multiple of $\gcd(m, d)$ satisfying*

$$n \geq \max(d, \operatorname{lcm}(m, d) - m - d + 1, 2m^2 - m).$$

Then we have

$$N_{n,C}(X) \gg X^{\delta_n}, \tag{3.1.3}$$

where δ_n is a constant depending on m, d, and n given explicitly in (3.5.1) and $\delta_n \to \frac{1}{m^2}$ as $n \to \infty$. The implied constant in (3.1.3) depends only on n and (the equation for) C.

Moreover, for all sufficiently large n (relative to m and d) with $m \mid d$, we have the

improvement

$$\delta_n = \frac{1}{m^2}\left(1 + \frac{(2m-2dr+1)n + d^2r^2 - mdr + mk - k^2}{2n(n-1)}\right), \tag{3.1.4}$$

where $1 \le r < m$ *and* $0 \le k < m$ *are integers depending only on the residue classes of* $n, d \pmod m$.

Remark 3.1.6. We make note of a few properties of the constant δ_n in Theorem 3.1.5.

(i) For any fixed choice of m, d, the constant δ_n in (3.1.3) satisfies $\delta_n - \frac{1}{m^2} \sim \frac{m-m^2-dr+3}{m^2(n-1)}$ in the limit as $n \to \infty$, where $1 \le r < m$ is an integer depending only on $n, d \pmod m$. In particular, $\frac{m-m^2-dr+3}{m^2(n-1)}$ is negative, so we can say that in (3.1.3), δ_n approaches $\frac{1}{m^2}$ from below.

(ii) In contrast, the improved exponent in (3.1.4) satisfies $\delta_n - \frac{1}{m^2} \sim \frac{2m-2dr+1}{2m^2(n-1)}$. In the case $m = d$ we have $r = 1$ and thus $2m - 2dr + 1 = 1$, so $\delta_n \to \frac{1}{m^2}$ from above as $n \to \infty$. If $m < d$, the improved δ_n will approach $\frac{1}{m^2}$ from below as in (3.1.3).

(iii) The improved exponent in (3.1.4) takes effect when we have good enough asymptotic upper bounds for $N_n(X)$. The best currently known to the author, due to Lemke Oliver and Thorne [LT22, Theorem 1.1], suffices when n is taken to be large. We discuss how large n must be for (3.1.4) to be known to hold in §3.5.4; see Figure 3.5.1.

(iv) Theorem 3.1.5 agrees with or improves upon known lower bounds for $N_{n,C}(X, S_n)$ in the cases where C is an elliptic curve [LT21] or a hyperelliptic curve [Key22].

(v) We do not expect this lower bound to be sharp; in the case where C is an ellpitic curve, Lemke Oliver–Thorne [LT21] suggest a heuristic of $X^{3/4+o(1)}$ for the asymptotics of the number of fields $K/\mathbb{Q}$ for which $\operatorname{rk} E(K) = \operatorname{rk} E(\mathbb{Q}) + 2$.

The strategy for proving Theorems 3.1.2, 3.1.3, and 3.1.5, employed also in [LT21], is to use the equation for $C/\mathbb{Q}$ to find an explicit parameterized family of polynomials generating degree n extensions $\mathbb{Q}(P)/\mathbb{Q}$ with Galois closure S_n. Some effort is required to verify that the members of the family are in fact irreducible and, when appropriate, have Galois group

S_n. We then count the polynomials in this family and bound how often the number fields they generate are isomorphic.

A notable limitation of Theorem 3.1.5 is the condition that $m \mid n$. We suspect that as in the case of hyperelliptic curves, the presence of at least one rational point should allow a similar parameterization strategy to produce infinite families of degree n fields $\mathbb{Q}(P)/\mathbb{Q}$ for all n sufficiently large. However, we do not expect this to be the general case, though we are aware of no analogue of [BGW17] for superelliptic curves with $m > 2$.

In §3.6 we speculate as to whether for superelliptic curves, points of degrees n such that $\gcd(m, d) \mid n$ are more common than points of degrees n where $\gcd(m, d) \nmid n$. This section contains a description of various geometric sources from which we expect to find infinitely many points on these curves. We also discuss the relationship of these sources to the points obtained by the parameterization strategy. As a first step towards making these heuristics concrete, we prove the following. Informally, we find that for a certain family of superelliptic curves, many have only finitely many points of certain small degrees n.

Proposition 3.1.7 (See also Proposition 3.6.8)**.** *Suppose m, d are positive even integers such that $d > 4$. Let $n < \frac{d}{2} - 1$ have 2-adic valuation strictly less than that of m, i.e. $v_2(n) < v_2(m)$. Then for a positive proportion approaching 100% of squarefree degree d polynomials $f(x)$, ordered by height, the superelliptic curve $C: y^m = f(x)$ has only finitely many points of degree n.*

3.1.1 Layout

This chapter is organized as follows. In §3.2 we give an overview of the parameterization strategy used in the proofs of the main theorems, while §3.3 and §3.4 are devoted to proving that our parameterization strategy almost always produces irreducible polynomials in the hyperelliptic and superelliptic cases, respectively. Here we use the theory of Newton polygons developed earlier in §2.1.3 as well as the criteria for a transitive permutation group to be the symmetric group from §2.2. Then in §3.5 we describe how to count the polynomials produced by our parameterization and adjust for multiplicity to obtain lower bounds for $N_{n,C}(X)$. Wherever possible, we attempt to streamline our exposition to apply to both

hyperelliptic and superelliptic curves. A discussion of the geometric sources for infinite collections of points on superelliptic curves, and their relevance to field counting problems of this flavor, is given in §3.6.

3.2 The parametrization strategy

To produce algebraic points on C, our strategy is to parameterize the coordinates x and y as rational functions in an auxiliary variable t. We set

$$x(t) = \frac{\gamma(t)}{\eta(t)} \quad \text{and} \quad y(t) = \frac{g(t)}{h(t)}.$$

Substituting into the equation for C, given by (3.1.2), and clearing denominators, we obtain the polynomial equation

$$F_{g,h,\gamma,\eta}(t) = h(t)^m\Big(c_d\gamma(t)^d + c_{d-1}\gamma(t)^{d-1}\eta(t) + \cdots + c_1\gamma(t)\eta(t)^{d-1} + c_0\eta(t)^d\Big) - g(t)^m\eta(t)^d = 0. \tag{3.2.1}$$

Suppose g, h, γ, η are chosen in $\mathbb{Z}[t]$ such that $F_{g,h,\gamma,\eta}(t)$ is irreducible with some root α. Then

$$P = (x(\alpha), y(\alpha)) = \left(\frac{\gamma(\alpha)}{\eta(\alpha)}, \frac{g(\alpha)}{h(\alpha)}\right)$$

is a point on C defined over the field $\mathbb{Q}(\alpha)$, and $\mathbb{Q}(\alpha)$ is the field generated by P. Given a degree n, our approach is to count how many ways we can choose g, h, γ, η such that $F_{g,h,\gamma,\eta}$ is degree n, irreducible, and has Galois group S_n.

Generally, the degree of $F_{g,h,\gamma,\eta}$ is the maximum of $m(\deg h) + d(\deg \gamma)$ and $m(\deg g) + d(\deg \eta)$, both of which are multiples of $\gcd(m, d)$. Since we will eventually count the number of such parameterizations, we want to choose g, h, γ, η so the sum of their degrees is as large as possible, giving us the most degrees of freedom to count. Recall that in this paper, we have assumed $m \leq d$, so this sum of degrees will be maximized by letting $\deg g$ and $\deg h$ be large, while keeping those of γ and η small. To that end, we simply take $\eta = 1$ and suppress the notation by writing $F_{g,h,\gamma}$ for the remainder of this paper. However, in the general case, namely if $m > d$, it would be useful to take η to be nonconstant.

We observe that when n is a sufficiently large multiple of $\gcd(m,d)$, we can always choose the degrees of g, h, and γ to make the polynomial (3.2.1) have degree n in general. This is done by using $\deg\gamma$ to control the residue class of n modulo m if necessary, and letting $\deg g, \deg h$ be as large as possible. It remains to determine how large n must be for such degrees to exist. It is clear that we must have at least $n \geq d$ by looking at the minimum degree of $F_{g,h,\gamma}$. To give a more precise answer we recall the classical definition of the Frobenius number, with a straightforward generalization to integers that are not coprime.

Definition 3.2.1 (Frobenius number)**.** Given natural numbers a, b with $\gcd(a,b) = 1$, the **Frobenius number**, denoted $\mathrm{Frob}(a,b)$ is the largest natural number which is not a linear combination $ax + by$ where $x, y \geq 0$.

When $\gcd(a,b) \neq 1$, we define a **generalized Frobenius number**, also denoted $\mathrm{Frob}(a,b)$, to be the largest multiple of $\gcd(a,b)$ that is not a linear combination $ax + by$ for $x, y \geq 0$.

We have the elementary result that for coprime integers a, b, the Frobenius number is given by $\mathrm{Frob}(a,b) = ab - a - b$. Recognizing that for any natural numbers a, b we have

$$\mathrm{Frob}(a,b)/\gcd(a,b) = \mathrm{Frob}\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right),$$

we find that the generalized Frobenius number satisfies $\mathrm{Frob}(a,b) = \mathrm{lcm}(a,b) - a - b$.

For any $n \geq \max(d, \mathrm{Frob}(m,d) + 1)$ we can manipulate the degrees of g, h, and γ such that $\deg F_{g,h,\gamma} = n$ in (3.2.1). Moreover, this is sharp in the sense that (3.2.1) will not take degrees $n < d$ or $n = \mathrm{Frob}(m,d)$. We conclude this section by summarizing our discussion in the following proposition.

Proposition 3.2.2. *Let C be given by (3.1.2) with $m \leq d$. For all degrees n such that $n \geq \max(d, \mathrm{Frob}(m,d)+1)$ and $\gcd(m,d) \mid n$, there exist g, h, γ, η such that $F_{g,h,\gamma,\eta}(t)$ given in (3.2.1) has degree n.*

Explicitly, we can assume $\eta = 1$ *and take* g, h, γ *to have the degrees given below:*

$$\begin{aligned} &\deg g = n/m \\ &\deg h = \lfloor (n-d)/m \rfloor \qquad\qquad \textit{when } m \mid n, \\ &\deg \gamma = 1 \end{aligned} \tag{3.2.2}$$

and

$$\begin{aligned} &\deg g = \lfloor n/m \rfloor \\ &\deg h = (n - rd)/m \qquad\qquad \textit{when } m \nmid n, \\ &\deg \gamma = r \end{aligned} \tag{3.2.3}$$

where $r > 0$ *is the minimal integer such that* $n \equiv rd \pmod{m}$.

Notice that the choices above accomplish our goals of maximizing the total degrees of freedom by letting g, h have the largest possible degree, while $\deg \gamma$ is kept small, with $1 \leq r < m$.

Let C be a superelliptic curve with exponent m and defining polynomial $f(x)$, as in (3.1.2). As in Proposition 3.2.2, given any $n \geq n_0$ such that $\gcd(m, d) \mid n$, there exist choices of degrees (3.2.2) or (3.2.3) for g, h, γ such that the polynomial $F_{g,h,\gamma}(t)$ given in (3.2.1) has degree n in general. Writing

$$g(t) = \sum_{i=1}^{\deg g} a_i t^i, \qquad h(t) = \sum_{j=1}^{\deg h} b_j t^j, \qquad \gamma(t) = \sum_{\ell=1}^{\deg \gamma} \alpha_\ell t^\ell,$$

we can view $F_{g,h,\gamma}(t)$ as a degree n polynomial $F(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha}, t) \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})[t]$. Here $\boldsymbol{a}$ indicates the tuple of indeterminates $(a_0, \ldots, a_{\deg g})$, and similarly for $\boldsymbol{b}$ and $\boldsymbol{\alpha}$. For simplicity, since we have fixed the curve C and degree n, we will denote this polynomial family by $F \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})[t]$, and denote a rational specialization by $F_{\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0} \in \mathbb{Q}[t]$, where $\boldsymbol{a}_0 \in \mathbb{Q}^{\deg g + 1}, \boldsymbol{b}_0 \in \mathbb{Q}^{\deg h + 1}, \boldsymbol{\alpha}_0 \in \mathbb{Q}^{\deg \gamma + 1}$.

Since such $F \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})[t]$ is degree n, almost all specializations $F_{\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0}$ have degree n. With Hilbert's irreducibility theorem, we can say something stronger — that the

irreducibility and Galois group structure of the polynomial family carry over to most specializations. We state this classical result for a general polynomial $F(\boldsymbol{a}, t) \in \mathbb{Q}(\boldsymbol{a})[t]$ where $\boldsymbol{a}$ is some tuple of indeterminates.

Lemma 3.2.3 (Hilbert's irreducibility theorem)**.** *Let $F(\boldsymbol{a}, t) \in \mathbb{Q}(\boldsymbol{a})[t]$ with Galois group G. Suppose $\boldsymbol{a}_0$ is a rational specialization such that $F(\boldsymbol{a}_0, t) \in \mathbb{Q}[t]$ is irreducible with Galois group G_0. Then $F(\boldsymbol{a}, t)$ is irreducible as a polynomial in t over $\mathbb{Q}(\boldsymbol{a})$ and $G \simeq G_0$ for 100% of $\boldsymbol{a}_0$.*

The following corollary is more specific, as it refers to the permutation representations of the Galois groups. A proof may be found in [LT21, Theorem 4.2].

Corollary 3.2.4. *Suppose $F(\boldsymbol{a}, t) \in \mathbb{Q}(\boldsymbol{a})[t]$ is irreducible. If a permutation representation of G_0 contains a given cycle type for a positive proportion of integral specializations $\boldsymbol{a}_0$, then G contains an element of the same cycle type.*

Using Newton polygons as discussed in §2.1.3, our aim is to show that many integral specializations $F_{\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0}$ are in fact irreducible, and in some cases can be shown to have certain cycle types in their Galois groups. Corollary 3.2.4 implies that F must have those same cycles in its Galois group over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})$. In the case that C is a hyperelliptic curve, we will in fact prove that $G = \mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})) \simeq S_n$, and almost all specializations $F_{\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0}$ have Galois group S_n over $\mathbb{Q}$.

3.3 Polynomial families from hyperelliptic curves

We begin with the special case of hyperelliptic curves, i.e. taking $m = 2$ as in (3.1.1). Using the strategy outlined in the previous section, we construct a polynomial family whose specializations give rise to number fields generated by points on C with symmetric Galois group.

Let $g(t) = \sum_{i=0}^{d_g} a_i t^i \in \mathbb{Q}(\boldsymbol{a})[t]$ and $h(t) = \sum_{i=0}^{d_h} b_i t^i \in \mathbb{Q}(\boldsymbol{b})[t]$, where $\boldsymbol{a} = (a_0, \dots a_{d_g})$ and $\boldsymbol{b} = (b_0, \dots, b_{d_h})$. Then consider the polynomial in $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ given by

$$F_f(\boldsymbol{a}, \boldsymbol{b}, t) = g(t)^2 - f(t)h(t)^2, \tag{3.3.1}$$

which is the family described by Proposition 3.2.2. Since $0 < r < m = 2$, we take $r = \deg \gamma = 1$, and in this section we simply use $\gamma = t$ (though we occasionally will make change of variable arguments which are equivalent to choosing a different linear γ). We will use $F_{f,\boldsymbol{a}_0,\boldsymbol{b}_0}(t)$ to denote a specialization with $\boldsymbol{a}_0 \in \mathbb{Q}^{d_g+1}$ and $\boldsymbol{b}_0 \in \mathbb{Q}^{d_h+1}$.

Given $f(x)$ of degree $d \geq 3$ and a degree n, our goal is now to show that the polynomial family (3.3.1) is irreducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$ with Galois group $G \simeq S_n$. This will give us a means of producing many degree n number fields which are generated by algebraic points of C, which we can count later.

3.3.1 Curves with a Weierstrass point

Fix f with odd degree $d \geq 3$. Such curves C have a rational Weierstrass point at infinity. Fix a degree $n \geq d$. We take the degrees d_g and d_h as in Proposition 3.2.2,

$$d_g = \begin{cases} (n-1)/2, & n \text{ odd}, \\ n/2, & n \text{ even}, \end{cases}$$

$$d_h = \begin{cases} (n-d)/2, & n \text{ odd}, \\ (n-d-1)/2, & n \text{ even}. \end{cases}$$

For simplicity, we denote the polynomial family (3.3.1) by $F(t) \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ and a specialization by $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}(t) \in \mathbb{Q}[t]$, leaving both f and n implicit when it will not create confusion.

Proposition 3.3.1. *Fix a polynomial f and integers n, d_g, d_h as above. Then F_f is irreducible in $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ and $\mathrm{Gal}(F_f/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})) \simeq S_n$.*

Proof. The irreducibility and Galois group of $F_f(t)$ over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$ are invariant under a linear change of variables in t. It will be convenient to assume that the constant term of f, c_0, is nonzero, which is always possible after such a linear change of variables. We treat the cases of n even and odd separately.

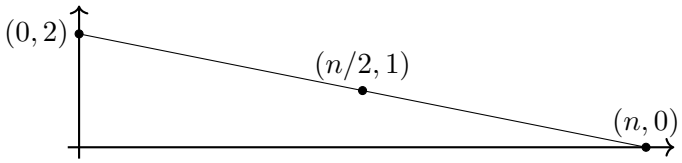
Case 1: n is even. When n is even, we take $d_g = n/2$ and $d_h = (n-d-1)/2$. Let p be a prime that does not divide any nonzero coefficient of f. Consider an integral specialization

$\boldsymbol{a}_0 = (a_0, \ldots, a_{n/2})$ and $\boldsymbol{b}_0 = (b_0, \ldots, b_{(n-d-1)/2})$ with the following p-adic valuations:

$$\begin{aligned} v_p(a_0) &= 1 \\ v_p(a_i) &\geq 1 \text{ for } 0 < i < n/2 \\ v_p(a_{n/2}) &= 0 \\ v_p(b_j) &\geq 2 \text{ for } 0 \leq j \leq (n-d-1)/2. \end{aligned} \tag{3.3.2}$$

These requirements on the valuations of b_j allow us to effectively ignore the $h_{\boldsymbol{b}_0}(x)^2 f(x)$ term of $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ in constructing the Newton polygon. Inspecting the valuations of the coefficients of $g_{\boldsymbol{a}_0}(x)^2$ gives the resulting $\mathbb{Q}_p$-adic Newton polygon for $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$, shown in Figure 3.3.1.

Figure 3.3.1: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with one segment of slope $-2/n$



The Newton polygon $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ has one segment of slope $-2/n$, so by Lemma 2.1.26, if $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ is reducible over $\mathbb{Q}_p$ then it is the product of two degree $n/2$ irreducible factors. In particular, if F is reducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$, it must also be the product of two degree $n/2$ irreducible factors, as any other factorization would yield an incompatible factorization upon specializing by $\boldsymbol{a}_0, \boldsymbol{b}_0$ with the valuations given in (3.3.2).

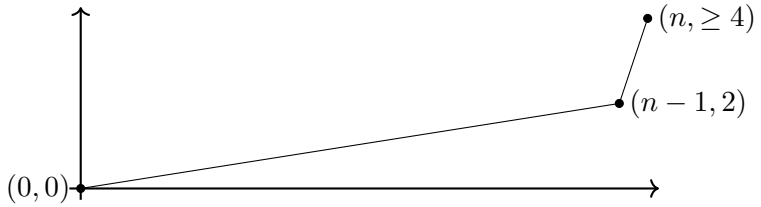
Let us now consider a different integral specialization $\boldsymbol{a}_0, \boldsymbol{b}_0$ with the following p-adic valuations:

$$\begin{aligned} v_p(a_0) &= 0 \\ v_p(a_i) &\geq 2 \text{ for } 0 < i \leq n/2 \\ v_p(b_j) &\geq 2 \text{ for } 0 \leq j < (n-d-1)/2 \\ v_p(b_{(n-d-1)/2}) &= 1. \end{aligned} \tag{3.3.3}$$

The constant term of $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ is $a_0^2 - b_0^2 c_0$ which has valuation 0. All other coefficients can be seen to have valuation at least 2, with the leading coefficient having valuation at least 4.

The coefficient of x^{n-1} is given by $2a_{n/2-1}a_{n/2} - b^2_{(n-d-1)/2}c_d$, which has valuation exactly 2. The resulting Newton polygon is shown below in Figure 3.3.2.

Figure 3.3.2: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with $(n-1)$-cycle



This Newton polygon has a segment of length $n-1$ and slope equal to $2/(n-1)$, so by Lemma 2.1.26 whenever $\boldsymbol{a}_0, \boldsymbol{b}_0$ have the p-adic valuations given in (3.3.3), we have that $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ factors as a degree $n-1$ irreducible polynomial times a linear polynomial over $\mathbb{Q}_p$. Such a factorization cannot occur if F has two irreducible degree $n/2$ factors over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$, so we may conclude that F is irreducible, and hence G is a transitive permutation subgroup of S_n. Moreover, Proposition 2.1.28 implies that the Galois group of $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ over $\mathbb{Q}$ contains a cycle of length $n-1$ whenever $\boldsymbol{a}_0$ and $\boldsymbol{b}_0$ satisfy the valuations in (3.3.3). These valuation criteria are satisfied for a positive proportion of integral specializations $\boldsymbol{a}_0$ and $\boldsymbol{b}_0$, so Corollary 3.2.4 implies that G contains an $(n-1)$-cycle.

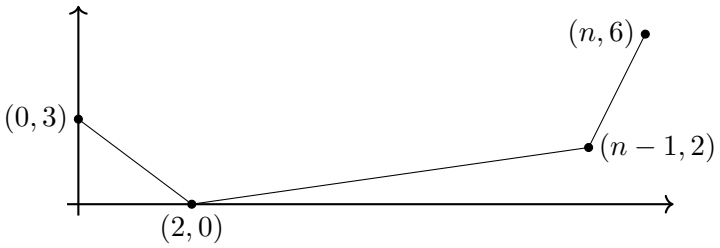
To produce a transposition in G, we apply a consequence of Chebotarev's density theorem, Lemma 2.3.10. Since f is squarefree, there exist infinitely many primes p for which there exists $x_0 \in \mathbb{Z}$ such that $p \mid f(x_0)$ but $p^2 \nmid f(x_0)$. Choosing one such prime $p > n$ with $p \nmid \operatorname{Disc} f, c_d$, after a possible change of variables, we may assume that $v_p(c_0) = 1$ and $v_p(c_1) = 0$.

We consider an integral specialization $\boldsymbol{a}_0, \boldsymbol{b}_0$ with the following p-adic valuations:

$$\begin{aligned} v_p(a_0) &= 2 \\ v_p(a_1) &= 0 \\ v_p(a_i) &\geq 2 \text{ for } 1 < i < n/2 \\ v_p(a_{n/2}) &= 3 \\ v_p(b_0) = v_p(b_{(n-d-1)/2}) &= 1 \\ v_p(b_j) &\geq 1 \text{ for } 0 < j < (n-d-1)/2. \end{aligned} \tag{3.3.4}$$

These requirements ensure that the constant term of $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ has valuation exactly 3, the coefficient of x^2 has valuation exactly 0, the x^{n-1} coefficient $2a_{n/2}a_{n/2-1} - b^2_{(n-d-1)/2}c_d$ has valuation exactly 2, and the leading term has valuation exactly 6, with all other coefficients having valuation at least 2. The resulting Newton polygon is shown below in Figure 3.3.3.

Figure 3.3.3: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with transposition



That $3 \leq d < n$ ensures that $\frac{2}{n-3} < 4$, so the two rightmost segments are distinct. These, together with the segment of length 2 and slope $-3/2$ above, ensure that $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ has factors of degree 2, $n-3$, and 1 over $\mathbb{Q}_p$, so Proposition 2.1.28 applies to reveal a transposition in $G_{\boldsymbol{a}_0,\boldsymbol{b}_0}$.

Since a positive proportion of integer tuples $\boldsymbol{a}_0, \boldsymbol{b}_0$ satisfy (3.3.4), Corollary 3.2.4 implies that G also contains a transposition. Thus G satisfies the hypotheses of Proposition 2.2.18 and we conclude that $G \simeq S_n$.

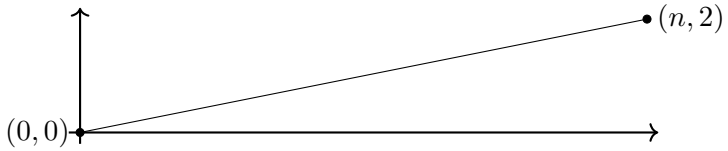
Case 2: n is odd. Now we take $d_g = (n-1)/2$ and $d_h = (n-d)/2$. Fix a prime p not dividing any nonzero coefficient of f. Consider an integral specialization $\boldsymbol{a}_0 = (a_0, \ldots, a_{(n-1)/2})$

and $\boldsymbol{b}_0 = (b_0, \dots b_{(n-d)/2})$ with the following p-adic valuations:

$$\begin{aligned} v_p(a_0) &= 0 \\ v_p(a_i) &\geq 2 \text{ for } i > 0 \\ v_p(b_j) &\geq 2 \text{ for } j < (n-d)/2 \\ v_p(b_{(n-d)/2}) &= 1. \end{aligned} \tag{3.3.5}$$

These requirements ensure that the constant term $a_0^2 - b_0^2 c_0$ has valuation exactly 0, the leading coefficient $b_{(n-d)/2}^2 c_d$ has valuation exactly 2, and all intermediate coefficients have valuation at least 2. This produces the p-adic Newton polygon for $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ shown below in Figure 3.3.4.

Figure 3.3.4: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with n-cycle



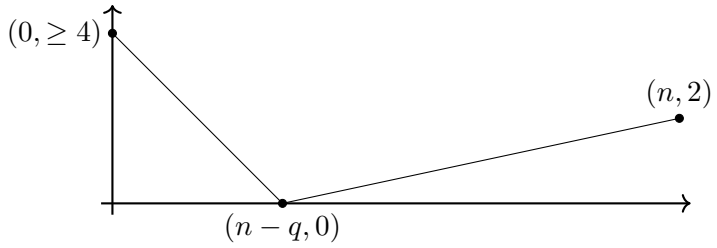
This Newton polygon has one segment of slope $2/n$, and since n is odd we have $\gcd(2, n) = 1$. Thus Lemma 2.1.26 implies that the specialization $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ is irreducible over $\mathbb{Q}_p$, hence over $\mathbb{Q}$, and we have that F must be irreducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$, with its Galois group G a transitive subgroup of S_n.

Next, we aim to produce a q-cycle in G for a prime $q > n/2$. We will assume $n > 3$ for now, as the case of $n = d = 3$ will be handled by later arguments. Recalling Bertrand's postulate, there exists some prime q such that $\frac{n-1}{2} < q < n - 1$, which is odd and satisfies $q > n/2$. Consider now a specialization $\boldsymbol{a}_0, \boldsymbol{b}_0$ satisfying

$$\begin{aligned} v_p(a_{(n-q)/2}) &= 0 \\ v_p(a_i) &\geq 2 \text{ for } i \neq (n-q)/2 \\ v_p(b_j) &\geq 2 \text{ for } j < (n-d)/2 \\ v_p(b_{(n-d)/2}) &= 1. \end{aligned} \tag{3.3.6}$$

These requirements ensure that the valuations of all coefficients of $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ are at least 2, except for the degree $n-q$ term, whose coefficient has valuation zero coming from the presence of an $a^2_{(n-q)/2}$ term. The leading coefficient $b^2_{(n-d)/2}c_d$ has valuation exactly 2. An example p-adic Newton polygon for such a specialization $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ is shown below in Figure 3.3.5.

Figure 3.3.5: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with q-cycle



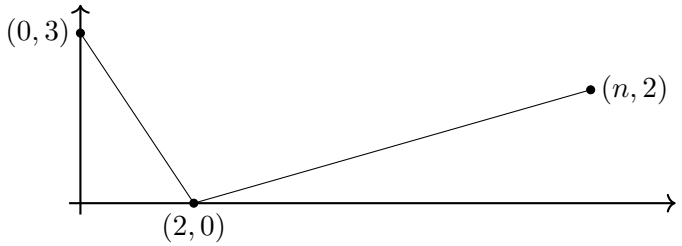
Note that the left side of the Newton polygon in Figure 3.3.5 need not be a single segment, or if $n = q$ it will not exist at all. This is inconsequential however, because the right side is of interest to us, in particular the segment of slope $2/q$ and length q. Since $q > n/2$ is an odd prime, we have $\gcd(2, q) = 1$ and q is coprime to any integers less than or equal to $n-q$, so Proposition 2.1.28 applies, ensuring the existence of a q-cycle in $G_{\boldsymbol{a}_0,\boldsymbol{b}_0}$. Since a positive proportion of integral specializations satisfy (3.3.6), Corollary 3.2.4 implies that G contains a q-cycle as well.

Finally, we can produce a transposition in G using essentially the same argument as in the case of even n. After a possible change of variables, let $p > n$ be a prime such that $v_p(c_0) = 1$ and $p \nmid \mathrm{Disc}\, f, c_d$. We consider specializations with the following p-adic valuations.

$$\begin{aligned} v_p(a_0) &= 2 \\ v_p(a_1) &= 0 \\ v_p(a_i) &\geq 2 \text{ for } 1 < i \leq (n-1)/2 \\ v_p(b_0) = v_p(b_{(n-d)/2}) &= 1 \\ v_p(b_j) &\geq 1 \text{ for } 0 < j < (n-d)/2. \end{aligned} \tag{3.3.7}$$

These conditions produce the Newton polygon shown below in Figure 3.3.6.

Figure 3.3.6: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with transposition



Since $n-2$ is odd, Proposition 2.1.28 applied to the segment of slope $-3/2$ implies that $G_{\boldsymbol{a}_0,\boldsymbol{b}_0}$, and hence G by Corollary 3.2.4, contains a transposition. Therefore, G satisfies the hypotheses of Proposition 2.2.19, and we conclude $G \simeq S_n$. □

3.3.2 Generic case

We now present the analogous proposition for the generic case, in which we assume d is even. Let $f(x) \in \mathbb{Z}[x]$ be squarefree given by $f(x) = \sum_{i=0}^{d} c_i x^i$, with $d \geq 4$ even. Fix an even integer $n \geq d+2$ and take $d_g = n/2$ and $d_h = (n-d)/2-1$. Let $F_f(\boldsymbol{a}, \boldsymbol{b}, x) \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ denote the polynomial family in (3.3.1), which is seen to have degree n. Again, for simplicity we denote this by $F(x)$ when it will not create confusion.

Proposition 3.3.2. *Fix a polynomial f, an even integer n, and degrees d_g, d_h as above. Then F_f is irreducible in $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ and $\mathrm{Gal}(F_f/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})) \simeq S_n$.*

Proof. We will again need that the irreducibility of F_f and its Galois group G are invariant under linear change of coordinates in x, to allow us to assume certain conditions on the valuations of the c_i.

As in the proof of Proposition 3.3.1, there exists a prime $p > n$ not dividing both $\mathrm{Disc}\, f, c_d$ such that p divides $f(k)$ exactly once for some integer k. Thus after changing variables, we assume that $v_p(c_0) = 1$.

Consider now the change of variables by scaling x to be px. The constant term c_0 remains unchanged, but this allows us to assume that $p \mid c_i$ for $i \geq 1$. These assumptions are useful for finding long cycles in $G = \mathrm{Gal}(F_f/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}))$. We consider an integral specialization $\boldsymbol{a}_0, \boldsymbol{b}_0$

with the following p-adic valuations:

$$\begin{aligned} v_p(a_i) &\geq 1 \text{ for } i < n/2 \\ v_p(a_{n/2}) &= 0 \\ v_p(b_0) &= 0, \end{aligned} \tag{3.3.8}$$

and no restrictions on b_j for $j > 0$. These restrictions, and assumptions on the coefficients c_i, ensure that every term of $F(x)$ is divisible by p, except for the leading coefficient $a_{n/2}^2$, which has valuation 0. Moreover, the valuation of the constant term $a_0^2 - b_0^2 c_0$ is exactly 1, so the Newton polygon of $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ has exactly one segment of length n and slope $-1/n$, as shown in Figure 3.3.7.

Figure 3.3.7: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with n-cycle

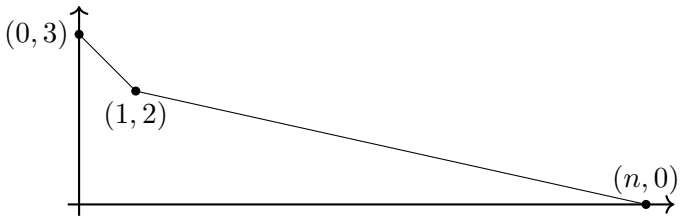
Proposition 2.1.28 implies that $F_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ is irreducible over $\mathbb{Q}_p$, and hence over $\mathbb{Q}$, so F is irreducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$ and G is transitive, containing an n-cycle by Corollary 3.2.4.

We use a variation of this argument to find an $(n-1)$-cycle in G. Fix another prime $p > n$ such that after a change of variables we have $v_p(c_0) = 1$ and $p \nmid c_1$. We consider an integral specialization $\boldsymbol{a}_0, \boldsymbol{b}_0$ with the following p-adic valuations:

$$\begin{aligned} v_p(a_i) &\geq 3 \text{ for } i < n/2 \\ v_p(a_{n/2}) &= 0 \\ v_p(b_0) &= 1 \\ v_p(b_j) &\geq 2 \text{ for } j > 0. \end{aligned} \tag{3.3.9}$$

These restrictions ensure that the constant term has valuation 3, while the linear coefficient, $2a_0a_1 - b_0^2c_1 - 2b_0b_1c_0$, has valuation exactly 2. All other terms have valuation at least 2 except for the leading term, which has valuation 0. This produces the Newton polygon below in Figure 3.3.8.

Figure 3.3.8: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with $(n-1)$-cycle



Since $n \geq 4$, the two segments are distinct, with the rightmost one of length $n-1$ and slope $-2/(n-1)$. As n is even, Proposition 2.1.28 is satisfied, producing an $(n-1)$-cycle in $G_{\boldsymbol{a}_0,\boldsymbol{b}_0}$ and thus in G.

Finally, we produce a transposition in G, assuming that $n \geq 8$ for simplicity; nearly identical arguments suffice for the case of $d = 4$ and $n = 6$. More care is needed here to find a Newton polygon with exactly one segment of even length to satisfy the hypotheses of Proposition 2.1.28.

Fix a prime $p > n$ such that $p \nmid c_d, \operatorname{Disc} f$, c_d is a quadratic residue modulo p, and $p \mid f(k)$ for some integer k. Such a prime exists by our earlier Chebotarev argument, this time looking for primes splitting completely in the splitting field of $f(x)(x^2 - c_d)$. After a change of coordinates, we assume $v_p(c_0) = 1$ and $p \nmid c_1$. We consider an integral specialization $\boldsymbol{a}_0, \boldsymbol{b}_0$ with the following restrictions:

$$
\begin{aligned}
v_p(a_i) &\geq 4 \text{ for } i < \frac{n}{2} - 2 \qquad (3.3.10)\\
v_p(a_{n/2-2}) &= 0\\
v_p(a_{n/2-1}) &= 1\\
v_p(a_{n/2}) &= 1 \text{ such that } \frac{a_{n/2}^2}{p^2} \equiv c_d \pmod{p^2}\\
v_p(b_0) &= 1\\
v_p(b_j) &\geq 1\\
v_p(b_{(n-d)/2}) &= 1 \text{ such that } \frac{b_{(n-d)/2}^2}{p^2} \equiv 1 \pmod{p^2}.
\end{aligned}
$$

Note that such $a_{n/2}$ exists, since c_d is a quadratic residue, and these assumptions ensure that $p^4 \mid a_{n/2}^2 - b_{(n-d)/2}^2 c_d$, the leading coefficient. Furthermore, we have that the constant

coefficient has valuation 3, the linear coefficient has valuation 2, the x^{n-4} coefficient has valuation 0, and both the x^{n-3} and x^{n-2} coefficients have valuation 1, with all other terms having valuation at least 2.

Looking more closely at the coefficient of x^{n-1} given by

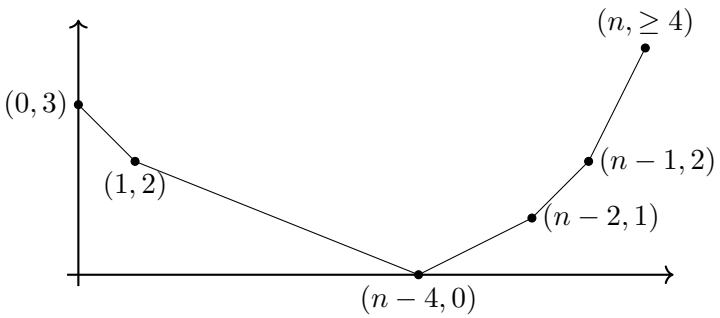
$$2a_{n/2-1}a_{n/2} - b_{(n-d)/2-1}b_{(n-d)/2}c_d - b_{(n-d)/2}^2 c_{d-1},$$

we see that its valuation at least 2. To ensure it has valuation exactly 2, we fix a residue class for $\frac{1}{p}b_{(n-d)/2-1}$ modulo p and ask that $a_{n/2-1}$ satisfy

$$\frac{a_{n/2-1}}{p} \not\equiv \left(2\frac{a_{n/2}}{p}\right)^{-1} \frac{1}{p^2}\left(b_{(n-d)/2-1}b_{(n-d)/2}c_d - b_{(n-d)/2}^2 c_{d-1}\right) \pmod{p}. \tag{3.3.11}$$

Thus combining (3.3.10) and (3.3.11), we produce the Newton polygon in Figure 3.3.9 below.

Figure 3.3.9: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0})$ with transposition



The segment of length 2 and slope 1/2, together with the fact that all other segments have odd length l' and slopes r'/l' with $\gcd(r', l') = 1$, allow us to apply Proposition 2.1.28 with $l = 2$ to produce a transposition in $G_{\boldsymbol{a}_0,\boldsymbol{b}_0}$. The requirements (3.3.10) and (3.3.11) are satisfied for a positive proportion of integral $\boldsymbol{a}_0, \boldsymbol{b}_0$, so Corollary 3.2.4 implies that G contains a transposition. Thus with its n-cycle, $(n-1)$-cycle, and transposition, Proposition 2.2.18 gives that $G \simeq S_n$. □

3.4 Polynomial families from superelliptic curves

We now return to the case of a superelliptic curve for general $m \geq 2$. Recall our restrictions on d and $f(x)$ out of convenience. First, we assume $d = \deg f(x)$ is divisible by m; this corresponds to the superelliptic map $C_f \to \mathbb{P}^1$ being unramified at infinity. We also ask for $f(x) \neq f_0(x)^e$ for any nontrivial divisor $e \mid m$. This is automatic if we enforce that the curve C_f is geometrically irreducible.

Proposition 3.4.1. *Fix a polynomial $f(x)$ as above and an integer $n \geq \max(d, \mathrm{Frob}(m, d)+1)$ such that $m \mid n$. Let the degrees d_g, d_h, d_γ as in (3.2.2). Then F_f is irreducible in $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})[t]$.*

Moreover, for 100% of specializations $\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0$ we have $F_{\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0} \in \mathbb{Q}[t]$ is irreducible of degree n.

Remark 3.4.2. Note that unlike Propositions 3.3.1 and 3.3.2, we make no claims about the Galois group $G = \mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha}))$. From irreducibility it follows that G is transitive, but identifying elements in the Galois group using a similar Newton polygon proves somewhat more difficult. For now we content ourselves with irreducibility, but we see no reason not to suspect $G \simeq S_n$ in general.

Proof of Proposition 3.4.1. The second statement follows from the first by Hilbert irreducibility, Lemma 3.2.3.

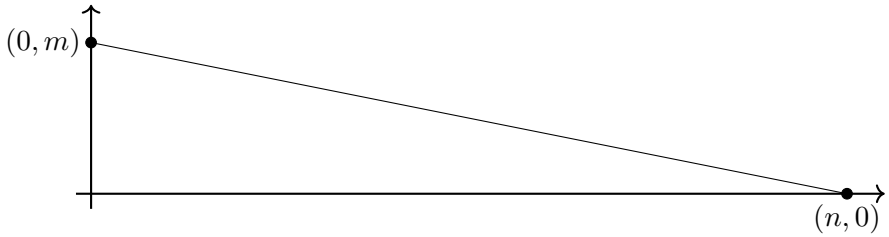
For the first statement, we exhibit specializations with incompatible p-adic factorizations for several primes p, arguing via Newton polygons and Lemma 2.1.26.

Fix a prime p such that $p \nmid c_i$ for all i. Consider an integral specialization $\boldsymbol{a}_0, \boldsymbol{b}_0, \boldsymbol{\alpha}_0$ satisfying

$$\begin{aligned} v(a_0) &= 1 \\ v(a_i) &\geq 1 \text{ for } 0 < i < n/m \\ v(a_{n/m}) &= 1 \\ v(b_j) &\geq 1 \text{ for } 0 \leq j \leq (n-d)/m, \end{aligned} \tag{3.4.1}$$

with no restrictions on α_0, α_1. We end up with the Newton polygon featured below.

Figure 3.4.1: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0,\boldsymbol{\alpha_0}})$ with one segment of slope $-m/n$



In particular, since we have assumed $m \mid n$, we have that $m = \gcd(m, n)$ so by Lemma 2.1.26, all irreducible factors of F over $\mathbb{Q}_p$ must have degree divisible by $\frac{n}{m}$.

Consider now an alternative specialization. By Corollary 2.3.11 there are infinitely many primes p such that for some $\alpha_0 \in \mathbb{Z}$ we have $f(\alpha_0)$ is divisible by p exactly e times, where e the multiplicity of an irreducible factor of $f(x) = \prod_i f_i(x)^{e_i}$. Note that we may not be able to enforce $e = 1$ as we did in §3.3 since f may not be squarefree, or even have an irreducible factor of multiplicity one.

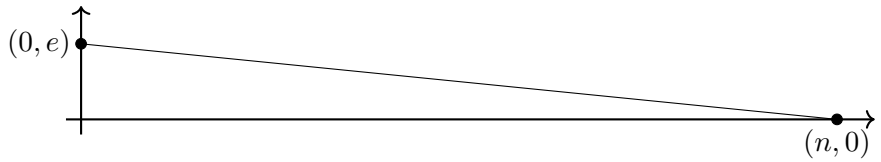
Choose some such p and α_0 such that $p \nmid c_i$ for all i. Set $\gamma(t) = p^e t + \alpha_0$, so that p^e exactly divides the constant term $f(\alpha_0)$ of $f(\gamma(t))$ and all higher coefficients are divisible by p. Consider now a specialization satisfying

$$\begin{aligned} v(a_i) &\geq e \text{ for } 0 \leq i < n/m \\ v(a_{n/m}) &= 0 \\ v(b_0) &= 0 \\ v(b_j) &\geq 0 \text{ for } 0 \leq j \leq (n-d)/m. \end{aligned} \tag{3.4.2}$$

This ensures that p^e exactly divides the constant term of F and all other terms except the leading term, yielding the Newton polygon below.

As earlier, Lemma 2.1.26 implies that the an irreducible factor of F over $\mathbb{Q}_p$ must have degree a multiple of $\frac{n}{\gcd(n,e)}$.

Figure 3.4.2: $\mathrm{NP}_{\mathbb{Q}_p}(F_{\boldsymbol{a}_0,\boldsymbol{b}_0,\boldsymbol{\alpha}_0})$ with one segment of slope $-e/n$



Let F_0 be an irreducible factor of F. We have seen that

$$\frac{n}{m} \;\Big|\; \deg F_0 \quad \text{and} \quad \frac{n}{\gcd(n, e_i)} \;\Big|\; \deg F_0 \text{ for } 1 \le i \le r.$$

Starting with $i = 1$, we apply an elementary fact, stated and proven below in Lemma 3.4.3, with $a = m$ and $b = \gcd(n, e_i)$, giving

$$\frac{n}{\gcd(m, \gcd(n, e_1))} = \frac{n}{\gcd(n, m, e_1)} \;\Big|\; \deg F_0.$$

Applying again for $2 \le i \le r$ with $a = \gcd(n, m, e_1, \ldots, e_{i-1})$ and $b = \gcd(n, e_i)$ we obtain

$$\frac{n}{\gcd(n, m, e_1, \ldots, e_r)} = \frac{n}{1} \;\Big|\; \deg F_0$$

by our assumptions on the multiplicities e_i, coming from the irreducibility of C_f. Hence F is irreducible over $\mathbb{Q}$. □

Lemma 3.4.3. *Suppose $\frac{n}{a}, \frac{n}{b} \mid d$ for some integers n, d, a, b such that $a, b \mid n$. Then $\frac{n}{\gcd(a,b)} \mid d$.*

Proof. Recall the elementary identity $\gcd(a, b)\,\mathrm{lcm}(a, b) = ab$. We have

$$\frac{n}{a} \mid d \implies \frac{n}{\gcd(a, b)} \;\Big|\; d\frac{\mathrm{lcm}(a, b)}{b},$$

and similarly $\frac{n}{\gcd(a,b)} \mid d\frac{\mathrm{lcm}(a,b)}{a}$.

Since $\frac{\mathrm{lcm}(a,b)}{a} = \frac{b}{\gcd(a,b)}$ and $\frac{\mathrm{lcm}(a,b)}{b} = \frac{a}{\gcd(a,b)}$ are coprime, any prime factor $p \mid \frac{n}{\gcd(a,b)}$ must divide d, and the conclusion follows. □

3.5 Accounting for multiplicity

In this section, we describe how to obtain an asymptotic lower bound for $N_{n,C_f}(X)$ or $N_{n,C_f}(X, S_n)$ in our cases of interest by counting polynomials and accounting for the multiplicity of the fields that they generate.

Proposition 3.5.1. *Fix m, f, and n divisible by $\gcd(m, d)$ and suppose F as given in (3.2.1) is irreducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})$. Then we have*

$$N_{n,C_f}(X) \gg X^{\delta_n},$$

where

$$\delta_n = \tfrac{1}{m^2} + \tfrac{2n^2(m-m^2-dr+3)+n(km-k^2+4(m-m^2-dr)-dmr+d^2r^2)+2(km-k^2-dmr+d^2r^2)}{2m^2n^2(n-1)}. \quad (3.5.1)$$

Here we take $r = \deg \gamma$ to be the minimal positive integer such that $n \equiv dr \pmod m$ as in Proposition 3.2.2, and

$$k = \begin{cases} \min\{k_1 \in \mathbb{Z}_{\geq 0} \mid \frac{n-d-k_1}{m} \in \mathbb{Z}\} & m \mid n, \\ \min\{k_2 \in \mathbb{Z}_{>0} \mid \frac{n-k_2}{m} \in \mathbb{Z}\} & m \nmid n. \end{cases}$$

Moreover, if $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})) \simeq S_n$ then

$$N_{n,C_f}(X, S_n) \gg X^{\delta_n}.$$

Theorems 3.1.2, 3.1.3, 3.1.5 follow from Proposition 3.5.1 combined with one of Proposition 3.3.1, 3.3.2, or 3.4.1, as appropriate, to ensure F satisfies the relevant irreducibility and Galois group hypotheses. The improved exponents in the large n case follow from the discussion in 3.5.4.

3.5.1 Coefficient bounds

In this section, we construct a family of polynomials $P_{f,n}(Y)$ arising from certain specializations of (3.2.1) in §3.2. We will do this by imposing bounds on the coefficients of $g(t)$ and $h(t)$ in $F(t) = g(t)^m - h(t)^m f(\gamma(t))$. These bounds will be useful for counting multiplicities of fields generated by this family of polynomials because of the following lemma that relates the absolute values of the coefficients of a polynomial to the absolute values of its roots.

Lemma 3.5.2. *Let $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{C}[x]$ be monic and have degree n. There exist positive constants A_i such that for any $Y > 0$, if $|c_i| \leq A_i Y^{n-i}$ for $0 \leq i \leq n$ then $|\alpha| \leq Y$ for all roots α of $f(x)$.*

Proof. The result follows from a bound of Fujiwara [Fuj16], see [Key22, Lemma 4.1]. □

For the remainder of this section, we work with the hypotheses of Proposition 3.5.1, namely that C_f is a nonsingular superelliptic curve, n is a fixed sufficiently large multiple of $\gcd(m, d)$, and $F \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})[t]$ given in Proposition 3.2.2 is irreducible (possibly with Galois group S_n).

It will be useful to specialize $\boldsymbol{\alpha}$ to $\boldsymbol{\alpha}_0$, or equivalently to choose some $\gamma_0(t) \in \mathbb{Z}[t]$, so that $F_{\alpha_0} \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ is irreducible (possibly with Galois group S_n).

Lemma 3.5.3. *Assume the same hypotheses as Proposition 3.5.1. Then there exists $\boldsymbol{\alpha}_0 \in \mathbb{Z}^{r+1}$, for which the partial specialization $F_{\boldsymbol{\alpha}_0} \in \mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})[t]$ is irreducible and such that $f(\gamma_0(t))$ is also m-th power free.*

Moreover, if $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})) \simeq S_n$ then $\boldsymbol{\alpha}_0$ may be chosen such that the partial specialization also has full Galois group $\mathrm{Gal}(F_{\boldsymbol{\alpha}_0}/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})) \simeq S_n$.

Proof. By assumption, we have that F is irreducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})$. Hilbert's irreducibility theorem (Lemma 3.2.3 but for arbitrary base field) implies that for almost all choices of $\boldsymbol{\alpha}_0$, $F_{\boldsymbol{\alpha}_0}$ is irreducible over $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})$. If $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})) \simeq S_n$ then for almost all $\boldsymbol{\alpha}_0$ we have $\mathrm{Gal}(F_{\boldsymbol{\alpha}_0}/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b})) \simeq S_n$.

Let us know examine more closely when $f(\gamma_0(t))$ is also m-th power free. Writing f as a product of irreducible factors $f = \prod_i f_i^{e_i}$ and taking $f_{\mathrm{rad}} = \prod_i f_i$, it is enough to check that we can choose γ_0 such that $f_{\mathrm{rad}}(\gamma_0(t))$ is *squarefree*.

Now we may use the discriminant $\operatorname{Disc} f_{\mathrm{rad}}(\gamma(t))$, viewed as a polynomial function in variables $\boldsymbol{\alpha}$; $f_{\mathrm{rad}}(\gamma(t))$ has a multiple root whenever this polynomial vanishes, which is a Zariski closed condition on the affine space $\mathbb{A}^{r+1}$ from which we are choosing $\boldsymbol{\alpha}_0$. Hence the space of $\boldsymbol{\alpha}_0$ giving rise to γ_0 with $f_{\mathrm{rad}}(\gamma_0(t))$ squarefree — and thus $f(\gamma_0(t))$ m-th power free — is Zariski dense. In particular, some such α_0 satisfies both F_{α_0} irreducible and $f(\gamma_0(t))$ m-th power free. □

Moving forward, we fix some $\gamma_0(t) \in \mathbb{Z}[t]$ such that $F_{\boldsymbol{\alpha}_0}$ is irreducible (with Galois group S_n if appropriate) and $f(\gamma_0)$ m-th power free, by Lemma 3.5.3.

We now take Y to be a a positive real number. Let $P_{f,n}(Y)$ be the set of polynomials of the form

$$F(t) = h(t)^m f(\gamma_0(t)) - g(t)^m$$

that arise from certain integral specializations of (3.2.1) for which we will give certain constraints on $g(t)$ and $h(t)$ below depending on Y. That is, $P_{f,n}(Y)$ is a set of integral specializations $F_{\boldsymbol{a}_0,\boldsymbol{b}_0,\boldsymbol{\alpha}_0}$ where the choice of Y imposes constraints on $\boldsymbol{a}_0, \boldsymbol{b}_0$ and $\boldsymbol{\alpha}_0$ is precisely the coefficients of γ_0. We write the coefficients of $F(t)$ as follows:

$$F(t) = d_n t^n + d_{n-1} t^{n-1} + \cdots + d_0. \tag{3.5.2}$$

In order to apply Lemma 3.5.2, we need bounds on the coefficients d_i in terms of Y. To achieve this, we impose restrictions on the coefficients of g and h. In the case where $m \mid n$ we take

$$\begin{aligned} g(t) &= a_{n/m} t^{n/m} + a_{n/m-1} t^{n/m-1} + \cdots + a_0, \\ h(x) &= b_{(n-d-k_1)/m} t^{(n-d-k_1)/m} + b_{(n-d-k_1)/m-1} t^{(n-d-k_1)/m-1} + \cdots + b_0, \\ f(\gamma_0(t)) &= c'_d x^d + \cdots + c'_1 x + c'_0. \end{aligned} \tag{3.5.3}$$

Here k_1 is the minimal nonnegative integer such that $(n-d-k_1)/m$ is an integer. This realizes the degrees in (3.2.2). Fix $a_{n/m}$ to be an integer so that the partial specialization $F_{a_{n/m},\boldsymbol{\alpha}}$ is irreducible (and $\operatorname{Gal}(F_{a_{n/m},\boldsymbol{\alpha}_0}, \mathbb{Q}(\boldsymbol{a},\boldsymbol{b})) \simeq S_n$ if appropriate). Such $a_{n/m}$ exists by

Lemma 3.2.3. If $k_1 = 0$, we similarly take $b_{(n-d)/m}$ such that $F_{a_{n/m},b_{(n-d)/m},\boldsymbol{\alpha}_0}$ is irreducible (and $\mathrm{Gal}(F_{a_{n/m},b_{(n-d)/m},\boldsymbol{\alpha}_0}/\mathbb{Q}(\boldsymbol{a},\boldsymbol{b})) \simeq S_n$ if appropriate). We then impose the restrictions that a_i, b_j are integers satisfying $|a_{n/m-i}| \leq Y^i$ for $i > 0$, and $|b_{(n-d-k_1)/m-j}| \leq Y^{k_1/m+j}$ for $j > 0$, with $|b_{(n-d-k_1)}| \leq Y^{k/m}$ if $k_1 \neq 0$.

In the case where $m \nmid n$, we choose r, the degree of $\gamma(t)$, to be the minimal positive integer for which $n \equiv dr \pmod{m}$. As above, we have

$$\begin{aligned} g(t) &= a_{(n-k_2)/m}t^{(n-k_2)/m} + a_{(n-k_2)/m-1}t^{(n-k_2)/m-1} + \cdots + a_0, \\ h(t) &= b_{(n-dr)/m}t^{(n-dr)/m} + b_{(n-dr)/m-1}t^{(n-dr)/m-1} + \cdots + b_0, \\ f(\gamma_0(t)) &= c'_d t^{dr} + \cdots + c'_1 x + c'_0. \end{aligned} \tag{3.5.4}$$

Here k_2 is the minimal positive integer such that $(n-k_2)/m$ is an integer so this realizes the degrees in (3.2.3). This time, we use Lemma 3.2.3 to find an integer $b_{(n-dr)/m}$ such that the partial specialization $F_{b_{(n-dr)/m},\boldsymbol{\alpha}_0}$ is irreducible (with $\mathrm{Gal}(F_{b_{(n-dr)/m},\boldsymbol{\alpha}_0}/\mathbb{Q}(\boldsymbol{a},\boldsymbol{b})) \simeq S_n$ if appropriate). We then impose the restrictions that a_i, b_j are integers satisfying $|a_{(n-k_2)/m-i}| \leq Y^{k_2/m+i}$ for $i \geq 0$, and $|b_{(n-dr)/m-j}| \leq Y^j$ for $j > 0$.

We note that these polynomials $F \in P_{f,n}(Y)$ have degree n, and these restrictions on the coefficients imply that $|d_i| \ll A_i Y^{n-i}$. Applying Lemma 3.5.2 and accounting for the implied constant, we see that for all $F \in P_{f,n}(Y)$, we have that all roots α of F satisfy $|\alpha| \ll_{n,f} Y$ and thus we also have $|\mathrm{Disc}(F)| \leq BY^{n(n-1)}$ for a constant B depending on f and n.

3.5.2 Bounding multiplicities

We bound the number of fields arising from specializations in (3.2.1) by counting the number of polynomials in $P_{f,n}(Y)$ and adjusting for two possible sources of multiplicity. The first potential source of multiplicity is the case where two different $g(t)$, $h(t)$ give rise to the same element $F(t)$ in $P_{f,n}(Y)$. The second potential source of multiplicity is that multiple elements $F(t)$ in $P_{f,n}(Y)$ produce isomorphic number fields. The first potential source of multiplicity is dealt with by the following lemma, building on the strategy in [LT21, Lemma 7.4].

Lemma 3.5.4. *Let $F(t) \in \mathbb{Z}[t]$ be a polynomial of degree n. The number of ways to choose nonzero polynomials $g(t), h(t) \in \mathbb{Z}[t]$ of some fixed degrees $\deg g \leq \frac{n}{m}$ and $\deg h < \frac{n}{m}$ with one of the leading coefficients of g or h fixed, such that $F(t) = g(t)^m - f(\gamma_0(t))h(t)^m$ is $O_{m,n}(1)$.*

Proof. Note that we assumed $f(x)$ is m-th power free in our definition of a superelliptic curve in (3.1.2). We then chose $\gamma_0(t)$ as in Lemma 3.5.3 such that $f(\gamma_0(t))$ is also m-th power free. The coordinate ring $R = \mathbb{C}[t, y]/(y^m - f(\gamma_0(t)))$ is a Noetherian domain of Krull dimension one, thus its integral closure $\widetilde{R}$ is a Dedekind domain (see e.g. [Lan94, Ch. 1, §6, Theorem 2]). Thus in $\widetilde{R}$, the ideal (F) factors uniquely into a product of finitely many primes, of the form $(t - t_0, y - y_0)$ satisfying both $y_0 = f(\gamma(t_0))$ and $F(t_0) = 0$. There are mn such solutions, counted with multiplicity, so we have at most mn prime factors of (F).

As in the proof of [LT21, Lemma 7.4], we observe that given any such g, h there is a factorization

$$F = g^m - f(\gamma_0)h^m = \prod_{i=0}^{m-1} \left(g - \zeta^i f(\gamma_0)^{1/m} h\right),$$

where ζ is a primitive m-th root of unity. The ideal $(g - f(\gamma_0)^{1/m}h)$ divides (F) so there are at most 2^{mn} possibilities for its prime factorization. Thus there are at most 2^{mn} choices for the ideal $(g - f(\gamma_0)^{1/m}h)$. It remains to show that if g and h satisfy the hypotheses of the lemma, this ideal determines them precisely.

Suppose we have g', h' satisfying the hypotheses with $(g - f(\gamma_0)^{1/m}h) = (g' - f(\gamma_0)^{1/m}h')$. Then for some unit $u \in \widetilde{R}^\times$, we have $g - f(\gamma_0)^{1/m}h = u(g' - f(\gamma_0)^{1/m}h')$. This unit u necessarily satisfies a minimal monic polynomial

$$u^k + v_{k-1}u^{k-1} + \cdots + v_1 u + v_0 = 0, \tag{3.5.5}$$

where $v_i \in R$ and $v_0 \in R^\times$. Multiplying by $g' - f(\gamma_0)^{1/m}h'$, this becomes

$$\begin{aligned} 0 &= \left(g' - f(\gamma_0)^{1/m}h'\right)\left(u^k + v_{k-1}u^{k-1} + \cdots + v_1 u + v_0\right) \\ &= (g - f(\gamma_0)^{1/m}h)\left(u^{k-1} + v_{k-1}u^{k-2} + \cdots + v_1\right) + v_0\left(g' - f(\gamma_0)^{1/m}h'\right). \end{aligned}$$

If $k > 1$ then this contradicts minimality of (3.5.5), so we must have $k = 1$, in which case we have $u \in R^\times$.

With this in hand, we may write $u = u(t)$ as

$$u(t) = \sum_{i=0}^{m-1} f(\gamma_0(t))^{i/m} u_i(t)$$

with $u_i(t) \in \mathbb{C}[t]$. The relation $u(g - f(\gamma_0)^{1/m}h) = g' - f(\gamma_0)^{1/m}h'$ implies

$$\begin{aligned} u_0 g - u_{m-1} f(\gamma_0) h &= g' \\ u_1 g - u_0 h &= h' \\ u_2 g - u_1 h &= 0 \\ &\vdots \\ u_i g - u_{i-1} h &= 0 \quad \text{for all } 2 \le i \le m-1 \\ &\vdots \\ u_{m-1} g - u_{m-2} h &= 0 \end{aligned} \tag{3.5.6}$$

as polynomials in $\mathbb{C}[t]$. Multiplying each line by appropriately by powers of g and/or h, we determine

$$u_{m-1} F = u_{m-1}(g^m - h^m f(\gamma_0)) = g' h^{m-1} + g h^{m-2} h'. \tag{3.5.7}$$

If $u_{m-1} \neq 0$, the left hand side has degree $\deg u_{m-1} + n$, while the right hand side has degree at most $\deg g + (m-1)\deg h < n$, producing a contradiction. Therefore, we have $u_{m-1} = 0$, and tracing through the relations, this implies $u_i = 0$ for all $1 \le i \le m-1$, i.e. $u(t) = u_0(t)$.

Finally, we observe that since the degrees of g and h are fixed, $u = u_0$ must be a constant. Moreover, since we also require the leading coefficients of either g, g' or h, h' to be fixed, we must have $u = 1$. Therefore, the ideal $(g - f(\gamma_0)^{1/m}h)$ can come from at most one g, h satisfying the hypotheses. □

When $m \mid n$, the restrictions imposed in (3.5.3) and the following discussion fix the

degrees of g and h and the leading coefficient of g such that the hypotheses of Lemma 3.5.4 are satisfied. Thus each choice of $g(t)$ and $h(t)$ coincides with at most finitely many others. The same is true for the $m \nmid n$ case by (3.5.4). Thus we can give a count for the number of $F(t)$ in $P_{f,n}(Y)$ based on the number of choices for $g(t)$ and $h(t)$. More precisely, $\#P_{f,n}(Y) \asymp Y^c$ for c to be determined below.

In the case where $m \mid n$, we have

$$c = \sum_{i=1}^{n/m} i + \sum_{j=0}^{(n-d-k_1)/m} \left(j + \frac{k_1}{m}\right) = \frac{1}{m^2}\left(n^2 + n(m-d) + \frac{d^2 + (k_1-d)m - k_1^2}{2}\right). \quad (3.5.8)$$

In the case where $m \nmid n$, we have

$$c = \sum_{i=0}^{(n-k_2)/m} \left(\frac{k_2}{m} + i\right) + \sum_{j=1}^{(n-rd)/m} j = \frac{1}{m^2}\left(n^2 + n(m-dr) + \frac{d^2r^2 + (k_2-dr)m - k_2^2}{2}\right). \quad (3.5.9)$$

Let $P_{f,n}(Y, \mathrm{irr})$ denote the subset of $P_{f,n}(Y)$ consisting of irreducible polynomials. Similarly, let $P_{f,n}(Y, S_n)$ denote the subset of irreducible polynomials with Galois group S_n over $\mathbb{Q}$. Since we have assumed F is irreducible and chosen $a_{n/m}$ or $b_{(n-dr)/m}$ appropriately, Lemma 3.5.3 implies that $\#P_{f,n}(Y, \mathrm{irr}) \asymp Y^c$. Similarly, $\#P_{f,n}(Y, S_n) \asymp Y^c$ if F has symmetric Galois group.

To address the second source of potential multiplicity (that there may be multiple elements of $F(t)$ that produce isomorphic number fields), we use a strategy of Ellenberg and Venkatesh [EV06] for counting number fields, and the multiplicity counts of Lemke Oliver and Thorne [LT21]. See also [Key22, §5] for a detailed discussion.

As mentioned previously our assumptions on the sizes of $|a_i|$, $|b_j|$ ensure that the coefficients of (3.5.2) are bounded by $|d_{n-i}| \leq AY^i$ for some constant A. In particular the leading terms are bounded, and hence we may divide by some constant integer w. We define the set

$$S(Y) := \left\{F = t^n + d'_{n-1}t^{n-1} + \ldots + d'_0 \in (1/w)\mathbb{Z}[t] : \left|d'_{n-i}\right| \ll_{n,f} Y^i\right\}$$

with the additional condition that $F(t)$ is irreducible. Note that by this construction, elements of $P_{f,n}(Y, \mathrm{irr})$ (and $P_{f,n}(Y, S_n)$) are in bijection with a subset of $S(Y)$, provided

we choose the implied constant appropriately.

We define the multiplicity of a number field K of degree n in $S(Y)$ to be the number of polynomials in $S(Y)$ that cut out the field K,

$$M_K(Y) := \#\left\{F \in S(Y) \mid \mathbb{Q}[t]/F(t) \simeq K\right\}.$$

We state here several bounds related to this multiplicity $M_K(Y)$ that we will use to compute bounds on $N_{n,C}(X, S_n)$. The following is a bound of Lemke Oliver and Thorne on $M_K(Y)$.

Lemma 3.5.5 (Lemke Oliver–Thorne [LT21, Proposition 7.5])**.** *We have*

$$M_K(Y) \ll \max\left(Y^n \left|\mathrm{Disc}(K)\right|^{-1/2}, Y^{n/2}\right).$$

The proof of this lemma uses the geometry of numbers, building on the strategy suggested in [EV06].

This bound of Lemke Oliver and Thorne for $M_K(Y)$ together with the following theorem of Schmidt on general number field counts with bounded discriminant are used in [Key22] to give a bound for the sum of multiplicities of fields with discriminant bounded by T.

Theorem 3.5.6 (Schmidt, [Sch95])**.** *For $n \geq 3$, we have*

$$N_n(X) \ll X^{\frac{n+2}{4}}. \tag{3.5.10}$$

Lemma 3.5.7 (K., [Key22, Lemma 5.4])**.** *Let $T \leq Y^n$. Then*

$$\sum_{|\mathrm{Disc}(K)| \leq T} M_K(Y) \ll Y^n T^{n/4},$$

where the sum runs over all degree n number fields K such that $|\mathrm{Disc}(K)| \leq T$.

Remark 3.5.8. Schmidt's bound in Theorem 3.5.6 has been superseded both in the large and intermediate degree case, meaning Lemma 3.5.7 could be improved. However, we defer this discussion until §3.5.4, where we discuss how better upper bounds for $N_n(X)$ improve our lower bound on $N_{n,C}(X)$ for n sufficiently large.

3.5.3 Bounding $N_{n,C}(X, S_n)$

We now have all the tools to prove Proposition 3.5.1.

Proof of Proposition 3.5.1. By our construction, for any $F \in P_{f,n}(Y, \text{irr})$ and any root α of F, we have $(\alpha, \frac{g(\alpha)}{h(\alpha)}) \in C_f(K)$ where $K = \mathbb{Q}(\alpha)$ is a field of degree n. Recall also that we have $|\text{Disc}(K)| \leq BY^{n(n-1)}$ for a constant B. Roughly speaking, we are taking our count for the polynomials and dividing by a bound for the multiplicity (i.e. the number of polynomials per field) to get the number of fields.

First, we will show fields of low discriminant are negligible in their contributions to $N_{n,C}(X)$. Using Lemma 3.5.7, we choose $T = \kappa Y^{\frac{1}{m^2}(4n-4(dr+(m-1)m)+(2(dr-k)(dr+k-m))/n)}$ so that

$$\sum_{|\text{Disc}(K)| \leq T} M_K(Y) \ll \kappa^{n/4} Y^c, \tag{3.5.11}$$

and we recall that

$$\#P_{f,n}(Y, \text{irr}) \asymp Y^c \tag{3.5.12}$$

where c is given either by (3.5.8) or (3.5.9). We choose κ to be sufficiently small so that the quantity in 3.5.11 is at most $\#P_{f,n}(Y, \text{irr})/2$. Thus we produce negligibly many fields of discriminant at most T. Since the bound in Lemma 3.5.5 is decreasing with respect to $|\text{Disc}(K)|$, we have $M_K(Y) \ll T^{-1/2}Y^n$ for all K of discriminant $T < |\text{Disc}(K)| \leq BY^{n(n-1)}$. We obtain a lower bound for $N_{n,C}(BY^{n(n-1)})$ by dividing $\#P_{f,n}(Y, \text{irr})$ by this worst case multiplicity.

$$\begin{aligned} N_{n,C}(BY^{n(n-1)}) &\gg Y^{c-n}T^{1/2} \\ &= Y^{\frac{1}{m^2}\left(n^2+n(2+m-m^2-dr)+(-k^2+4m+km-4m^2-4dr-dmr+d^2r^2)/2+(d^2r^2-k^2+km-dmr)/n\right)}. \end{aligned} \tag{3.5.13}$$

To obtain the exponent δ_n in (3.1.3), we replace Y in (3.5.13) by $(X/B)^{1/n(n-1)}$. This

produces (3.5.1)

$$\delta_n = \tfrac{1}{m^2} + \tfrac{2n^2(m-m^2-dr+3)+n(km-k^2+4(m-m^2-dr)-dmr+d^2r^2)+2(km-k^2-dmr+d^2r^2)}{2m^2n^2(n-1)}$$

and thus $N_{n,C}(X) \gg X^{\delta_n}$, as desired.

In the case $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{\alpha})) \simeq S_n$, no changes to the above strategy are required, since $P_{f,n}(Y, S_n) \asymp Y^c$ as well. □

3.5.4 Improvements for n sufficiently large

As in [Key22, §5.4], we can improve on our lower bound when n is sufficiently large by employing better known upper bounds for $N_n(X)$. The idea is to show that if the upper bound for $N_n(X)$ is good enough, then the best case scenario of Lemma 3.5.5 applies, and we can assume $M_K(Y) \ll Y^{n/2}$. Thus

$$N_n(Y^{n(n-1)}) \gg Y^{c-\frac{n}{2}}$$

where c is given in (3.5.8) or (3.5.9), as appropriate. It remains to compute this exponent and determine when the improved upper bounds for $N_n(X)$ take effect.

Assume we have an upper bound of the form

$$(*) \quad N_n(X) \ll X^{\varepsilon(n,m,d)},$$

where $\varepsilon(n,m,d) \geq 1$ is a constant depending on n and the m, d values for our curve C. We will use a modification of (the proof of) Lemma 5.5 which is somewhat more flexible.

Lemma 3.5.9. *Let $T \leq Y^n$. Assume $(*)$ for some constant $\varepsilon(n,m,d)$. Then*

$$\sum_{|\mathrm{Disc}\, K| \leq T} M_K(Y) \ll Y^n T^{\varepsilon(n,m,d)-1/2} + \frac{Y^n T^{\varepsilon(n,m,d)-\frac{1}{2}}}{2\varepsilon(n,m,d)-1}.$$

In particular, when we take $T = Y^n$ we have

$$\sum_{|\mathrm{Disc}\, K| \leq Y^n} M_K(Y) \ll Y^{\frac{n}{2}+n\varepsilon(n,m,d)}.$$

Proof. Write

$$M(Y)(t) = \max\{M_K(Y) : |\mathrm{Disc}\, K| = t\}$$

for the maximal multiplicity of a number field with discriminant t. Note that the bound in Lemma 3.5.5 depends only on the discriminant so we have $M(Y)(t) \ll \max\left(Y^n t^{-1/2}, Y^{n/2}\right)$. We set up a Riemann-Stieljes integral as in [Key22, Lemma 5.4],

$$\begin{aligned}\sum_{|\mathrm{Disc}\, K| \leq T} M_K(Y) &\leq \int_{1^-}^{T} M(Y)(t) dN_n(t) \\ &\ll \int_{1^-}^{T} Y^n t^{-\frac{1}{2}} dN_n(t) \\ &= Y^n T^{-\frac{1}{2}} N_n(T) + \frac{Y^n}{2} \int_{1^-}^{T} t^{-\frac{3}{2}} N_n(t) dt.\end{aligned}$$

Substituting $(*)$ into the last line above gives the first statement of the lemma. □

Note that Lemma 3.5.7 follows from this by taking $\varepsilon(n,m,d) = \frac{n+2}{4}$ as in (3.5.10), Schmidt's bound [Sch95]. However, this is not good enough for $Y^{\frac{n}{2}+n\varepsilon(n,m,d)}$ to be $o(Y^c)$. For this we need

$$(**) \quad \varepsilon(n,m,d) < \frac{c}{n} - \frac{1}{2}.$$

Using the best known upper bounds we can find when $(**)$ is satisfied for a given C and n.

Theorem 3.5.10 (Lemke Oliver–Thorne, [LT22, Theorem 1.1])**.** *For $n \geq 6$ we have*

$$N_n(X) \ll X^{1.564(\log n)^2}.$$

This is sufficient to give the proof of (3.1.4) in Theorem 3.1.5, which we state as a corollary.

Corollary 3.5.11. *Fix m, f and suppose that for all sufficiently large n, F as given in*

(3.2.1) *is irreducible over* $\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha})$. *Then for* $n \gg 0$ *we have*

$$N_{n,C_f}(X) \gg X^{\delta'_n},$$

where

$$\delta'_n = \frac{1}{m^2}\left(1 + \frac{(2m - 2dr + 1)n + d^2r^2 - mdr + mk - k^2}{2n(n-1)}\right).$$

Here r, k *are defined as in Proposition 3.5.1.*

Moreover, if for all sufficiently large n, $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha}) \simeq S_n$, *then for* $n \gg 0$ *we have*

$$N_{n,C_f}(X, S_n) \gg X^{\delta'_n}.$$

Proof. Fix a choice of C_f, so m and d are fixed. Assume $n \geq 6$ and set $\varepsilon(n, m, d) = 1.564(\log n)^2$, so Theorem 3.5.10 ensures $(*)$ is satisfied. Recalling c from (3.5.8) or (3.5.9) we see that in either case, $\frac{c}{n} - \frac{1}{2}$ grows linearly with n, as k_1, k_2, and/or r are bounded, depending on m, d. Clearly $(\log n)^2$ grows more slowly with n, so for n sufficiently large $(**)$ is satisfied.

As noted above, Lemma 3.5.9 together with $(*), (**)$ implies that

$$\sum_{|\mathrm{Disc}\, K| \leq Y^n} M_K(Y) = o(Y^c).$$

Thus the contribution of fields with discriminant up to Y^n to $\#P_{f,n}(Y, \mathrm{irr})$ is negligible. For fields K with $Y^n < |\mathrm{Disc}\, K| \leq Y^{n(n-1)}$ we have $M_K(Y) \ll Y^{n/2}$ by Lemma 3.5.5. Hence, we have

$$N_{n,C_f}(Y^{n(n-1)}) \gg \#P_{f,n}(Y, S_n)Y^{-\frac{n}{2}} \gg Y^{c-\frac{n}{2}}.$$

To get δ'_n we set $Y = X^{\frac{1}{n(n-1)}}$ and take $\delta'_n = \frac{c-n/2}{n(n-1)}$, which we can compute explicitly to obtain the stated value.

The same argument applies for $N_{n,C_f}(X, S_n)$ since $\#P_{f,n}(Y, S_n) \asymp Y^c$. □

The question remains to find when the improved asymptotic lower bound above takes effect; that is, to determine when $(*)$ and $(**)$ are both satisfied. To do this, we make use

of a more flexible version upper bound of Lemke Oliver and Thorne, which we state below with some variables changed to avoid confusion with our notation.

Theorem 3.5.12 (Lemke Oliver–Thorne, [LT22, Theorem 1.2])**.** *Let $n \geq 2$.*

1. *Let a be the least integer for which $\binom{a+2}{2} \geq 2n+1$. Then*

$$N_n(X) \ll X^{2a-\frac{a(a-1)(a+4)}{6n}}.$$

2. *Let $3 \leq b \leq n$ and let a be such that $\binom{a+b-1}{b-1} > bn$. Then*

$$N_n(X) \ll X^{ab}.$$

For a fixed superelliptic curve, i.e. choice of m and d, we aim to find an integer N such that for all $n \geq N$ satisfying $\gcd(m,d) \mid n$ and the irreducibility (or Galois group) hypothesis, Corollary 3.5.11 is true. Below we summarize this procedure.

1. Set $\varepsilon(n,m,d) = 1.564(\log n)^2$ and find N_0 such that $(**)$ is satisfied for all $n \geq N_0$. ($(*)$ satisfied by Theorem 3.5.10.)

2. For $n_0 = \max(d, \operatorname{lcm}(m,d) - m - d, 2m^2 - m) \leq N < N_0$, use Theorem 3.5.12 search for a, b values to find $\varepsilon(n,m,d)$ satisfying both $(*)$ and $(**)$.

For several small values of m and d, we compute N with this procedure, displayed below in Figure 3.5.1.

m	2		3		4		5		6		7		10	
d	n_0	N	n_0	N	n_0	N	n_0	N	n_0	N	n_0	N	n_0	N
3	6	106	15	552										
4	6	108	15	553	28	1164								
5	6	110	15	555	28	1161	45	2015						
6	6	112	15	558	28	1162	45	2014	66	3192				
7	7	114	15	559	28	1163	45	2015	66	3187	91	4438		
10	10	120	17	565	28	1166	45	2020	66	3190	91	4438	190	10860
100	100	234	197	662	100	1256	100	2110	194	3278	593	4525	190	10940
1000	1000	1000	1997	1997	1000	2040	1000	3045	1994	4130	5993	5993	1000	11800

Figure 3.5.1: When is Corollary 3.5.11 taking effect?

3.6 Geometric sources of higher degree points

Let C be a superelliptic curve over $\mathbb{Q}$ given by an affine equation of the form $y^m = f(x)$ where $f(x)$ has degree d. The parametrization strategy in (3.2.1) produces points on superelliptic curves that generate degree n field extensions, whenever we can prove that F given in (3.3.1) is irreducible. The entire strategy fails to produce degree n extensions when $\gcd(m,d) \nmid n$ in general. In this section, we attempt to provide some heuristics for why one should expect degree n points on superelliptic curves with $\gcd(m,d) \nmid n$ to appear less often compared to degree n points with $\gcd(m,d) \mid n$.

As previously mentioned, in the case of hyperelliptic curves, $m = 2$ and $\gcd(2,d) = 2$, this parametrization does not produce any odd degree points (cf. [Key22]). This is consistent with a result of Bhargava–Gross–Wang [BGW17] which says that a positive proportion of locally soluble hyperelliptic curves have no odd degree points (and thus that a positive proportion of all hyperelliptic curves have no odd degree points).

While we are far from proving an analogous result to [BGW17] for degree n points with $\gcd(m,d) \nmid n$ on superelliptic curves, we attempt to give some heuristics and examples suggesting that points of degree n with $\gcd(m,d) \mid n$ appear more often than those with $\gcd(m,d) \nmid n$ and we ask the following:

Question 3.6.1. *What, if anything, can be said about the sparsity or abundance of various degrees n of points on superelliptic curves given by affine equation of the form $C : y^m = f(x)$ where $f(x)$ has degree d? In particular, can something be said in terms of the relationship of n to the quantities m, d, and $\gcd(m,d)$?*

Another way to phrase this question is in terms of the index of the curve C/K. The *index* of a curve C, denoted $I(C)$, is the greatest common divisor of degrees $[L : K]$, where L/K ranges over algebraic extensions such that $C(L) \neq \emptyset$. See [GLL13, Sha18] for more on the index of a curve. The result of Bhargava–Gross–Wang [BGW17] can be phrased as stating that a positive proportion of hyperelliptic curves over $\mathbb{Q}$ have index 2 over $\mathbb{Q}$.

For a general superelliptic curve $C/\mathbb{Q}$, one can ask whether its index over $\mathbb{Q}$ is related to $\gcd(m,d)$. It is already clear for instance that $I(C) \mid \gcd(m,d)$ but we ask if more is true. If the exponent m is prime, Creutz [Cre13] describes how descent can be used to determine

whether or not $\mathrm{Pic}^1(C)$ contains no divisor classes defined over $\mathbb{Q}$ — which implies the index of $C/\mathbb{Q}$ is m — and gives a specific example of a curve with $m = 3$, $d = 6$ with index 3 (see [Cre13, Example 7.3]). At present, the authors are not aware of similar explicit examples for other (m, d) pairs or of families of superelliptic curves with index $\gcd(m, d)$ aside from $m = 2$.

3.6.1 Arithmetic from geometry

A geometric source from which we can expect to find infinitely many points on C are maps to $\mathbb{P}^1$. The most apparent of these are the natural maps of degree m and d from our curve C to $\mathbb{P}^1$. That is, we can get infinitely many points by pulling back along the degree m and degree d maps to $\mathbb{P}^1$. Thus we know there are infinitely many degree n points that are either multiples of d or multiples of m. For other discussions on sources of infinitely many points on different types of curves, or more general curves, see [AH91, BEL+19, DF93, HS91, SV22].

In what follows, for n the degree of the points and g the genus of the curve, we discuss maps from C to $\mathbb{P}^1$ in the case $n < g$ and in the case $n \geq 2g$.

The case of $n < g$

We first wish to characterize potential sources of infinitely many points on C of degree $n < g$. Suppose further that the exponent m is prime (we remark about the composite case below), so we have either $\gcd(m, d) = 1$ or $\gcd(m, d) = m$. In the former case, the normalization of C has a ramified rational point at infinity. If $\gcd(m, d) = m$, then we are only guaranteed the existence of points of degree n a multiple of m.

Let $n < g$, and define the nth symmetric product of C as usual by $\mathrm{Sym}^n(C) := C^n/S_n$. The points of $\mathrm{Sym}^n(C)$ correspond to effective degree n divisors on C. We have a natural map

$$\alpha : \mathrm{Sym}^n(C) \to \mathrm{Pic}^n(C),$$

defined by taking $D \mapsto [D]$. $\mathrm{Pic}^n(C)$ is a g-dimensional variety (it is a torsor of the Jacobian of C), and the image $\alpha(\mathrm{Sym}^n(C))$, often denoted by W_n, is a proper closed subvariety of $\mathrm{Pic}^n(C)$.

Suppose there exists a degree n divisor class $[D_0]$, defined over $\mathbb{Q}$. Then $\mathrm{Pic}^n(C)$ is isomorphic to the Jacobian of C, denoted J_C, by the map $[D] \mapsto [D] - [D_0]$, and we extend the map α above to J_C by composition with the isomorphism. In the case where m is prime, by a result of Zarhin [Zar18, Theorem 1.2] we have that for a generic C, J_C is geometrically simple. That is, generically J_C does not contain a translated proper abelian subvariety and therefore $\alpha(\mathrm{Sym}^n(C))$ does not contain an abelian subvariety.

By a theorem of Faltings [Fal94], this implies there are only finitely many points of $\alpha(\mathrm{Sym}^n(C))$ and therefore only finitely many points of $\mathrm{Sym}^n(C)$ that do not come from a g^r_d on C.

Theorem 3.6.2 (Faltings, [Fal94])**.** *Let X be a closed subvariety of an abelian variety A, with both defined over a number field K. Then the set $X(K)$ equals a finite union $\cup B_i(K)$, where each B_i is a translated abelian subvariety of A contained in X.*

In other words, there are only finitely many points of $\mathrm{Sym}^n(C)$ apart from those coming from the positive dimensional fibers of α. We know that for some n (namely, $n = m$ or n a multiple of m) the map α must have positive dimensional fibers, because in particular the points of $\mathrm{Sym}^n(C)$ that are the result of pulling back points from maps from C to $\mathbb{P}^1$ (e.g. a g^1_m) map to a point of J_C. This is because the Jacobian of $\mathbb{P}^1$ is trivial. However, the lack of a complete characterization of the positive dimensional fibers prevents us from concluding anything about finiteness of $C(K)$ in certain degrees.

For hyperelliptic curves, there is a complete characterization of the positive dimensional fibers (see e.g., Arbarello–Cornalba–Griffiths–Harris, [ACGH85] page 13). Any effective degree n divisor D having positive rank on a hyperelliptic curve H must contain a subdivisor of the form $P + \iota(P)$ where P is some point on H and ι is the hyperelliptic involution. In other words, the only positive dimensional fibers of the map α when C is a hyperelliptic curve are multiples of the g^1_2 (i.e. the only source of infinitely many points is pulling back along the degree 2 map to $\mathbb{P}^1$). Gunther–Morrow in [GM19, Proposition 2.6] use this and argue as above to show that for 100% of hyperelliptic curves C (asymptotically as $g \to \infty$), C has finitely many degree $n < g$ points that do not arise from pulling back a degree $n/2$ point of $\mathbb{P}^1$.

Remark 3.6.3. In the case of m composite, we no longer have that J_C is geometrically simple, however work of Occhipinti–Ulmer [OU15] provides a useful understanding of the abelian subvarieties that appear in the Jacobian. More precisely, for a fixed polynomial $f(x)$ with $m = p_1^{a_1} \dots p_l^{a_l}$ (composite), the curve $C_m : y^m = f(x)$ has maps to other curves of the form $C_{m'} : y^{m/p_i^{b_i}} = f(x)$ where $1 \leq b_i \leq a_i$ and $m' := m/p_i^{b_i}$. These maps between curves induce homomorphisms from the Jacobian $J_{C'_m}$ to J_{C_m}. They define J_m^{new} to be the quotient of J_{C_m} by the sum of the images of these morphisms for all proper divisors m' of m. J_{C_m} is isogenous to the product of $J_{m'}^{\text{new}}$ with m' ranging over all divisors of m. They show that for some sufficiently large M, J_M^{new} does not contain any abelian subvarieties of dimension less than or equal to the genus of C.

The case of $n \geq 2g$

For a fixed curve $y^m = f(x)$ where $f(x)$ has degree d, the parametrization in Proposition 3.2.2 produces infinitely many points of sufficiently large degrees n divisible by $\gcd(m, d)$. Choose finitely many such points $P_1 \dots P_w$ of degrees $n_1 \dots n_w$ on C.

We now illustrate how one can use such points to produce a degree $n = \sum_{i=1}^{w} n_i$ map to $\mathbb{P}^1$, that is, another source of infinitely many points of degree n. In this case n will (by construction) be a multiple of $\gcd(m, d)$.

To each point P_i, one can associate an element of $\text{Sym}^{n_i}(C)$ i.e., the effective degree n_i divisors D_i defined over $\mathbb{Q}$ corresponding to the Galois conjugates of P_i. Take $D := D_1 + \dots + D_w$. Let w be a positive integer large enough such that $n \geq 2g$. Using that C is smooth and integral, we may identify Weil divisors with line bundles (see e.g., [Har77], II.6.16), and hence consider the line bundle $L(D)$, which is defined over $\mathbb{Q}$. By Riemann–Roch (see e.g., [Har77], IV.1.3), the line bundle $L(D)$ is basepoint free and has

$$h^0(C, L(D)) = h^1(C, L(D)) + n + 1 - g \geq g + 1 \geq 2,$$

and so the sections of $L(D)$ define a map to $\mathbb{P}^1$. We may assume that the sections of $L(D)$ define a degree n map to $\mathbb{P}^1$. If $h^0(C, L(D))$ is greater than 2, we may instead take a sub-linear series. Using a geometric version of the Hilbert Irreducibility Theorem (see e.g.,

[Ser97] §9.2, Proposition 1), the fibers over all but a thin set of the rational points on $\mathbb{P}^1$ give us degree n points on C. Note that if for our given curve, $\gcd(m,d) = 1$, then this produces a degree n map to $\mathbb{P}^1$ giving us infinitely many points on C for all n sufficiently large.

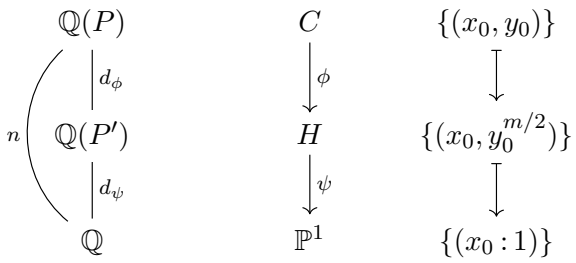
Remark 3.6.4. The above construction of a degree n map to $\mathbb{P}^1$ began with points $P_1 \dots P_w$ coming from parametrization (3.2.1) that each had degrees that were multiples of $\gcd(m,d)$. The same construction could be carried out with $P_1 \dots P_{w+1}$ if one found a point P_{w+1} on the curve not coming from the parametrization, but instead having some degree n_{w+1} that is not a multiple of $\gcd(m,d)$. The result of this would be that for n sufficiently large, there is an infinite source of points that have degree n (i.e. a degree n map to $\mathbb{P}^1$) where n is not a multiple of $\gcd(m,n)$.

Remark 3.6.5. If $g+1 \leq n < 2g$ and $L(D)$ is not basepoint free, we can still obtain a degree n map to $\mathbb{P}^1$ from the curve minus the base point locus. By the "curve to projective" extension theorem, such a map extends to a map to $\mathbb{P}^1$ from the curve but the degree can be smaller by the degree of the base locus divisor. The degree of the base locus divisor must be divisible by the index of the curve.

3.6.2 Heuristics for a special case using a result of Bhargava–Gross–Wang

Suppose we have a curve C given by an affine equation $y^m = f(x)$ where $f(x)$ has degree $d > 4$. Suppose further that m and d satisfy $2^i \mid \gcd(m,d)$ where $i \geq 2$. Let $n = 2q$ for q an odd prime. In particular, for this case we have that $\gcd(m,d) \nmid n$. In what follows we suggest that for q sufficiently large, one should not expect to find many points of degree n.

Let C be the superelliptic curve given by $y^m = f(x)$ with $f(x)$ of degree d and let H be the hyperelliptic curve given by $y^2 = f(x)$ (note that this is the same $f(x)$ as in the equation of C). We made the assumption that $d > 4$, so H has genus at least 2. We have a natural map ϕ from C to H, given by sending points $\{(x, \sqrt[m]{f(x)})\}$ to $\{(x, \sqrt[2]{f(x)})\}$. If P is a point of degree n on C, we can map it to a point P' on H as below. Let $\mathbb{Q}(P)$ and $\mathbb{Q}(P')$ be the extensions generated by a point P on C and by a point P' on H, respectively.



By assumption, $[\mathbb{Q}(P) : \mathbb{Q}] = n = 2q$. This means that the possibilities for d_ψ and d_ϕ are as follows:

Map	Case 1	Case 2	Case 3	Case 4
d_ϕ	1	n	q	2
d_ψ	n	1	2	q

Case 1: One should expect this to happen rarely as this would imply $\mathbb{Q}(P) = \mathbb{Q}(P')$, or equivalently $\mathbb{Q}\left(x_0, \sqrt[m]{f(x_0)}\right) = \mathbb{Q}\left(x_0, \sqrt{f(x_0)}\right)$, is an equality of degree n number fields.

Case 2: In this case H has a rational point. Since we assumed $g(H) \geq 2$, Faltings' theorem [Fal83] implies that the set $H(\mathbb{Q})$ is finite. In fact, Shankar–Wang [SW18] show that for even, monic hyperelliptic curves H of genus $g(H) \geq 9$ with a marked rational non-Weierstrass point ∞, a positive proportion (tending to 100% as $g(H) \to \infty$) have exactly two rational points, namely ∞ and $-\infty$, the conjugate of ∞ under the hyperelliptic involution. By assumption we have that H is even, but even if H is not monic, we may still be able to bound the number of rational points. Under certain technical assumptions (when $r \leq g(H) - 3$, for r the rank of J_H), Stoll [Sto19] gives an explicit uniform bound for $\#H(\mathbb{Q})$ depending only on the genus of the curve and the rank of its Jacobian using the Chabauty–Coleman method [Cha41, Col85] (see also [MP12]). Therefore we may say that this does not happen often.

Case 3: We have that d_ϕ is bounded above by the degree of ϕ, so the Riemann–Hurwitz

formula gives an upper bound

$$d_\phi \leq \deg(\phi) \leq \frac{g(C)-1}{g(H)-1}.$$

Thus for n sufficiently large (i.e. q sufficiently large), Case 3 is excluded entirely.

Case 4: Here P' is an odd degree point of H. However, Bhargava–Gross–Wang [BGW17] show that a positive proportion of hyperelliptic curves H have no odd degree points, excluding this case. Note that for this positive proportion of curves, Case 2 also does not occur.

We conclude with an illustrative special case, in which we show that for many curves C satisfying some conditions on m, d, k, we have at most finitely many points of degree n.

Let $f(x)$ be a squarefree polynomial of even degree $d = 2g+2$. This gives a hyperelliptic curve with affine equation

$$H\colon y^2 = f(x) = c_{2g+2}x^{2g+2} + c_{2g+1}x^{2g+1} + \cdots + c_0 \tag{3.6.1}$$

with coefficients $c_i \in \mathbb{Z}$. We define the height of the polynomial $f(x)$ to be

$$\mathrm{ht}(f) := \max\{|c_i|\},$$

where c_i are as above.

We remark that [GM19, Propositions 2.5 and 2.6(2)] hold for even degree hyperelliptic curves as in (3.6.1). The results of Gunther–Morrow are stated for (odd) hyperelliptic curves with a rational Weierstrass point and their hyperelliptic curves are ordered by a slightly different height. We phrase the result in terms of densities of polynomials $f(x)$ so that our height is compatible with the height used in [BGW17]. We record the minor differences in the proofs in the following lemma.

Lemma 3.6.6. *For n an even positive integer and $g > n$, for 100% of squarefree polynomials $f(x)$ ordered by height, the corresponding hyperelliptic curve H given in (3.6.1) of genus g over $\mathbb{Q}$ have finitely many degree n points not obtained by pulling back degree $\frac{n}{2}$ points of*

$\mathbb{P}^1$.

Proof. First we show, as in [GM19, Proposition 2.5], that for 100% of squarefree polynomials $f(x)$, the corresponding genus g hyperelliptic curves with affine equation $y^2 = f(x)$ have geometrically simple Jacobian.

To see this, let $t_0, \dots t_{2g+2}$, so that we may show that polynomial $F(x, t_0, \dots, t_n) = t_{2g+2}x^{2g+2} + \cdots + t_0$ has Galois group S_{2g+2} over $\mathbb{Q}(t_0, \dots t_{2g+2})$. Take the specialization with $t_2 = \cdots = t_{2g} = 0$, $t_0 = t_1 = -1$, and $t_{2g+2} = 1$. This gives us the polynomial $x^{2g+2} - x - 1$, which is irreducible and has Galois group S_{2g+2} by Corollary 3 of [Osa87]. This implies that the curve H given by affine equation $H\colon y^2 = f(x)$ has geometrically simple Jacobian by a result of Zarhin [Zar10]. By Hilbert's irreducibility theorem, Lemma 3.2.3, we see that 100% of specializations of $F(x, t_1, \dots, t_n)$ have Galois group S_{2g+2} and thus for 100% of squarefree polynomials $f(x)$ the corresponding genus g hyperelliptic curve H with affine equation $y^2 = f(x)$ has geometrically simple Jacobian.

The rest follows from exactly the same proof as [GM19, Proposition 2.6], outlined in §3.6.1, except that since we do not assume there is a rational Weierstrass point, one defines an Abel Jacobi map $\mathrm{Sym}^n(H) \to J_H$ using a fixed degree 2 divisor D_0 on the curve and sending $D \mapsto 2D - nD_0$ (we know such a divisor exists because of the map to $\mathbb{P}^1$). □

We also note that the above height on the polynomials $\mathrm{ht}(f) := \max\{|c_i|\}$ agrees with the height defined by Bhargava–Gross–Wang in [BGW17] when H is embedded in the weighted projective space $\mathbb{P}(1, g+1, 1)$ and expressed by the following equation:

$$H\colon y^2 = f(x, z) = c_{2g+2}x^{2g+2} + c_{2g+1}x^{2g+1}z + \cdots + c_0 z^{2g+2}. \tag{3.6.2}$$

Bhargava–Gross–Wang define the height of such a curve C to be $\mathrm{ht}'(H) := \max\{|c_i|\}$. This height on curves in weighted projective space corresponds exactly to the height $\mathrm{ht}(f)$ on the defining polynomial $f(x)$ when we dehomogenize by taking $z = 1$. Thus by [BGW17, Theorem 1] when ordered by height, a positive proportion of squarefree polynomials $f(x)$ have no odd degree points.

Proposition 3.6.7. *Suppose m and d are positive even integers and q is an odd prime satisfying*

- $4 \mid m \mid d$,
- $\frac{m}{2} < q$,
- $n = 2q < \frac{d}{2} - 1$.

Then for a positive proportion of squarefree degree d polynomials $f(x)$ ordered by height, the superelliptic curve given by $C: y^m = f(x)$ has finitely points of degree n.

Moreover, for such a curve C and point $P \in C$ of degree n, the image $\phi(P) \in H$ as defined above is of degree n and is not the pullback of a degree q point on $\mathbb{P}^1$.

Proof. Let H be the corresponding hyperelliptic curve with equation $H: y^2 = f(x)$. By methods of [GM19] (see Lemma 3.6.6), we have that for 100% of polynomials $f(x)$ of degree d, the corresponding hyperelliptic curve has only finitely many points of degree $n < g(H)$ that are not the pullback of a degree $\frac{n}{2}$ point on $\mathbb{P}^1$. We also know that a positive proportion of such hyperelliptic curves do not have any odd degree points by [BGW17, Theorem 1]. Thus for a positive proportion of polynomials $f(x)$, the hyperelliptic curve H has both of these properties. For such H, let $C: y^m = f(x)$ be the superelliptic curve with map to H given by $\phi: (x_0, y_0) \mapsto (x_0, y_0^{m/2})$ as above. Take P to be a point on C of degree n with $\phi(P) = P'$ its image in H. By considering Cases 1 — 4 above, we show there are only finitely many such P.

Cases 2 and 4 are excluded by the fact that H has no odd degree points. To see that Case 3 is impossible, we recall $q = d_\phi \leq \deg(\phi) = \frac{m}{2}$. This contradicts the hypothesis, so d_ϕ cannot be equal to q.

All that remains is Case 1, in which both P and its image P' are degree n points. Suppose $P = (x_0, y_0)$, so $P' = (x_0, y_0^{m/2})$, and the image of P, P' in $\mathbb{P}^1$ is x_0. If P' is the pullback of a degree $q = n/2$ point of $\mathbb{P}^1$, then $[\mathbb{Q}(x_0) : \mathbb{Q}] = q$ and $f(x_0)$ is not a square in $\mathbb{Q}(x_0)$. However, this implies that the degree of $\sqrt[m]{f(x_0)}$ over $\mathbb{Q}(x_0)$ is greater than 2, which contradicts that the degree of P is n.

Thus we see that P' cannot be the pullback of a degree q point of $\mathbb{P}^1$. Since $n < \frac{d}{2} - 1 = g(H)$ by our assumption, we have that only finitely many such P' can exist. Hence at most finitely many points P on C of degree n can exist. □

The argument for Case 1 in the proof of Proposition 3.6.7 can be refined to prove Proposition 3.1.7, restated below, at the expense of the description of the image of P in H. For this, we do not use [BGW17, Theorem 1], allowing us to obtain a proportion approaching 100%.

Proposition 3.6.8 (See Proposition 3.1.7)**.** *Suppose m, d are positive even integers such that $d > 4$. Let $n < \frac{d}{2} - 1$ have 2-adic valuation strictly less than that of m, i.e. $v_2(n) < v_2(m)$. Then for a positive proportion approaching 100% of squarefree degree d polynomials $f(x)$, ordered by height, the superelliptic curve $C\colon y^m = f(x)$ has only finitely many points of degree n.*

Proof. Fix a squarefree polynomial $f(x)$ of degree d. Since m is even, we have a map $C \to H$ given by $(x, y) \mapsto (x, y^{m/2})$ in affine coordinates. Let $P \in C(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(P) : \mathbb{Q}] = n$ and denote its image $P' \in H(\overline{\mathbb{Q}})$, setting $n' = [\mathbb{Q}(P') : \mathbb{Q}]$.

By Lemma 3.6.6, for a positive proportion (approaching 100%) of $f(x)$ ordered by height, H has finitely many points of degree $n' \leq n < g(H) = \frac{d}{2} - 1$ which are not the pullback of a degree $\frac{n'}{2}$ point of $\mathbb{P}^1$. Suppose P' is the pullback of a degree $\frac{n'}{2}$ point on $\mathbb{P}^1$. Then since the composition $C \to H \to \mathbb{P}^1$ is the degree m superelliptic map $C \to \mathbb{P}^1$, we have that P is the pullback of a degree n/m point on $\mathbb{P}^1$. This implies that $n' = \frac{2n}{m}$.

However, by our hypothesis on the 2-adic valuations, $v_2(2n) \leq v_2(m)$, so $v_2(n') \leq 0$. Since n' is an integer, it must be odd, contradicting that P' is the pullback of a degree $\frac{n'}{2}$ point on $\mathbb{P}^1$. Hence we conclude that P' is not the pullback of a degree $\frac{n'}{2}$ point on $\mathbb{P}^1$, and for each $n' \mid n$ there are finitely many points of degree n' on H which could be the image of a degree n point on C. Since each such P' has finitely many preimages in C, we conclude that C has finitely many points of degree n for all $f(x)$ in the aforementioned positive proportion. □

Chapter 4

Solubility densities in families of superelliptic curves

4.1 Introduction

In 1983, Faltings proved that if C is a curve of genus $g > 1$ over $\mathbb{Q}$, then the set of $\mathbb{Q}$-rational points of C, $C(\mathbb{Q})$, is finite [Fal83]. The questions of counting and classifying the $\mathbb{Q}$-rational points of a given curve and the study of how $C(\mathbb{Q})$ varies as C varies in families are areas of active work. For example, there has been recent work on sparsity of rational points on hyperelliptic and superelliptic curves by Ellenberg–Hast, Poonen–Stoll, Shankar–Wang, and Stoll [EH21, PS14, SW18, Sto19]. See also [Cha41, Col85, Kim05, Kim09, MP12] for work on the Chabauty–Coleman method and its generalization, the Chabauty–Kim method. In studying the $\mathbb{Q}$-rational points of a curve it is often useful to examine the $\mathbb{Q}_p$-rational points of the curve, for p a place of $\mathbb{Q}$.

In particular, one can ask when a curve is everywhere locally soluble, that is, if the curve has a point over $\mathbb{Q}_p$ for every place p of $\mathbb{Q}$ (including the infinite place, $\mathbb{Q}_\infty = \mathbb{R}$). Poonen–Stoll [PS99b, PS99a] using the sieve of Ekedahl [Eke91] have shown that this proportion is positive in the case of hyperelliptic curves. Bright–Browning–Loughran [BBL16] have generalized this method to certain families of varieties over number fields. Bhargava–Cremona–Fisher [BCF16, BCF21] determined the proportion of everywhere locally sol-

uble plane cubics ($\approx 75.96\%$) and genus one curves ($\approx 97.3\%$) by expressing the local densities as rational functions of p (in forthcoming work, they compute this quantity for hyperelliptic curves of genus $g > 1$). In higher dimensions, Bright–Browning–Loughran, Fisher–Ho–Park and Poonen–Voloch have studied local solubility of various hypersurfaces [BBL16, FHP21, PV04]. Further, Browning [Bro17] studied certain cubic hypersurfaces in $\mathbb{P}^3$, giving explicit rational functions for the local densities to show that nearly all ($\approx 99\%$) are everywhere locally soluble, and moreover proving that a positive proportion of such surfaces have global points.

In recent years, there have been several works studying the arithmetic of superelliptic curves such as [Aru21, Aru20, EH21, BK21a], including work of Watson [Wat21] on the failure of the Hasse principle in twist families of superelliptic curves. In this chapter, we study the proportion of (everywhere) locally soluble superelliptic curves.

We recall from Definition 3.1.4 that a superelliptic curve $C_f/\mathbb{Q}$ of exponent $m \geq 2$ is a projective curve with affine equation

$$C_f \colon y^m = f(x) = \sum_{i=0}^{d} c_i x^i. \tag{4.1.1}$$

Note that unlike in Chapter 3, we need not enforce that f is m-th power free, nor that f is not a perfect e-th power for a nontrivial divisor $e \mid m$; these conditions represent 0% of polynomials f, and hence will not affect the proportions in which we are interested.

Such a curve C_f possesses a cyclic degree m map to the projective line $\mathbb{P}^1$ defined over $\mathbb{Q}$, sending a point $(x, y) \mapsto x$. The genus of C_f over an algebraically closed field k is computed by the Riemann–Hurwitz formula to be

$$g(C_f) = \frac{1}{2}\left(m(|B|-2) - \sum_{\alpha \in B}(m, r_\alpha)\right) + 1, \tag{4.1.2}$$

where we denote by B the set of branch points of the map to $\mathbb{P}^1$ and we denote by r_α the order of α as a root of $f(x)$. The value r_∞ is analogously defined and we use that $(m, r_\infty) = (m, \deg(f))$. When $m \mid d$, equivalent to the superelliptic map $C_f \to \mathbb{P}^1$ being unramified at infinity, C_f embeds as a closed subvariety into the weighted projective space

$\mathbb{P}\left(1, \frac{d}{m}, 1\right)$ as the vanishing set of

$$F(x, y, z) = y^m - f(x, z) = y^m - \sum_{i=0}^{d} c_i x^i z^{d-i}. \tag{4.1.3}$$

We study the local solubility of these curves in three ways. First, by showing that the proportion of everywhere locally soluble superelliptic curves is positive and given by a product of local factors. Next, we prove explicit lower bounds for the proportion of everywhere locally soluble superelliptic curves in terms of an Euler product depending on m. Finally, we give an explicit rational function for the local factors, in the case of superelliptic curves with $m = 3$ and $d = 6$.

We now define precisely this proportion. Given a superelliptic curve C_f of exponent m and degree d divisible by m as in (4.1.3), we define its height $h(C_f)$ to be the height of its defining polynomial $h(f) := \max\{|c_0|, \dots, |c_d|\}$, the maximum of the absolute values of the coefficients. Then we define the proportion as

$$\rho_{m,d} = \lim_{B \to \infty} \frac{\#\{C_f \mid C_f \text{ is everywhere locally soluble and } h(C_f) \leq B\}}{\#\{C_f \mid h(C_f) \leq B\}}, \tag{4.1.4}$$

where here C_f ranges over superelliptic curves of exponent m and degree d. We refer to $\rho_{m,d}$ as the *adelic density* of equations of everywhere locally soluble such curves.

To define the corresponding local densities, let p be a prime and μ_p be a Haar measure on the additive group $\mathbb{Z}_p^{d+1}$, normalized such that $\mu_p\left(\mathbb{Z}_p^{d+1}\right) = 1$. We define

$$\rho_{m,d}(p) = \mu_p\left(\left\{(c_0, \dots, c_d) \in \mathbb{Z}_p^{d+1} \mid y^m = c_d x^d + \cdots + c_0 z^d \text{ has a } \mathbb{Q}_p\text{-point}\right\}\right). \tag{4.1.5}$$

For the place at infinity, we let μ_∞ denote the usual Euclidean measure on $\mathbb{R}^{d+1}$ and set

$$\rho_{m,d}(\infty) = \frac{1}{2^{d+1}} \mu_\infty\left(\left\{(c_0, \dots, c_d) \in [-1, 1]^{d+1} \mid y^m = c_d x^d + \cdots + c_0 z^d \text{ has an } \mathbb{R}\text{-point}\right\}\right). \tag{4.1.6}$$

Our first result shows that the proportion of locally soluble superelliptic curves of exponent m and degree d, $\rho_{m,d}$ is positive using the methods of Poonen–Stoll and Bright–Browning–Loughran [BBL16, PS99b, PS99a] and further that the adelic density $\rho_{m,d}$ can

be computed as a product of the local densities.

Theorem 4.1.1. *Fix integers $m \geq 2$ and d divisible by m, such that $(m,d) \neq (2,2)$. Then we have $\rho_{m,d} > 0$, i.e. a positive proportion of superelliptic curves over $\mathbb{Q}$ of the form (4.1.3) are everywhere locally soluble.*

Moreover, the adelic density may be computed as the product of local densities,

$$\rho_{m,d} = \rho_{m,d}(\infty) \prod_p \rho_{m,d}(p).$$

Remark 4.1.2. A version of this theorem holds over number fields as well as over $\mathbb{Q}$; for the statement (and proof) of this theorem in full generality see Corollary 4.2.6.

For the remainder of the paper we focus on bounding and computing the local densities $\rho_{m,d}(p)$ for the finite primes p of $\mathbb{Q}$, using these to compute or bound the adelic densities $\rho_{m,d}$. Given m, d, we find explicit lower bounds for $\rho_{m,d}(p)$ in Propositions 4.3.2, 4.3.4, 4.3.6, and 4.3.9, and an upper bound for $\rho_{m,d}(2)$ in Lemma 4.4.1. By Theorem 4.1.1, this yields upper and lower bounds for $\rho_{m,d}$; see Corollary 4.3.10 and Examples 4.3.15 and 4.3.16.

These bounds are sufficient to then bound the limiting behavior of $\rho_{m,d}$ for fixed m as $d \to \infty$; see Corollaries 4.3.14, 4.3.13, and 4.4.2. We summarize these below for prime m.

Theorem 4.1.3. *Fix a prime m and suppose $m \mid d$. The limiting behavior of $\rho_{m,d}$ as $d \to \infty$ may be described by*

$$\liminf_{d\to\infty} \rho_{m,d} \geq \left(1 - \frac{1}{m^{m+1}}\right) \prod_{p\equiv 1(m)} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right) \prod_{p\not\equiv 0,1(m)} \left(1 - \frac{1}{p^{2(p+1)}}\right).$$

When $m > 2$, we have the following numerical estimates, uniform in m:

$$\liminf_{d\to\infty} \rho_{m,d} \geq 0.83511$$

and

$$\limsup_{d\to\infty} \rho_{m,d} \leq 1 - \frac{1}{2^9} \approx 0.99804.$$

Remark 4.1.4. When the exponent m is composite, the methods of bounding $\rho_{m,d}(p)$ from below discussed in Section 4.3 still apply, but the resulting expressions for a lower bound of $\rho_{m,d}$ may be less compact. See Example 4.3.18 for a discussion in the case of $m = 4$.

After giving several examples of lower bounds for various pairs m, d, we employ methods similar to those of Bhargava–Cremona–Fisher to compute exact formulas for the local densities $\rho_{3,6}(p)$ for p sufficiently large, the first case of superelliptic curves not already addressed by [BCF16], [BCF21], or their forthcoming paper on hyperelliptic curves of higher genus.

We give this local density as a rational function in p depending on the residue class of p modulo 3 (assuming p is sufficiently large). We compute lower bounds for the solubility when p is small using a brute force search, allowing us to give an approximate proportion of locally soluble $m = 3$, $d = 6$ superelliptic curves.

Theorem 4.1.5. *For superelliptic curves of the form (4.1.3) with $m = 3$ and $d = 6$, the exact value of $\rho_{3,6}$ is about 96.94%.*

Moreover, there exist rational functions $R_1(t)$ and $R_2(t)$ such that the local density $\rho_{3,6}(p)$ is given by

$$\rho_{3,6}(p) = \begin{cases} R_1(p), & p \equiv 1 \pmod 3 \text{ and } p > 43 \\ R_2(p), & p \equiv 2 \pmod 3 \text{ and } p > 2. \end{cases}$$

The explicit formula is given in (4.8.1). The asymptotic behavior of $R_1(t)$ and $R_2(t)$ is described by

$$1 - R_1(t) \sim \frac{2}{3} t^{-4},$$
$$1 - R_2(t) \sim \frac{53}{144} t^{-7}.$$

Remark 4.1.6. The proof, given in §4.5, involves relating $\rho_{3,6}$ to several quantities. These relations were implemented in Sage [Sag21] to solve for the explicit formula. The Sage notebook used for these calculations can be found in the GitHub repository associated to this paper [BK21b, `SEC_rho36_23Aug21.ipynb`], accessible at the link below:

https://github.com/c-keyes/Density-of-locally-soluble-SECs.

Remark 4.1.7. In contrast to the work of Bhargava–Cremona–Fisher, where the local density at a prime p for a genus one curve is given by a degree-9 rational function of p [BCF21] and the that of a plane cubic curve is given by a degree-12 rational function of p [BCF16], the local density of our superelliptic curves $\rho_{3,6}(p)$ is a degree-57 rational function of p. This situation produced considerably more cases to check. Moreover, one can see that the number of such cases increases quickly in both m and d, and certain independence arguments we make do not hold for $d \geq 8$; see Remark 4.5.20. For this reason, we restricted our attention to $m = 3, d = 6$ superelliptic curves for the exact expression.

This chapter is organized as follows. §4.2 contains the proof of a more general version of Theorem 4.1.1, that the proportion of locally soluble superelliptic curves over any number field k is positive. §4.3 contains the proof of Theorem 4.1.3, the lower bounds for the proportion of locally soluble superelliptic curves with exponent m and degree d with $m \mid d$ and several examples of lower bounds for $\rho_{m,d}(p)$ for specific pairs m, d. This is contrasted in §4.4 with a discussion of upper bounds for the local densities, leading to a general upper bound for $\rho_{m,d}$. §4.5 contains the proof of the exact formula for the local densities $\rho_{3,6}(p)$. §4.6 contains an explanation of a computational approach to bounding the local densities $\rho_{m,d}(p)$ for small primes. In §4.7 we detail how to count the number of degree $2 \leq d \leq 6$ binary forms $f(x, z)$ over $\mathbb{F}_p$ having the different possible factorization types. Finally, in §4.8 we provide the explicit expressions for numerous rational functions from §4.5, including $\rho_{3,6}(p)$ itself.

Acknowledgments

The authors are grateful to Manjul Bhargava, Henri Darmon, Jackson Morrow, and David Zureick-Brown for helpful conversations. The authors would also like to thank Tim Browning, Jackson Morrow, Jeremy Rouse, Lori Watson, and David Zureick-Brown for their valuable feedback on an earlier draft. In addition, we thank an anonymous referee for their thorough reading of the manuscript and thoughtful suggestions that improved the paper.

4.2 The proportion is positive

In proving Theorem 4.1.1, we can in fact produce a more general statement about superelliptic curves over number fields. For the remainder of this section, let $m \geq 2$ be an integer and d be a multiple of m. Let $k/\mathbb{Q}$ be an algebraic number field, with $\mathcal{O}_k$ denoting the ring of integers, k_v denoting the v-adic completion at a place v, and $\mathbf{A}_k$ denoting the ring of adeles.

Definition 4.2.1. A scheme X/k is **everywhere locally soluble** if $X(k_v) \neq \emptyset$ for all places v of k.

If X is proper over k, then the adelic points of X are the product of the k_v-points,

$$X(\mathbf{A}_k) = \prod_v X(k_v).$$

In this case we have that X is everywhere locally soluble if and only if $X(\mathbf{A}_k) \neq \emptyset$. Note that a superelliptic curve C_f/k is projective, and therefore proper over k.

To define the density of superelliptic curves C_f of the form (4.1.3) with integral coefficients $(c_i)_{i=0}^d = \boldsymbol{c} \in \mathcal{O}_k^{d+1}$ which are locally soluble, we will need a suitable way to take limits, which specializes to the usual density over $\mathbb{Q}$. Let $k_\infty = \mathcal{O}_k \otimes_{\mathbb{Z}} \mathbb{R}$ and take $\Psi \subset k_\infty^{d+1}$ to be a bounded subset of positive measure whose boundary has measure zero, $\mu_\infty(\partial\Psi) = 0$. One can then take a limit to define the density

$$\rho_{m,d,k,\Psi} = \lim_{B\to\infty} \frac{\#\left\{\boldsymbol{c} \in \mathcal{O}_k^{d+1} \cap B\Psi^{d+1} \mid C_f(\mathbf{A}_k) \neq \emptyset\right\}}{\#\left\{\boldsymbol{c} \in \mathcal{O}_k^{d+1} \cap B\Psi^{d+1}\right\}}. \tag{4.2.1}$$

Note that in the case of $k = \mathbb{Q}$, we have $k_\infty = \mathbb{R}$ and may choose $\Psi = [-1, 1]$, so that $\rho_{m,d,\mathbb{Q},\Psi}$ takes the form

$$\rho_{m,d,\mathbb{Q},[-1,1]} = \lim_{B\to\infty} \frac{\#\left\{\boldsymbol{c} \in \mathbb{Z}^{d+1} \cap [-B, B]^{d+1} \mid C_f(\mathbf{A}_k) \neq \emptyset\right\}}{\#\left\{\boldsymbol{c} \in \mathbb{Z}^{d+1} \cap [-B, B]^{d+1}\right\}},$$

which agrees with (4.1.4) upon observing $h(C_f) \leq B$ precisely when $\boldsymbol{c} \in [-B, B]^{d+1}$. Note also that this definition depends on the choice of Ψ; for example taking $k = \mathbb{R}$ and $\Psi =$

$[0,1]^{d+1}$ instead would produce a different answer. Asking for Ψ to be convex and symmetric in k_∞ is likely desirable.

To extend the definitions of the local densities, for a finite place $v \nmid \infty$, we have

$$\rho_{m,d,k}(v) = \mu_v\left(\left\{\boldsymbol{c} \in (\mathcal{O}_k)_v^{d+1} \mid y^m = c_d x^d + \cdots + c_0 z^d \text{ has a } k_v\text{-point}\right\}\right),$$

where μ_v is a normalized Haar measure on $(\mathcal{O}_k)_v^{d+1}$, thus extending (4.1.5). At the infinite places, we take

$$\rho_{m,d,k,\Psi}(\infty) = \frac{\mu_\infty\left(\left\{\boldsymbol{c} \in \Psi \mid y^m = c_d x^d + \cdots + c_0 z^d \text{ has a } k_\infty\text{-point}\right\}\right)}{\mu_\infty(\Psi)}$$

This could further be broken down into a product of local densities for $v \mid \infty$, but it is not necessary for our analysis.

We can use ideas of Bright–Browning–Loughran [BBL16] to show that $\rho_{m,d,k,\Psi}$ exists, is nonzero, and is computable via a product of local densities. This was already known for hyperelliptic curves over $\mathbb{Q}$ (i.e. the $\rho_{2,d,\mathbb{Q},[-1,1]}$ case) by work of Poonen and Stoll [PS99b]. In particular, we will need the following result, which is a slight weakening of [BBL16, Theorem 1.4].

Theorem 4.2.2 (see [BBL16, Theorem 1.4])**.** *Let k be a number field and $\pi\colon X \to \mathbb{A}^n$ a dominant quasiprojective k-morphism with geometrically integral generic fiber, and let X_P denote the fiber of π over a point $P \in \mathbb{A}_k^n$. Assume further that*

(i) the fiber of π above each codimension 1 point of $\mathbb{A}^n$ is geometrically integral,

(ii) $X(\mathbf{A}_k) \neq \emptyset$,

(iii) for each real place v of k, we have $B\pi(X(k_v)) \subseteq \pi(X(k_v))$ for all $B \geq 1$.

Let $\Psi' \subset k_\infty^n$ be a bounded subset of positive measure lying in $\pi(X(k_\infty))$ whose boundary has measure zero. Then the limit

$$\lim_{B\to\infty} \frac{\#\left\{P \in \mathcal{O}_k^n \cap B\Psi' \mid X_P(\mathbf{A}_k) \neq \emptyset\right\}}{\#\left\{P \in \mathcal{O}_k^n \cap B\Psi'\right\}} \tag{4.2.2}$$

exists, is nonzero, and is equal to the product of local densities,

$$\prod_{v\nmid\infty} \mu_v\left(\{P \in (\mathcal{O}_k)_v^n \mid X_P(\mathbb{Q}_p) \neq \emptyset\}\right).$$

We now translate our problem into this language. Consider the affine space $\mathbb{A}_k^{d+1} = \operatorname{Spec} k[c_0, \ldots, c_d]$ and let $\mathcal{P}_k = \mathbb{P}_k\left(1, \frac{d}{m}, 1\right)$ be the weighted projective space into which curves of the form C_f naturally embed, with coordinates $[x : y : z]$. Thus the vanishing set of $F(x, y, z) =$ (4.1.3) gives a variety $X \subset \mathbb{A}_k^{d+1} \times \mathcal{P}_k$. We have a natural map $\pi\colon X \to \mathbb{A}_k^{d+1}$, where the fiber X_P over a k-point $P \in \mathbb{A}_k^{d+1}(k)$ corresponds to a specialization C_f, where the coefficients of f are given by the coordinates of P.

If $\Psi \subset k_\infty^{d+1}$ is a bounded subset of positive measure with $\mu_\infty(\partial\Psi) = 0$, we take $\Psi' = \Psi \cap \pi(X(k_\infty))$; that is, the polynomials f with coefficients given in Ψ such that C_f has points over all archimedean completions of k. Thus if Theorem 4.2.2 holds, we have

$$\begin{aligned}\rho_{m,d,k,\Psi} &= \lim_{B\to\infty} \frac{\#\left\{P \in \mathcal{O}_k^{d+1} \cap B\Psi' \mid X_P(\mathbf{A}_k) \neq \emptyset\right\}}{\#\left\{P \in \mathcal{O}_k^{d+1} \cap B\Psi'\right\}} \cdot \frac{\#\left\{P \in \mathcal{O}_k^{d+1} \cap B\Psi'\right\}}{\#\left\{P \in \mathcal{O}_k^{d+1} \cap B\Psi\right\}} \\ &= \rho_{m,d,k,\Psi}(\infty) \prod_{v\nmid\infty} \rho_{m,d,k}(v),\end{aligned}$$

as the ratio of the lattice points contained in $B\Psi'$ to $B\Psi$ approaches $\mu_\infty(\Psi')/\mu_\infty(\Psi)$ as $B \to \infty$. To apply Theorem 4.2.2, we need to prove that π and Ψ' has the desired properties and verify (i), (ii), and (iii). We begin by characterizing when varieties cut out by equations of the form (4.1.3) are geometrically integral.

Lemma 4.2.3. *Fix $m \geq 2$ and d divisible by m. Let k be any base field. Suppose $f(x, z) \in k[x, z]$ is homogeneous of degree d and take C_f the closed subvariety of $\mathbb{P}_k\left(1, \frac{d}{m}, 1\right)$ cut out by* (4.1.3)*. The following are equivalent.*

(a) $f \neq ah^q$ for all prime divisors $q \mid m$, $a \in k$, and homogeneous degree d/q polynomials $h(x, z) \in k[x, z]$.

(b) $f \neq g^q$ for all prime divisors $q \mid m$ and homogeneous degree d/q polynomials $g(x, z) \in \overline{k}[x, z]$.

(c) C_f is geometrically integral.

Proof. For the (a) $\implies$ (b) direction, we prove the contrapositive. Suppose $f = g^q$ for some prime divisor $q \mid m$ and $g \in \overline{k}[x, z]$. We will find $a \in k$ and $h \in k[x, z]$ such that $f = ah^q$. For the moment, let us further assume that the characteristic of k is prime to q.

Write $g = a_0 g_0$ where $a_0 \in \overline{k}$ and g_0 has leading coefficient 1 (i.e. the highest power of x appears with coefficient 1). Then we have

$$f = a_0^q g_0^q = a_0^q \left(b_{d/q} x^{d/q} + b_{d/q-1} x^{d/q-1} z + \cdots + b_0 z^{d/q} \right)^q.$$

Assume for convenience that $b_{d/q} = 1$; if not, it must be zero by our construction, and the proof proceeds identically, starting with the first nonzero value of $b_{d/q-i}$. The leading term of f is $a_0^q x^d$, so $a_0^q \in k$. Set $a = a_0^q$. Now we examine the $x^{d-1}z$ term: it is $aqb_{d/q-1}x^{d-1}z$, so using the fact that a and q are units in k (here we use $\mathrm{char}(k) \nmid q$), we see that $b_{d/q-1} \in k$.

Proceeding inductively, we show $b_{d/q-i} \in k$ for all $0 \leq i \leq d/q$. The $x^{d-i}z^i$ term of f looks like

$$a(\ldots + qb_{d/q-i})x^{d-i}z^i,$$

where the omitted terms consist only of $b_{d/q-j}$ for $j < i$, and hence are already known to be in k by the induction hypothesis. Thus we conclude $b_{d/q-i} \in k$, showing that $g_0 \in k[x, z]$. Setting $h = g_0$, we have written $f = ah^q$ for h defined over k.

Suppose now that $\mathrm{char}(k) = q$ and write $g = b'_{d/q} x^{d/q} + \cdots + b'_0 z^{d/q}$. We have

$$f = g^q = (b'_{d/q})^q x^d + \cdots + (b'_0)^q z^d.$$

Hence $(b'_i)^q \in k$ for all i. Moreover, the q-th power map $k^\times \to k^\times$ is an isomorphism, so we take $a = 1$ and $h = b_{d/q} x^{d/q} + \cdots + b_0 z^{d/q}$ for the unique $b_i \in k$ such that $(b'_i)^q = b_i^q$, finding that $f = ah^q$.

To prove (b) $\implies$ (c), we claim it suffices to show that the standard open affine pieces $U : y^m = f(x, 1)$ and $U' : y^m = f(1, z)$, obtained by pulling back the map $C_f \to \mathbb{P}^1$ along the standard affine patches, are geometrically integral. In particular, this implies that the stalks of the structure sheaf of C_f (over $\overline{k}$) are integral domains. A straightforward computation

shows that this sheaf has only the constants as its global sections, hence C_f is geometrically connected. Since C_f is Noetherian and nonempty, geometric connectedness and integral stalks suffice to ensure C_f is geometrically integral (see e.g. [Vak17, Exercise 5.3.C]).

We now argue that $U = \operatorname{Spec} \overline{k}[x,y]/(y^m - f(x,1))$ is geometrically integral by exploiting its map to $\mathbb{A}^1 = \operatorname{Spec} \overline{k}[x]$. The same argument applies to U'. We compute the generic fiber of this map to be the spectrum of $\overline{k}(x) \otimes_{\overline{k}[x]} \overline{k}[x,y]/(y^m - f(x,1)) \simeq \overline{k}(x)[y]/(y^m - f(x,1))$. This is a field by our hypothesis (b); if not, $f(x,1) = g_0(x)^q$ for some prime $q \mid m$, and we have

$$f(x,z) = z^d f(x/z,1) = z^d g_0(x/z)^q = \left(z^{d/q} g_0(x/z)\right)^q,$$

violating (b).

Finally, we verify that the natural map of rings $\overline{k}[x,y]/(y^m - f(x,1)) \to \overline{k}(x)[y]/(y^m - f(x,1))$ is injective. Taking $g(x,y)$ in the kernel of this map and assuming its degree in y is less than m, we have

$$g(x,y) = \sum_{0 \le i < m} g_i(x) y^i = \left(\sum_{j \ge 0} h_j(x) y^j \right) (y^m - f(x,1)),$$

where $h_i \in \overline{k}(x)$ for all i. Expanding the right hand side, we see $g_i(x) = -h_i(x) f(x,1)$ for $0 \le i < m$ and $h_j(x) = h_{j+m}(x) f(x,1)$ for all j. Since $h_j(x) = 0$ for all $j \gg 0$, we must have $h_j = 0$ for all j, hence $g(x,y) = 0$. Thus $\overline{k}[x,y]/(y^m - f(x,1))$ injects into a field, and therefore must be an integral domain, making U geometrically integral.

The (c) $\implies$ (a) direction follows from the observation that if $f = ah^q$ then over $\overline{k}$ we have the nontrivial factorization of (4.1.3)

$$y^m - f(x,z) = \prod_{1 \le i \le q} \left(y^{m/q} - \zeta^i \alpha h(x,z) \right),$$

for ζ a primitive q-th root of unity and $\alpha \in \overline{k}$ satisfying $\alpha^q = a$. □

Lemma 4.2.4. *Let $\pi \colon X \to \mathbb{A}^{d+1}$, as above, be considered as a morphism of k-varieties. Then π is dominant, projective, and has geometrically integral generic fiber.*

Proof. The generic fiber of π is the curve given by (4.1.3), but viewed as a closed subscheme

of $\mathcal{P}_{k(c_0,\ldots,c_d)}$. This is geometrically integral by an application of Lemma 4.2.3 over the base field $k(c_0,\ldots,c_d)$ because the generic degree d polynomial is not an q-th power over the algebraic closure of $k(c_0,\ldots,c_d)$ for any prime divisor $q \mid m$ (in fact it is squarefree, since the discriminant of such a polynomial is nonzero in $k(c_0,\ldots,c_d)$). Interpreting this (or rather Spec of the function field) as the generic point of X, we see that the generic point of X maps to that of $\mathbb{A}_k^{d+1}$, so π is dominant . For quasiprojectivity, we note that since $\mathcal{P}_k \to \operatorname{Spec} k$ is projective and projectivity is preserved under base change, we have $\mathbb{A}_k^{d+1} \times \mathcal{P}_k \to \mathbb{A}_k^{d+1}$ is projective. Closed embeddings are projective and projectivity is closed under composition, giving that $X \to \mathbb{A}_k^{d+1} \times \mathcal{P}_k \to \mathbb{A}_k^{d+1}$ is projective. □

In order to justify (i) of Theorem 4.2.2, we first need to understand the q-th power map on polynomials for a prime q. Viewing $\mathbb{A}^{d+1}$ as the space of polynomials of degree up to d, we define a map

$$\begin{aligned} \phi\colon \mathbb{A}^{d/q+1} &\to \mathbb{A}^{d+1} \\ g(x) &\mapsto g(x)^q \end{aligned}$$

for q any prime dividing d. By identifying a polynomial $g(x) = a_{d/q}x^{d/q} + \cdots + a_0$ with the prime ideal $(a_0 - t_0, \ldots, a_{d/q} - t_{d/q}) \in \operatorname{Spec} \overline{k}[t_0,\ldots,t_{d/q}]$ and studying the coefficients of $g(x)^q$, one can produce the equations for ϕ.

What we need from this is a lower bound on the codimension of the image of this map, a fact which is proven for the $q = 2$ case in [PS99b, Lemma 3], so long as $d > 2$.

Lemma 4.2.5. *For a positive integer d and a prime $q \mid d$, let $\phi\colon \mathbb{A}_k^{d/q+1} \to \mathbb{A}_k^{d+1}$ be the q-th power map described above. Let $V \subseteq \mathbb{A}_k^{d+1}$ be the scheme theoretic image of ϕ. So long as $(d,q) \neq (2,2)$, V has codimension at least 2.*

Proof. Let I be the ideal of V and Δ the discriminant of a degree d polynomial (viewed as a function on $\mathbb{A}_k^{d+1}$). Since I corresponds to the functions vanishing on V, and an element of the image of the q-th power map is necessarily not separable, we have $(\Delta) \subseteq I$. Moreover, only in the case $q = 2$ and $d = 2$ is $(\Delta) = I$. A degree two polynomial is a perfect square if and only if it is nonseparable, but for all $(d,q) \neq (2,2)$, there exist degree d polynomials

which are neither separable nor perfect q-th powers. As (Δ) is prime (see e.g. [GKZ08, Example 1.4]), we have the chain $(0) \subsetneq (\Delta) \subsetneq I$, making the codimension of V at least 2. □

Corollary 4.2.6. *Suppose $d > 2$. Let k be a number field and $\pi\colon X \to \mathbb{A}_k^{d+1}$, as above, be considered as a morphism of k-varieties. Suppose $\Psi \subseteq k_\infty^{d+1}$ is a bounded subset such that $\Psi' = \Psi \cap \pi(X(k_\infty))$ has positive measure with $\mu_\infty(\partial\Psi') = 0$. Then $\rho_{m,d,k,\Psi}$, as defined in (4.2.1), exists, is nonzero, and is equal to a product of local densities.*

Proof. By Lemma 4.2.4, we have that π is dominant, projective, and has geometrically integral generic fiber. It remains to show that the hypotheses (i), (ii), and (iii) of Theorem 4.2.2 apply.

Let $P \in \mathbb{A}_k^{d+1}$ be a codimension one point. By Lemma 4.2.3, the fiber X_P is geometrically integral precisely when $P \notin V_q$ for some prime $q \mid m$, where V_q is the scheme-theoretic image of the q-th power map described above. By Lemma 4.2.5, each such V_q has codimension at least 2 and thus cannot contain P. Put informally, it takes more than just one algebraic relation on the coefficients to force $f(x, z)$ to be an q-th power for some $q \mid m$. Thus (i) is satisfied.

For (ii), we have $X(\mathbf{A}_k) \neq \emptyset$ because $X(k) \neq \emptyset$. That is, there exist superelliptic curves C_f with k-rational points. For example, one can take

$$C_f\colon y^m = x^d + xz^{d-1},$$

which has a k-rational point at $[0 : 0 : 1]$.

Finally, to see that for real places v, $\pi(X(k_v))$ is closed under the action of $\mathbb{R}_{\geq 1}$, simply note that positive m-th roots are in $\mathbb{R}$, so if C_f has a k_v point $[x : y : z]$ then C_{Bf} has the k_v point $[x : \sqrt[m]{B}y : z]$. □

To prove Theorem 4.1.1, we need only specialize $k = \mathbb{Q}$ and find an appropriate $\Psi \subseteq \pi(X(\mathbb{R}))$ satisfying the desired properties in Corollary 4.2.6, such that the limit (4.2.2) computes the limit in Theorem 4.1.1.

Proof of Theorem 4.1.1. When $k = \mathbb{Q}$ we have $k_\infty = \mathbb{R}$, so we set $\Psi = [-1,1]^{d+1} \cap \pi(X(\mathbb{R}))$, which may be viewed as the set of homogeneous polynomials $f(x,z)$ of degree d with real coefficients of absolute value at most 1 such that C_f has a real point. This subset is clearly bounded, and has positive measure since it contains the set $\left\{\boldsymbol{c} \in [-1,1]^{d+1} \mid 0 \leq c_0 \leq 1\right\}$, whose measure is half that of the unit cube. To see why, we merely recognize that if $c_0 \geq 0$ then C_f has an $\mathbb{R}$-point $[0 : \sqrt[m]{c_0} : 1]$.

To check $\mu_\infty(\partial\Psi) = 0$, with respect to the Euclidean measure μ_∞ on $[-1,1]^{d+1}$, we use the evaluation map, $\mathrm{ev}_{[x:z]}$ for a point $[x : z] \in \mathbb{P}^1_{\mathbb{R}}$. This map takes $\mathrm{ev}_{[x:z]}(\boldsymbol{c}) = f(x,z)$, where f is the degree d binary form in $\mathbb{R}[x,z]$ defined by $\boldsymbol{c}$. We observe

$$\Psi = \left(\bigcup_{[x:z] \in \mathbb{P}^1_{\mathbb{R}}} \mathrm{ev}^{-1}_{[x:z]}\left((0,\infty)\right) \right) \cup \left\{ \boldsymbol{c} \in [-1,1] \mid f(x,z) = 0 \text{ for some } [x:z] \in \mathbb{P}^1_{\mathbb{R}} \right\}.$$

As $\mathrm{ev}_{[x:z]}$ is continuous (in fact it is linear), the union $\cup_{[x:z] \in \mathbb{P}^1_{\mathbb{R}}} \mathrm{ev}^{-1}_{[x:z]}\left((0,\infty)\right)$ is open, and hence $\partial\Psi$ is contained in the set

$$\left\{ \boldsymbol{c} \in [-1,1] \mid f(x,z) \leq 0 \text{ for all } [x:z] \in \mathbb{P}^1_{\mathbb{R}} \text{ and } f(x,z) = 0 \text{ for some} \right\}.$$

To be in this set, it is necessary for each such root of $f(x,z) = 0$ to have even multiplicity, and in particular $\boldsymbol{c}$ is contained in the vanishing set of the discriminant polynomial, which has measure zero.

Thus the limit (4.2.2) computes $\frac{\rho_{m,d}}{\rho_{m,d}(\infty)} = \prod_{p \nmid \infty} \rho_{m,d}(p)$ as a product of local densities $\rho_{m,d}(p) = \mu_p\left(\pi(X(\mathbb{Q}_p))\right)$, completing the proof of Theorem 4.1.1. □

We conclude this section by making some observations about $\rho_{m,d,k}(\infty)$. If k is totally complex, i.e. it has no real places and only complex places, then we have that $\rho(\infty) = 1$. Using the fact that $\mathbb{C}$ is algebraically closed, any choice of $f(x,z)$ with coefficients k_∞ will have a solution $[x : y : z]$ for any choice of $[x : z] \in \mathbb{P}^1_{k_\infty}$.

Whenever m is odd, we have $\rho_{m,d,k}(\infty) = 1$, because real numbers always have an m-th root in this case. Geometrically, we observe that π is surjective on k_∞-points, $\pi(X(k_\infty)) = \mathbb{A}^{d+1}(k_\infty)$. Conversely, if m is even, $\rho_{m,d,k}(\infty)$ depends only on d, and not on m. In

particular, $\rho_{m,d,\mathbb{Q}}(\infty)$ is equal to the proportion of (real) polynomials $f(x,z)$ which take a positive value somewhere.

One can easily determine

$$\rho_{m,d,\mathbb{Q},[-1,1]}(\infty) \geq \frac{3}{4}$$

by observing that $c_d \geq 0$ or $c_0 \geq 0$ is sufficient to ensure the existence of a real point, but at present no analytic approach for computing it is known. Bhargava–Cremona–Fisher [BCF21, Proposition 3.1] determined

$$0.873914 \leq \rho_{m,4,\mathbb{Q}}(\infty) \leq 0.874196$$

for even m using a rigorous numerical approach. As observed in [BCF21], one could also use a Monte Carlo method to sample the coefficient space to estimate $\rho(\infty)$. See Example 4.3.18 for such approximations of $\rho_{4,d}(\infty)$ when $4 \leq d \leq 20$.

4.3 Lower bounds for the proportion

In this section, we give a closed form lower bound for the density $\rho_{m,d}$, albeit one containing infinite products over primes, using only a naïve form Hensel's lemma (Theorem 2.1.7), which allows us to lift roots of equations over $\mathbb{F}_p$ to ones over $\mathbb{Z}_p$. We restate what we need from Corollary 2.1.8 and Theorem 2.1.9 in the special case $\mathcal{O} = \mathbb{Z}_p$ below.

Theorem 4.3.1 (Hensel's lemma)**.** *Let $F(t) \in \mathbb{Z}_p[t]$ be a polynomial and $\overline{F}(t) \in \mathbb{F}_p[t]$ its reduction modulo p. Use $\overline{F}'(t)$ to denote the formal derivative with respect to t. If there exists $\overline{t_0} \in \mathbb{F}_p$ such that*

$$\overline{F}(\overline{t_0}) = 0 \quad \text{and} \quad \overline{F}'(\overline{t_0}) \neq 0,$$

then there exists a lift $t_0 \in \mathbb{Z}_p$ such that $F(t_0) = 0$ and the reduction of t_0 modulo p is $\overline{t_0}$.

More generally, if there exists $t_1 \in \mathbb{Z}_p$ such that

$$v\left(F(t_1)\right) > 2v\left(F'(t_1)\right), \tag{4.3.1}$$

where v denotes the p-adic valuation, then there exists $t_0 \in \mathbb{Z}_p$ such that $F(t_0) = 0$ and

$v(t_0 - t_1) \geq v(F(t_1)) - 2v(F'(t_1))$.

Let S be a subset of the set of binary degree d forms over $\mathbb{F}_p$. The translation invariance of the Haar measure μ_p implies that the measure of the set of degree d forms over $\mathbb{Z}_p$ which reduce modulo p to an element of S is equal to the ratio of $\#S$ to the (finite) number of binary degree d forms over $\mathbb{F}_p$,

$$\mu_p\left(\left\{f(x,z) \in \mathbb{Z}_p[x,z] \mid f \text{ deg. } d \text{ form}, \ \overline{f} \in S\right\}\right) = \frac{\#S}{\#\left\{\overline{f}(x,z) \in \mathbb{F}_p[x,z] \mid \overline{f} \text{ deg. } d \text{ form}\right\}}.$$

In particular, this means that when conditions on the reduction $\overline{f}(x,z)$ guarantee C_f to have a $\mathbb{Q}_p$-point, we can count the number of forms over $\mathbb{F}_p$ satisfying these conditions to give a lower estimate of $\rho_{m,d}(p)$.

In the case of this section, we use the first statement of Theorem 4.3.1 to give sufficient conditions on $\overline{f}(x,z)$ for C_f to have a $\mathbb{Q}_p$-point, with $F(x,y,z) =$ (4.1.3), with one of x, y, or z taking the place of the lifting variable t. This relatively simple approximation strategy yields lower bounds for $\rho_{m,d}$, as demonstrated for $(m,d) = (3,6)$ and $(5,5)$ in Examples 4.3.15 and 4.3.16. Moreover, they give clues as to the limiting behavior of the density for fixed m as $d \to \infty$; see Corollary 4.3.13 and Example 4.3.17.

4.3.1 Lower bounds for local densities $\rho_{m,d}(p)$

Fix a prime exponent m and a degree d divisible by m. Recall that the genus of a superelliptic curve $C_f\colon y^m = f(x,z)$ is given by (4.1.2). If f is separable of degree d, this becomes $g = \frac{(m-1)(d-2)}{2}$.

When C is a smooth curve and p is sufficiently large, the Weil conjectures imply that $C(\mathbb{F}_p) \to \infty$ as p grows large among primes of good reduction. C has bad reduction at only finitely many primes, so this together with Hensel's lemma shows that C is soluble over $\mathbb{Q}_p$ for all but finitely many primes p.

To make this effective, we can use the Hasse–Weil bound, which states that

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}. \tag{4.3.2}$$

This can be improved further,

$$|\#C(\mathbb{F}_p) - (p+1)| \leq g\lfloor 2\sqrt{p} \rfloor \tag{4.3.3}$$

see [Ser12, §4.7.2.2]. This implies that for the superelliptic curve C_f, if $f(x,z)$ is separable over $\mathbb{F}_p$ then whenever

$$p + 1 - g\lfloor 2\sqrt{p} \rfloor > 0,$$

we have $\#C_f(\mathbb{F}_p) > 0$. Taking $p > 4g^2 - 1 = (m-1)^2(d-2)^2 - 1$ is sufficient in the case that $m \mid d$. This leads us to the following proposition.

Proposition 4.3.2. *Suppose m is prime and d is divisible by m. For all primes $p > (m-1)^2(d-2)^2 - 1$ we have the lower bound*

$$\rho_{m,d}(p) \geq 1 - p^{\frac{-d(m-1)}{m}}.$$

Proof. Let $\overline{f}$ denote the reduction of f modulo p. By Lemma 4.2.3, If $\overline{f} \neq ah^m$ for $a \in \mathbb{F}_p$ and $h \in \mathbb{F}_p[x,z]$, then the curve over $\mathbb{F}_p$ given by $y^m = \overline{f}(x,z)$ is geometrically integral, hence the reduction of C_f modulo p is geometrically integral. A straightforward count shows that there are $p^{\frac{d}{m}+1}$ homogeneous polynomials $f(x,z) = ah(x,z)^m \in \mathbb{F}_p[x,z]$ of degree d, or equivalently, that the fraction of f which are *not* m-th powers modulo p is given in the statement.

It remains to prove that if $\overline{f}$ is not an m-th power modulo p, then its reduction modulo p has a smooth point. If $\overline{C_f}$ is smooth, then the size assumption on p and the bound (4.3.2) ensure that $\overline{C_f}(\mathbb{F}_p) \neq \emptyset$, and the smoothness allows us to lift to a point in $C_f(\mathbb{Q}_p)$ via Hensel's lemma (Theorem 4.3.1).

If $\overline{C_f}$ is not smooth, then we must normalize. Denote the normalization by $\widetilde{C_f}$. The genus of $\widetilde{C_f}$ is $g - \sum_{P \text{ sing}} \frac{1}{2} r_P(r_P - 1)$, where r_P denotes the multiplicity at P (see e.g.

[Har77, Ch. V, Example 3.9.2]). When P is singular we have $r_P \geq 2$, allowing us to compute

$$\begin{aligned}
\#\overline{C_f}^{\mathrm{sm}}(\mathbb{F}_p) &= \#\widetilde{C_f} - \sum_{P \text{ sing}} r_P \\
&\geq p + 1 - 2\left(g - \sum_{P \text{ sing}} \frac{1}{2} r_P(r_P - 1)\right)\sqrt{p} - \sum_{P \text{ sing}} r_P \qquad \text{(by (4.3.2))} \\
&= p + 1 - 2g\sqrt{p} + \sum_{P \text{ sing}} \left(r_P(r_P - 1)\sqrt{p} - r_P\right) \\
&> p + 1 - 2g\sqrt{p} + \sum_{P \text{ sing}} r_P(r_P - 2) \qquad (\sqrt{p} > 1) \\
&\geq p + 1 - 2g\sqrt{p}.
\end{aligned}$$

This quantity is positive by our assumption on the size of p. □

The argument of Proposition 4.3.2 can be extended to the case of m composite by considering the prime divisors of m and proceeding via inclusion-exclusion.

Corollary 4.3.3. *Fix positive integers m, d such that $m \mid d$ and let ω denote the number of distinct prime divisors of m. Set g_0 to be the genus of C_f when f is separable of degree d, given by (4.1.2). For all primes p such that $p + 1 - g_0\lfloor 2\sqrt{p} \rfloor > 0$, we have the lower bound*

$$\rho_{m,d}(p) \geq 1 - \sum_{q \mid m} p^{\frac{-d(q-1)}{q}} + \sum_{\substack{q_1, q_2 \mid m \\ q_1 \neq q_2}} p^{\frac{-d(q_1 q_2 - 1)}{q_1 q_2}} - \cdots + (-1)^{\omega} \sum_{\substack{q_1, \ldots, q_\omega \mid m \\ q_i \text{ distinct}}} p^{\frac{-d((q_1 \cdots q_\omega) - 1)}{q_1 \cdots q_\omega}}.$$

Consider now the case of primes p with $\gcd(p-1, m) = 1$. If m is prime, this is equivalent to $p \not\equiv 1 \pmod{m}$. Here the m^{th} power map $\mathbb{F}_p \to \mathbb{F}_p$ is an isomorphism of rings, and in particular is surjective. Suppose $[x_0 : z_0] \in \mathbb{P}^1_{\mathbb{F}_p}$ such that $f(x_0, z_0) \not\equiv 0 \pmod{p}$. Then we may apply Hensel's lemma to the polynomial (in y) $y^m = f(x_0, z_0)$ for any lift of x_0, z_0 to $\mathbb{Z}_p$, giving rise to a local solution.

Proposition 4.3.4. *Fix integers m and d divisible by m such that $\gcd(p - 1, m) = 1$ and $p \nmid m$.*

(a) If $p > \frac{d-1}{2}$ we have the lower bound

$$\rho_{m,d}(p) \geq 1 - \frac{1}{p^{d+1}}.$$

(b) If $p \leq \frac{d}{2} - 1$ we have the lower bound

$$\rho_{m,d}(p) \geq 1 - \frac{1}{p^{2(p+1)}}.$$

Proof. If $\overline{f}$ takes a nonzero value in $\mathbb{F}_p$ at any $[x_0 : z_0]$, then the above discussion can be used to lift an $\mathbb{F}_p$-solution to $y^m = f(x_0, z_0)$ to $\mathbb{Q}_p$. Also, if $\overline{f}$ has a simple root (x_0, z_0) in $\mathbb{F}_p$ then we can use Hensel's lemma on one of x or z to lift it to a $\mathbb{Q}_p$-solution $y^m = f(x, z)$ with $p \mid y$. The only case not immediately dealt with by Hensel's lemma is if $\overline{f}$ has a double root at every $[x_0 : z_0]$.

If $\overline{f}$ is nonzero modulo p and $p > \frac{d}{2} - 1$, then this cannot happen solely for degree reasons. Having a double root at each value is equivalent to the degree $2(p+1)$ polynomial $x^2(x-1)^2 \cdots (x-(p-1))^2 z^2$ dividing the degree d polynomial $\overline{f}$. This is not possible for $p > \frac{d}{2} - 1$, so the only case not addressed by Hensel's lemma is if $f \equiv 0 \pmod{p}$, giving the lower bound in (a).

To verify (b), we have

$$\overline{f}(x, z) = g(x, z)x^2(x - z)^2 \cdots (x - (p-1)z)^2 z^2 \tag{4.3.4}$$

for some degree $d - 2(p+1)$ form $g(x, z)$. There are $p^{d-2(p+1)+1}$ such choices of g, so the proportion of forms f for which $\overline{f}$ is not as in (4.3.4) is given in (b). □

We can also make use of some basic linear algebra to obtain lower estimates for $\rho_{m,d}(p)$, by viewing the evaluation of $\overline{f}$ as a matrix-vector product. This turns out to be useful, especially for primes $p \equiv 1 \pmod{m}$ that are too small for Proposition 4.3.2 to apply.

As usual write $f(x, z) = c_d x^d + c_{d-1} x^{d-1} z + \cdots + c_1 x z^{d-1} + c_0 z^d$ and denote by A the

$(p+1)\times(d+1)$ matrix

$$A=\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & \cdots & 2^{d-1} & 2^d \\ & & \vdots & & \\ 1 & (p-1) & \cdots & (p-1)^{d-1} & (p-1)^d \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

with entries in $\mathbb{F}_p$. We can simultaneously evaluate $f(x_0,z_0)$ at all $[x_0:z_0]$ in $\mathbb{P}^1_{\mathbb{F}_p}$ by taking the product

$$A\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \\ c_d \end{pmatrix}=\begin{pmatrix} \overline{f}(0,1) \\ \overline{f}(1,1) \\ \vdots \\ \overline{f}(p-1,1) \\ \overline{f}(1,0) \end{pmatrix}.$$

We use this relationship to find lower bounds for the number of $\overline{f}(x,z)\in\mathbb{F}_p[x,z]$ of degree d with at least one m-th power value in $\mathbb{F}_p$.

Lemma 4.3.5. *For the matrix A above, we have*

$$\dim_{\mathbb{F}_p}\ker A=\begin{cases} d-p, & p<d \\ 0, & p\geq d \end{cases}$$

which is equivalent to

$$\operatorname{rk} A=\begin{cases} p+1, & p<d \\ d+1, & p\geq d. \end{cases}$$

Proof. Suppose $\boldsymbol{c}\in\ker A$, where $\boldsymbol{c}$ is viewed as an element of $\mathbb{F}_p^{d+1}$. Then the corresponding degree d binary form $\overline{f}(x,z)$ has roots at all $[x:z]\in\mathbb{P}^1_{\mathbb{F}_p}$, and equivalently the degree $p+1$ form $x(x-z)\cdots(x-(p-1)z)z$ divides $\overline{f}$. If $p\geq d$ this is a contradiction unless $\boldsymbol{c}=\boldsymbol{0}$. If

$p < d$, then we write

$$\overline{f}(x,z) = g(x,z)x(x-z)\cdots(x-(p-1)z)z$$

for some degree $d-p-1$ form $g(x,z)$. There are p^{d-p} choices of such g, hence in this case the kernel of A has dimension $d-p$. The rank of A is given by $d+1-\dim\ker A$. □

Proposition 4.3.6. *Fix positive integers m and d. For a prime $p \nmid m$, denote the fraction of elements of $\mathbb{F}_p$ that are nonzero m-th powers by $\Phi(p) = \#(\mathbb{F}_p^\times)^m/\#\mathbb{F}_p$. Let r denote the rank of A. Then we have*

$$\rho(p) \geq 1-(1-\Phi(p))^r.$$

By Lemma 4.3.5 we have

$$\rho(p) \geq \begin{cases} 1-(1-\Phi(p))^{p+1}, & p < d \\ 1-(1-\Phi(p))^{d+1}, & p \geq d \end{cases}.$$

Proof. We may perform column reduction on A by multiplying on the right by UP, where U is an invertible upper triangular matrix and P is a permutation matrix, if appropriate. This gives $A' = AUP$ of rank r. Note that the image of A' coincides with that of A, so in particular an entry of $A\boldsymbol{c}$ is in $\left(\mathbb{F}_p^\times\right)^m$ whenever the corresponding entry of $A'(UP)^{-1}\boldsymbol{c}$ is.

We argue that the lower bound holds as follows. The first row of A' thus reveals that the proportion of f for which $f(0,1) = c_0$ is in $\left(\mathbb{F}_p^\times\right)^m$ is $\Phi(p)$. For a fixed c_0, we let c_1 vary and use the second row of A' to see that $f(1,1)$ ranges over all $\mathbb{F}_p$, and the proportion for which $f(1,1) \in \left(\mathbb{F}_p^\times\right)^m$ is again $\Phi(p)$.

Continuing in this fashion, we see that for any fixed $c_0,\ldots,c_{i-1}$ with $i \leq r-1$, $f(i,1)$ (or $f(1,0)$ if $i=d$) is given by the $(i+1)$-th row of A' containing a pivot (note that this may not coincide with the $(i+1)$-th row). Hence the $(i+1)$-th (pivot) entry is in $\left(\mathbb{F}_p^\times\right)^m$ for $\Phi(p)$ of the possible c_i. Thus letting $\boldsymbol{c}$ vary, the proportion for which at least one of the first r entries of $A\boldsymbol{c} = A'\boldsymbol{c}$ is in $\left(\mathbb{F}_p^\times\right)^m$ is

$$\Phi(p)+(1-\Phi(p))\left(\Phi(p)+(1-\Phi(p))\left(\Phi(p)+(1-\Phi(p))\left(\cdots\right)\right)\right) = 1-(1-\Phi(p))^r.$$

Since $p \nmid m$, one such value $\overline{f}(x,z) \in \left(\mathbb{F}_p^\times\right)^m$ is sufficient to lift via Hensel's lemma to a $\mathbb{Q}_p$-point of C_f. This yields the result, and Lemma 4.3.5 may be used to determine the rank r. □

Remark 4.3.7. This bound is somewhat crude in the sense that we are ignoring a great deal of possible liftable points, especially when $p \geq d$ is very large. By only using $d+1$ of the $p+1$ points $\overline{f}(x,z)$, we are able to compute an explicit lower bound, but it is quite likely that one of the points we ignore also lifts. Nevertheless, Proposition 4.3.6 will be sufficient for us to prove results about $\rho_{m,d}$ in the limit as $d \to \infty$, e.g. Corollary 4.3.13. For any fixed (m,d) one can use a brute force computer search to obtain much better estimates; see §4.6 and Examples 4.3.15 and 4.3.16.

Remark 4.3.8. Another way to refine the proof of Proposition 4.3.6 is to consider points $[x:z]$ where $\overline{f}(x,z) = 0$. These lift whenever the partial derivative $\overline{f}_x(x,z)$ or $\overline{f}_z(x,z)$ is nonzero. By formulating a matrix similar to A and applying the same column reduction used to obtain A', one can give a lower estimate that improves on Proposition 4.3.6 for $p \leq 7$. However, this method adds considerable effort and (what the authors believe is) unnecessary confusion, while providing only marginal improvement for finitely many primes, so we elect to omit this.

Finally, let us consider the case of primes p dividing m. These require some special attention, because the strategy of lifting using Hensel's lemma on $y^m = f(x_0,z_0)$ as in Proposition 4.3.4 fails when $p \mid m$, as the partial derivative with respect to y vanishes.

However, when $m = p$ or more generally $\gcd(p-1,m) = 1$, the m-th power map is an isomorphism of $\mathbb{F}_p$. In this case, for any point $[x_0 : z_0]$, there exists $y_0 \in \mathbb{F}_p$ such that $y_0^m \equiv f(x_0,z_0) \pmod{p}$. This means that for each $[x_0 : z_0]$, we need only check whether or not Hensel's lemma applies to lifting via x or z, allowing us to obtain a point of $C(\mathbb{Q}_p)$.

Proposition 4.3.9. *Fix positive integers m and d divisible by m. Suppose p is a prime*

dividing m with $\gcd(p-1, m) = 1$. *Then we have the lower bound*

$$\rho_{m,d}(p) \geq \begin{cases} 1 - \frac{1}{p^{p-1}}, & d = p \\ 1 - \frac{1}{p^p}, & d = 2p \\ 1 - \frac{1}{p^{p+1}} & d > 2p. \end{cases}$$

Proof. We begin by by evaluating f at the point at infinity, $f(1,0) = c_d$. We know that there exists $y_0 \in \mathbb{F}_p$ such that $y_0^m = c_d$, since the m-th power map is an isomorphism in this case, so the polynomial $f(1,z) - y_0^m = c_d + c_{d-1}z + \cdots + c_0 z^d - y_0^m$ has a solution at $z = 0$. The derivative with respect to z is $c_{d-1} + 2c_{d-2}z + \cdots + dc_0 z^{d-1}$, which is nonzero at $z = 0$ if and only if $c_{d-1} \not\equiv 0 \pmod{p}$. If this is the case, then Hensel's lemma applies and f has a $\mathbb{Q}_p$-point.

We have seen that $p \mid c_{d-1}$ is a necessary condition for the point at infinity not to lift, so we now study the affine points $[x : 1]$. Again, for any x_0, there exists y_0 solving $y_0^m \equiv f(x_0, 1) \pmod{p}$, and this solution lifts via Hensel's lemma if the derivative $f'(x_0) = dc_d x_0^{d-1} + \cdots + c_1 \not\equiv 0 \pmod{p}$. Thus for $\overline{f}$ not to have any liftable points we need $p \mid c_{d-1}$ and $x(x-1)\cdots(x-(p-1)) \mid f'(x)$.

We have $\deg f'(x) = d - 2$ since $p \mid d$ forces the x^{d-1} term to vanish. Let $h(x) = \sum_{i=0}^{d-2-p} a_i x^i$ be a polynomial, such that $x(x-1)\cdots(x-(p-1))h(x)$ has degree $d-2$. We count the number of h that produce

$$x(x-1)\cdots(x-(p-1))h(x) = f'(x).$$

If $d = p$, then this is only possible if $h \equiv f' \equiv 0 \pmod{p}$.

Notice that for all integers $0 < k < d/p$, the x^{pk-1} term of $f'(x)$ vanishes modulo p. This determines $d/p - 1$ independent linear conditions on the coefficients a_i, so there are at most $p^{d-2-p-d/p+2} = p^{d-p-d/p}$ choices of $h(x)$. We see this by observing that the leading term of $x(x-1)\cdots(x-(p-1))$ is x^p, while the trailing term is $(p-1)!\, x \equiv -x \pmod{p}$ by Wilson's theorem. We also impose the condition that $c_{d-1} = 0$, i.e. the linear condition

that $a_{d-p-2} = 0$. These conditions on the a_i's are summarized in the following matrix

$$\begin{pmatrix} * & \cdots & * & -1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & * & \cdots & * & -1 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ & & & & & & \vdots & & & & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & * & \cdots & * & -1 \\ 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

for which we require $\boldsymbol{a} = (a_0, \ldots, a_{d-p-2})^T$ to be in the kernel. When this matrix of relations has full rank, each condition is independent.

It is clear that the first $d/p - 1$ rows are independent. The final row is assured to be independent from the others so long as $d/p - 1 \geq 2$, i.e. $d > 2p$. This is sharp, as illustrated by the case of $p = 3$ and $d = 6$, when we find the rank of the 2×2 matrix above is one.

Suppose f_1, f_2 have $f_1' = f_2' = x(x-1)\cdots(x-(p-1))h(x)$. Then all coefficients are equal except those of x^{pk} for $0 \leq k \leq d/p$. Thus for each $h(x)$ there are $p^{d/p+1}$ polynomials f for which $f' = x(x-1)\cdots(x-(p-1))h$. This brings the total number of possible such f to be

$$p^2 \text{ when } d = p,$$
$$p^{p+1} \text{ when } d = 2p,$$
$$p^{d-p} \text{ when } d > 2p.$$

Upon dividing by the total number of forms, p^{d+1}, we obtain a lower bound for the proportion of f whose reduction modulo p has at least one Hensel-liftable point, given in the proposition. □

4.3.2 Lower bounds for the adelic density $\rho_{m,d}$

Assembling together Propositions 4.3.2, 4.3.4, 4.3.6, and 4.3.9, we give a lower bound for ρ which is explicitly computable, at least in principle, when the exponent m is a prime.

Corollary 4.3.10. *Let m be an odd prime and d an integer divisible by m. Define*

$$L_0(m,d) = \begin{cases} 1 - \frac{1}{m^{m-1}}, & d = m \\ 1 - \frac{1}{m^m}, & d = 2m \\ 1 - \frac{1}{m^{m+1}}, & d > 2m, \end{cases}$$

$$L_1^{\mathrm{sm}}(m,d) = \prod_{\substack{p \equiv 1(m) \\ p < d}} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right),$$

$$L_1^{\mathrm{med}}(m,d) = \prod_{\substack{p \equiv 1(m) \\ d < p < (m-1)^2(d-2)^2}} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{d+1}\right),$$

$$L_1^{\mathrm{big}}(m,d) = \prod_{\substack{p \equiv 1(m) \\ p \geq (m-1)^2(d-2)^2}} \left(1 - \frac{1}{p^{\frac{d(m-1)}{m}}}\right),$$

$$L_{\neq 1}^{\mathrm{sm}}(m,d) = \prod_{\substack{p \not\equiv 0,1(m) \\ p \leq \frac{d}{2} - 1}} \left(1 - \frac{1}{p^{2(p+1)}}\right),$$

$$L_{\neq 1}^{\mathrm{big}}(m,d) = \prod_{\substack{p \not\equiv 0,1(m) \\ p > \frac{d}{2} - 1}} \left(1 - \frac{1}{p^{d+1}}\right).$$

Then we have a computable lower bound

$$\rho_{m,d} \geq L_0(m,d) L_1^{\mathrm{sm}}(m,d) L_1^{\mathrm{med}}(m,d) L_1^{\mathrm{big}}(m,d) L_{\neq 1}^{\mathrm{sm}}(m,d) L_{\neq 1}^{\mathrm{big}}(m,d).$$

Proof. This follows directly from applying Propositions 4.3.2, 4.3.4, 4.3.6, or 4.3.9 to each local density $\rho(p)$ in

$$\rho_{m,d} = \prod_{p \text{ prime}} \rho(p) = \rho(m) \prod_{p \equiv 1(m)} \rho(p) \prod_{p \not\equiv 0,1(m)} \rho(p),$$

splitting the products further into the ranges in the statement as appropriate. When $p \equiv 1 \pmod{m}$, the fraction of nonzero m-th power residue classes used in Proposition 4.3.6 is $\Phi(p) = \frac{p-1}{mp}$. □

Remark 4.3.11. Corollary 4.3.10 provides a way to compute an explicit lower bound for

$\rho_{m,d}$. Notice that all the products involved are finite, save for $L_1^{\text{big}}(m,d)$ and $L_{\neq 1}^{\text{big}}(m,d)$. These products are related to the Riemann zeta function $\zeta(d(m-1)/m)$ and $\zeta(d+1)$, respectively, as the product runs over the appropriate Euler factors, but only for the primes in certain (unions of) conjugacy classes.

This alone ensures that when d is sufficiently large, these products are close to one, because they are part of the tail of $\zeta(s)$ and $\zeta(s) \to 1$ as $s \to \infty$. Explicit values, valid to several decimal places, of similar products of this form were computed in [Mat10, p. 26 – 34].

We can make this result less explicit, but somewhat more pleasant by fixing m and allowing $d \to \infty$, which is tantamount to allowing $g \to \infty$.

Lemma 4.3.12. *For a fixed prime m, we compute the limits of some of the products defined in Corollary 4.3.10 as $d \to \infty$;*

$$\lim_{d\to\infty} L_1^{\text{med}}(m,d) = 1,$$
$$\lim_{d\to\infty} L_1^{\text{big}}(m,d) = 1,$$
$$\lim_{d\to\infty} L_{\neq 1}^{\text{big}}(m,d) = 1.$$

Proof. For $L_1^{\text{big}}(m,d)$ and $L_{\neq 1}^{\text{big}}(m,d)$, the conclusion follows from recognizing that as $d \to \infty$, the product consists of a subset of factors of the convergent product $\zeta(s)$ for $s = \frac{d(m-1)}{m}, d+1$ respectively. Thus the limit is necessarily 1.

For $L_1^{\text{med}}(m,d)$ the conclusion requires more work. First, observe that since the product in $L_1^{\text{med}}(m,d)$ runs over primes congruent to 1 modulo m, we have $p \geq m+1$. This implies

$$1 - \left(1 - \frac{p-1}{mp}\right)^{d+1} \geq 1 - \left(\frac{m}{m+1}\right)^{d+1}.$$

Thus we have

$$1 \geq L_1^{\text{med}}(m,d) \geq \prod_{\substack{p\equiv 1(m) \\ d<p<(m-1)^2(d-2)^2}} \left(1 - \left(\frac{m}{m+1}\right)^{d+1}\right) \geq \prod_{\substack{p\equiv 1(m) \\ p<(m-1)^2(d-2)^2}} \left(1 - \left(\frac{m}{m+1}\right)^{d+1}\right).$$

We can compute the limit of the rightmost expression as $d \to \infty$ by taking logarithms.

Use $\pi_{1,m}(X)$ to denote the number of primes $p \equiv 1 \pmod{m}$ with $p \leq X$, so

$$\log \prod_{\substack{p \equiv 1(m) \\ p < (m-1)^2(d-2)^2}} \left(1 - \left(\frac{m}{m+1}\right)^{d+1}\right) = \left(\pi_{1,m}((m-1)^2(d-2)^2 - 1)\right) \log \left(1 - \left(\frac{m}{m+1}\right)^{d+1}\right).$$

Using the Taylor series for the logarithm, we have

$$\begin{aligned} \left|\log\left(1 - \left(\frac{m}{m+1}\right)^{d+1}\right)\right| &= \sum_{j \geq 1} \frac{1}{j} \left(\frac{m}{m+1}\right)^{(d+1)j} \\ &\leq \sum_{j \geq 1} \left(\frac{m}{m+1}\right)^{(d+1)j} \\ &= \frac{(\frac{m}{m+1})^{d+1}}{1 - (\frac{m}{m+1})^{d+1}}. \end{aligned}$$

Finally, we observe that upon taking limits, we have

$$\lim_{d \to \infty} \pi_{1,m}((m-1)^2(d-2)^2 - 1) \frac{(\frac{m}{m+1})^{d+1}}{1 - (\frac{m}{m+1})^{d+1}} = 0,$$

since the exponential $(\frac{m}{m+1})^{d+1}$ decays more quickly than $\pi_{1,m}((m-1)^2(d-2)^2 - 1)$, which is bounded above by a (fixed) polynomial in d.

Thus as d grows, $L_1^{\text{med}}(m,d)$ sits in between 1 and another product approaching 1, so we must have $\lim_{d \to \infty} L_1^{\text{med}}(m,d) = 1$. □

This gives us a way to see where these lower bounds are going for a fixed prime m dividing d as d grows, in an entirely computable way. We can restate this as follows.

Corollary 4.3.13. *Let m be a fixed odd prime. Then*

$$\liminf_{d \to \infty} \rho_{m,d} \geq \left(1 - \frac{1}{m^{m+1}}\right) \prod_{p \equiv 1(m)} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right) \prod_{p \not\equiv 0,1(m)} \left(1 - \frac{1}{p^{2(p+1)}}\right).$$

When $m = 2$ we have

$$\liminf_{d \to \infty} \frac{\rho_{2,d}}{\rho_{2,d}(\infty)} \geq \frac{7}{8} \prod_{p > 2} \left(1 - \left(1 - \frac{p-1}{2p}\right)^{p+1}\right) \approx 0.66120.$$

Proof. By Corollary 4.3.10 and Lemma 4.3.12, we need only take the limits of $L_0(m,d)$, $L_1^{\mathrm{sm}}(m,d)$, and $L_{\neq 1}^{\mathrm{sm}}(m,d)$ as $d \to \infty$, since $L_1^{\mathrm{med}}(m,d), L_1^{\mathrm{big}}(m,d)$, and $L_{\neq 1}^{\mathrm{big}}$ can all be made arbitrarily close to 1.

In the case of $m = 2$, Corollary 4.3.10 applies to the local densities at the finite places, but $\rho_{2,d}(\infty) \neq 1$. Thus by taking a limit as $d \to \infty$, we obtain a lower bound for $\liminf_{d\to\infty} \frac{\rho_{2,d}}{\rho_{2,d}(\infty)}$. □

Moreover, the infinite products in Corollary 4.3.13 are straightforward to compute to several decimal places of precision. By recognizing that $p \geq m+1$ in the first product, we have that

$$\prod_{p\equiv 1(m)} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right) \geq \prod_{\substack{p\equiv 1(m)\\ p\leq A}} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right) \prod_{\substack{p\equiv 1(m)\\ p> A}} \left(1 - \left(\frac{m}{m+1}\right)^{p+1}\right).$$

The rightmost factor is seen to converge to 1 quickly, e.g. by taking logarithms and comparing to a geometric series. In fact, we have

$$\prod_{\substack{p\equiv 1(m)\\ p> A}} \left(1 - \left(\frac{m}{m+1}\right)^{p+1}\right) \geq 1 - \left(\frac{m}{m+1}\right)^{A+1}, \tag{4.3.5}$$

so we may choose A large enough so this factor is as close to 1 as desired. It remains to compute the factors for the finitely many $p \leq A$. Furthermore, this is quite well behaved in m, in that for any level of precision, we need only choose A to be a sufficiently large multiple Cm, where C does not depend on m.

For the other factor, we employ a similar strategy and compare to the Riemann zeta function,

$$\prod_{p\not\equiv 0,1(m)} \left(1 - \frac{1}{p^{2(p+1)}}\right) \geq \prod_{\substack{p\not\equiv 0,1(m)\\ p\leq B}} \left(1 - \frac{1}{p^{2(p+1)}}\right) \prod_{p> B} \left(1 - \frac{1}{p^{2(B+2)}}\right). \tag{4.3.6}$$

The rightmost factor is the tail of $\zeta(2B+4)^{-1}$, which converges to 1 rapidly. For example,

taking $B = 10$ is sufficient to show

$$\prod_{p\not\equiv 0,1(m)} \left(1 - \frac{1}{p^{2(p+1)}}\right) \geq \frac{1}{\zeta(24)} \prod_{\substack{p\not\equiv 0,1(m)\\ p\leq 10}} \left(1 - \frac{1}{p^{2(p+1)}}\right) \prod_{p\leq 10} \left(1 - \frac{1}{p^{24}}\right)^{-1}.$$

When $m > 7$, the first product runs over all primes up to 10, producing the lower bound of at least 0.98422.

Corollary 4.3.14. *Let m be a fixed odd prime. Then*

$$\liminf_{d\to\infty} \rho_{m,d} \geq 0.83511.$$

Proof. Direct computation shows the result holds for $m = 3, 5, 7$; see Example 4.3.17. Suppose now that $m \geq 11$ is an odd prime. By the above discussion, using (4.3.6) with $B = 10$, we have

$$\prod_{p\not\equiv 0,1(m)} \left(1 - \frac{1}{p^{2(p+1)}}\right) \geq 0.98422...$$

and we note that $1 - \frac{1}{m^{m+1}} \geq 1 - \frac{1}{11^{12}}$, so it remains to bound the $\prod_{p\equiv 1(m)} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right)$ factor from below for an arbitrary prime $m \geq 11$.

Using (4.3.5) with $A = 20m$, we observe that if $p \equiv 1 \pmod{m}$ for $p \leq 20m$, then $p = 2km + 1$ for some $1 \leq k \leq 9$. Furthermore, we have $3 \mid 2km + 1$ for three such values of k, so we can omit those k's. Since these factors are increasing in p, we achieve a lower bound by omitting $k = 3, 6, 9$. We have then

$$\prod_{\substack{p\equiv 1(m)\\ p\leq A}} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right) \geq \prod_{k=1,2,4,5,7,8} \left(1 - \left(1 - \frac{2km}{m(2km+1)}\right)^{2km+2}\right),$$

$$\prod_{\substack{p\equiv 1(m)\\ p> A}} \left(1 - \left(\frac{m}{m+1}\right)^{p+1}\right) \geq 1 - \left(\frac{m}{m+1}\right)^{20m+1} \geq 1 - \left(\frac{11}{12}\right)^{221} \approx 0.999999995.$$

For the latter, we can take $m = 11$, as the right hand side is seen to be increasing in m. This factor is very nearly 1, and thus will have negligible impact. For the former, we observe the

right hand side is decreasing in m, so it suffices to take a limit as $m \to \infty$. We have

$$\lim_{m\to\infty}\left(1-\left(1-\frac{2km}{m(2km+1)}\right)^{2km+2}\right) = 1-e^{-2k},$$
$$\implies \prod_{\substack{p\equiv 1(m)\\ p\leq A}}\left(1-\left(1-\frac{p-1}{mp}\right)^{p+1}\right) \geq \prod_{k=1,2,4,5,7,8}\left(1-e^{-2k}\right) \approx 0.84850.$$

Taken together, this verifies the claim for $m \geq 11$. □

4.3.3 Examples

In this subsection, we compute numerical lower bounds for $\rho_{m,d}$ for selected (m, d) values. The reader primarily interested in such numerical values — especially for d sufficiently large relative to a fixed m — may find these lower bounds sufficient for their purposes without going through the considerable additional effort of computing local densities $\rho(p)$ exactly, as we do later only in the case of $(m, d) = (3, 6)$.

The computations referenced in the following examples are detailed in the GitHub repository [BK21b, `SEC_lowerbound_examples_28Aug21.ipynb`], available at

https://github.com/c-keyes/Density-of-locally-soluble-SECs/blob/main/SEC_lowerbound_examples_28Aug21.ipynb.

Example 4.3.15 $(m = 3, d = 6)$**.** In the case where $(m, d) = (3, 6)$ the genus of C_f is generically 4. We can use Corollary 4.3.10 to bound $\rho_{3,6}$ by computing

$$\begin{aligned}
L_0(3,6) &= 1 - \frac{1}{3^3} = \frac{26}{27},\\
L_1^{\mathrm{sm}}(3,6) &= 1,\\
L_1^{\mathrm{med}}(3,6) &= \prod_{\substack{p\equiv 1(3)\\ p\leq 61}} \left(1 - \left(1 - \frac{p-1}{3p}\right)^7\right) \approx 0.59724,\\
L_1^{\mathrm{big}}(3,6) &= \prod_{\substack{p\equiv 1(3)\\ p>61}} \left(1 - \frac{1}{p^4}\right) = \prod_{\substack{p\equiv 1(3)\\ p\leq 61}} \left(1 - \frac{1}{p^4}\right)^{-1} \prod_{p\equiv 1(3)} \left(1 - \frac{1}{p^4}\right) \approx 0.9999998,\\
L_{\neq 1}^{\mathrm{sm}}(3,6) &= \left(1 - \frac{1}{2^6}\right) = \frac{63}{64},\\
L_{\neq 1}^{\mathrm{big}}(3,6) &= \prod_{\substack{p\equiv 2(3)\\ p>2}} \left(1 - \frac{1}{p^7}\right) = \left(1 - \frac{1}{2^7}\right)^{-1} \prod_{p\equiv 2(3)} \left(1 - \frac{1}{p^7}\right) \approx 0.999987,
\end{aligned}$$

to find that

$$\rho_{3,6} \geq 0.56612.$$

That is, at least 56% of curves $y^3 = f(x, z)$ over $\mathbb{Q}$ with $\deg f = 6$ are locally soluble. Note that the infinite products $\prod_{p\equiv 1(3)} \left(1 - \frac{1}{p^4}\right)$ and $\prod_{p\equiv 2(3)} \left(1 - \frac{1}{p^7}\right)$ above are termed Euler modulo products and denoted $\zeta_{3,1}(4)$ and $\zeta_{3,2}(7)$ respectively in [Mat10, see p. 25], and the values used in the above computations were taken from that paper.

There is room for improvement in the lower bound above for $L_1^{\mathrm{med}}(3, 6)$, due to the fact that we expect Proposition 4.3.6 to be missing many liftable points; see Remark 4.3.7. Since there are only seven primes involved in $L_1^{\mathrm{med}}(3, 6)$, one may use a computer algebra system to enumerate all sextic forms $f(x, z)$ and search for points that lift. The results are tabulated in Table 4.3.1. See §4.6 for a more detailed description of this approach.

We can then take the product of these lower bounds and use them in place of $L_1^{\mathrm{med}}(3, 6)$ in the calculations above, producing

$$\rho_{3,6} \geq 0.93134.$$

Table 4.3.1: Lower bounds for $\rho_{3,6}(p)$ for primes $p \equiv 1 \pmod 3$ up to $p = 61$

p	$\rho_{3,6}(p) \geq$
7	$\frac{810658}{823543} \approx 0.98435$
13	$\frac{62655132}{62748517} \approx 0.99851$
19	$\frac{893660256}{893871739} \approx 0.99976$
31	$\frac{27512408250}{27512614111} \approx 0.99999$
37	$\frac{94931742132}{94931877133} \approx 0.999998$
43	$\frac{271818511748}{271818611107} \approx 0.9999996$
61	$\frac{3142742684700}{3142742836021} \approx 0.99999995$

Example 4.3.16 $(m = 5, d = 5)$**.** In the case where $(m, d) = (5, 5)$, we use Corollary 4.3.10 to obtain

$$\begin{aligned}
L_0(5,5) &= 1 - \frac{1}{5^4} = 0.9984, \\
L_1^{\text{sm}}(5,5) &= 1, \\
L_1^{\text{med}}(5,5) &= \prod_{\substack{p \equiv 1(5) \\ p \leq 131}} \left(1 - \left(1 - \frac{p-1}{5p}\right)^6\right) \approx 0.10671, \\
L_1^{\text{big}}(5,5) &= \prod_{\substack{p \equiv 1(5) \\ p > 131}} \left(1 - \frac{1}{p^4}\right) \approx 0.999999994, \\
L_{\neq 1}^{\text{sm}}(5,5) &= 1, \\
L_{\neq 1}^{\text{big}}(5,5) &= \prod_{p \not\equiv 0,1(5)} \left(1 - \frac{1}{p^6}\right) \approx 0.98301.
\end{aligned}$$

Putting these together with Corollary 4.3.10 yields the following (albeit somewhat disappointing) bound,

$$\rho_{5,5} \geq 0.10473.$$

As with Example 4.3.15, the primes $p \equiv 1 \pmod 5$ which are too small for Proposition 4.3.2 to apply are the limiting factor in this approach. We again improve these values with a computer search as described in §4.6, and tabulate them below in Table 4.3.2

Table 4.3.2: Lower bounds for $\rho_{5,5}(p)$ for primes $p \equiv 1 \pmod 5$ up to $p = 131$

p	$\rho_{3,6}(p) \geq$
11	$\frac{1729840}{1771561} \approx 0.97644$
31	$\frac{887443392}{887503681} \approx 0.99993$
41	$\frac{4750102896}{4750104241} \approx 0.9999997$
61	$\frac{51520371384}{51520374361} \approx 0.99999994$
71	$\frac{128100279888}{128100283921} \approx 0.99999996$
101	$\frac{1061520142440}{1061520150601} \approx 0.999999992$
131	$\frac{5053913130552}{5053913144281} \approx 0.999999997$

This produces the considerable improvement

$$\rho_{5,5} \geq 0.95826,$$

demonstrating once again the outsize impact that small primes have on the adelic density, as well as the limitations of Proposition 4.3.6.

We also note that these computations revealed that for all $p > 31$, irreducible curves of the form $y^5 = \overline{f}(x, z)$ where $\deg f = 5$ possess a smooth $\mathbb{F}_p$-point, and hence a lift $y^5 = f(x, z)$ possesses a $\mathbb{Q}_p$-point. This improves on the range of validity for Proposition 4.3.2 in the case when $m = 5$ and $d = 5$.

Example 4.3.17 ($d \to \infty$)**.** For a fixed prime m, we consider the behavior of the lower bound for $\rho_{m,d}$ given by Corollary 4.3.10 as d grows. For example, taking $m = 3$, we compute a lower bound for $\rho_{m,d}$ using Corollary 4.3.10 for several values of d. These lower bounds, and the approximate values of L_1^{sm}, L_1^{med}, and $L_{\neq 1}^{\mathrm{sm}}$ are included in the Table 4.3.3 below.

Note that $L_1^{\mathrm{med}}(3, d)$ is increasing with d, as expected by Lemma 4.3.12. Using Corollary 4.3.13 and the ensuing discussion, we can quickly compute a decimal approximation of a

Table 4.3.3: Lower bounds for $\rho_{3,d}(p)$ for small d via Corollary 4.3.10

d	$L_1^{\mathrm{sm}}(3,d) \approx$	$L_1^{\mathrm{med}}(3,d) \approx$	$L_{\neq 1}^{\mathrm{sm}}(3,d) \approx$	$\rho_{3,d} \geq$
6	1	0.59723	0.98437	0.56612
9	0.93223	0.69389	0.98437	0.62890
12	0.93223	0.81839	0.98437	0.74174
15	0.92682	0.91381	0.98437	0.82342
18	0.92682	0.96277	0.98437	0.86753
21	0.92635	0.98536	0.98437	0.88744

lower bound for $\liminf_{d\to\infty} \rho_{3,d}$. Taking $A = 60$ in (4.3.5) and $B = 10$ in (4.3.6), we find

$$\prod_{p\equiv 1(3)} \left(1 - \left(1 - \frac{p-1}{3p}\right)^{p+1}\right) \geq 0.92635,$$
$$\prod_{p\equiv 2(3)} \left(1 - \frac{1}{p^{2(p+1)}}\right) \geq 0.98437,$$

so

$$\liminf_{d\to\infty} \rho_{3,d} \geq 0.90061.$$

Below in Table 4.3.4, we compute a lower bound for $\liminf_{d\to\infty}$ for other small prime exponents m, where we take $A = 20m$ and $B = 10$ to compute the necessary infinite products, as above.

Table 4.3.4: Lower bounds for $\liminf_{d\to\infty} \rho_{m,d}$ via Corollary 4.3.13 for selected odd primes m

m	$\liminf_{d\to\infty} \rho_{m,d}(p) \geq$	m	$\liminf_{d\to\infty} \rho_{m,d}(p) \geq$
3	0.90061	⋮	⋮
5	0.89457	103	0.98183
7	0.97143	107	0.98156
11	0.87167	109	0.98418
13	0.96823	113	0.85336
17	0.98206	127	0.96662
19	0.98418	⋮	⋮
23	0.86036	1009	0.98417
29	0.85968	1013	0.84918
31	0.98418	1019	0.85128
37	0.96546	1021	0.98417
41	0.85737	⋮	⋮

We make a few brief observations about Table 4.3.4. First is that these methods will not produce lower bounds exceeding $\prod_{p\not\equiv 0,1(m)}\left(1-\frac{1}{p^{2(p+1)}}\right)$. In particular, when $m>7$ above, our lower bounds do not exceed 0.98422. However some m values come quite close, e.g. $m=19,31,109,1009,1021$, indicating that for such primes, to improve our lower bounds for $\rho_{m,d}$, we need to improve our bounds for $L^{\mathrm{sm}}_{\neq 1}(m,d)$.

Note the drops present at several m values, e.g. $m=11,23,29,113,1013,1019$. These can be explained by considering the smallest prime $p\equiv 1 \pmod m$. For example, when $m=7$, the smallest prime $p\equiv 1 \pmod 7$ is $p=29$, while the smallest prime $p\equiv 1 \pmod{11}$ is lower at $p=23$. The small primes have an outsize impact on our lower bounds for the infinite product $\prod_{p\equiv 1(m)}\left(1-\left(1-\frac{p-1}{mp}\right)^{p+1}\right)$.

Example 4.3.18 ($m=4$)**.** To illustrate the similarities and differences when m is composite, consider $m=4$ and d a multiple of 4. While we cannot apply Corollaries 4.3.10 or 4.3.13 directly, the methods of this section nevertheless apply to determine $\rho_{4,d}(p)$ for the finite primes p.

For the prime $p=2$ and primes $p\equiv 1 \pmod 4$, Propositions 4.3.2, 4.3.6, and 4.3.9 apply as usual, with the genus $g_0=\frac{3(d-2)}{2}$. If $p\equiv 3 \pmod 4$, we observe that $\left(\mathbb{F}_p^\times\right)^4=\left(\mathbb{F}_p^\times\right)^2$, so C_f has an $\mathbb{F}_p$-point if and only if the hyperelliptic curve $y^2-f(x,z)$ has one. This allows us to apply the result of Proposition 4.3.2 for all primes $p\equiv 1 \pmod 4$ such that $p\geq (d-2)^2$, instead of $p\geq 4g_0^2$. Thus whenever $d\geq 8$ we have

$$\frac{\rho_{4,d}}{\rho_{4,d}(\infty)}\geq \frac{7}{8}\prod_{\substack{p\equiv 1(4)\\ p<d}}\left(1-\left(1-\frac{p-1}{4p}\right)^{p+1}\right)\prod_{\substack{p\equiv 1(4)\\ d\leq p<4g_0^2}}\left(1-\left(1-\frac{p-1}{4p}\right)^{p+1}\right)\prod_{\substack{p\equiv 1(4)\\ p\geq 4g_0^2}}\left(1-\frac{1}{p^{d/2}}\right)$$
$$\times\prod_{\substack{p\equiv 3(4)\\ p<d}}\left(1-\left(1-\frac{p-1}{2p}\right)^{p+1}\right)\prod_{\substack{p\equiv 3(4)\\ d\leq p<(d-2)^2}}\left(1-\left(1-\frac{p-1}{2p}\right)^{p+1}\right)\prod_{\substack{p\equiv 3(4)\\ p\geq (d-2)^2}}\left(1-\frac{1}{p^{d/2}}\right).$$

In the case of $d=4$ we replace $7/8$ by $3/4$ to account for the behavior at $p=2$.

For small values of d, this produces the values in Table 4.3.5. In the limit as $d\to\infty$, we find

$$\liminf_{d\to\infty}\frac{\rho_{4,d}}{\rho_{4,d}(\infty)}\geq 0.49471,$$

which is slightly worse than the lower bound for $m = 2$ case computed in Example 4.3.17, as one might expect, given that for primes $p \equiv 1 \pmod 4$ there are fewer quartic residues in $\mathbb{F}_p$.

To deal with the infinite place, we observe that C_f has a real point precisely when $f(x, z)$ takes a positive value. When m is even and $d = 4$, [BCF21] rigorously show $\rho_{m,4}(\infty) \geq 0.873914$. For $4 \leq d \leq 20$, we obtained the approximations for $\rho_{m,d}(\infty)$ using a Monte Carlo approach with 10^7 samples and recorded them in Table 4.3.5.

Table 4.3.5: Lower bounds for $\rho_{4,d}/\rho_{4,d}(\infty)$ and approximations of $\rho_{4,d}(\infty)$ for small d

d	$\rho_{4,d}/\rho_{4,d}(\infty) \geq$	$\rho_{4,d}(\infty) \approx$
4	0.10125	0.8739562
8	0.01711	0.9183913
12	0.03419	0.9378118
16	0.08218	0.9493136
20	0.14848	0.9568297

4.4 Upper bounds for the proportion

In this section, we consider obstructions to local solubility to give upper bounds on $\rho_{m,d}(p)$, and thus $\rho_{m,d}$. Our primary goal is to show that even in the limit as $d \to \infty$, strictly fewer than 100% of superelliptic curves are everywhere locally soluble; see Corollary 4.4.2. For this, it is sufficient to study the behavior at $p = 2$.

Lemma 4.4.1. *Fix an integer $m \geq 2$ and suppose $d \geq 6$ is divisible by m. Then*

$$\rho_{m,d}(2) \leq 1 - \frac{1}{2^9} + \frac{1}{2^{d+4}}.$$

Proof. Consider the degree d forms $f(x, z)$ which reduce modulo 2 as

$$\overline{f}(x, z) = h(x, z)x^2(x + z)^2z^2 \tag{4.4.1}$$

for $h(x, z) \in \mathbb{F}_2[x, z]$ a nonzero form of degree $d - 6$. There are $2^{d+1-6} - 1$ such forms, so the probability that $f(x, z)$ reduces this way is $\frac{1}{2^6} - \frac{1}{2^{d+1}}$.

We now claim that if $f(x,z)$ satisfies (4.4.1) then the probability of $y^m = f(x,z)$ having no $\mathbb{Q}_2$-solutions is at least $\frac{1}{8}$. Consider first a solution $[x:y:1] \equiv [0:0:1] \pmod 2$, i.e. $x, y \in 2\mathbb{Z}_2$. A necessary condition for such a solution to exist is for $2^2 \mid c_0$, which occurs with probability $\frac{1}{2}$. The same argument shows that $2^2 \mid c_d$ and $2^2 \mid \sum_{i=0}^{d} c_i$ are necessary for the $\mathbb{F}_2$-solutions $[1:0:1]$ and $[1:0:0]$ to lift to $\mathbb{Q}_2$-solutions, each occurring with probability $1/2$. Thus the chance of none of these necessary conditions being met is $1/8$.

Combining this with our earlier calculation, we may compute a lower bound for the probability of $f(x,z)$ for which C_f has no $\mathbb{Q}_2$-points, hence

$$1 - \rho_{m,d}(2) \geq \frac{1}{8}\left(\frac{1}{2^6} - \frac{1}{2^{d+1}}\right) = \frac{1}{2^9} - \frac{1}{2^{d+4}}.$$

Rearranging the inequality gives the desired result. □

Taking limits as $d \to \infty$, we obtain upper bounds for the limiting behavior of $\rho_{m,d}$, complementing Corollary 4.3.14.

Corollary 4.4.2. *Fix an integer $m \geq 2$. Then*

$$\limsup_{d\to\infty} \rho_{m,d} \leq 1 - \frac{1}{2^9} \approx 0.99804.$$

Proof. We make the trivial observation that $\rho_{m,d} \leq \rho_{m,d}(2)$ and apply Lemma 4.4.1. Since this bound is uniform in d (and in fact in m) we can take the limit as $d \to \infty$. □

We conclude this section by turning our attention to primes p more generally. Following the convention established in §4.7, let $N_{d,0}$ denote the number of binary degree d forms in $\mathbb{F}[x,z]$ up to scaling which have no roots. Let $N_{d,\mathrm{irr}}$ denote the number of irreducible such forms. We have the trivial observation that $N_{d,\mathrm{irr}} \leq N_{d,0}$. In the following lemma only, we use μ to denote the usual Möbius function.

Lemma 4.4.3. *Fix positive integers $m \geq 2$ and d divisible by m such that $(m,d) \neq (2,2)$. Then*

$$\rho_{m,d}(p) \leq 1 - \frac{p-1}{p^{2d+2} - p^{d+1}} N_{d,0} \leq 1 - \frac{p-1}{d\left(p^{2d+2} - p^{d+1}\right)} \sum_{e \mid d} \mu\left(\frac{d}{e}\right) p^e.$$

Proof. Suppose $\overline{f}(x,z) = 0$, which occurs with probability $\frac{1}{p^{d+1}}$. Then for any point on C_f, we must have $p \mid y$. Since $m \geq 2$, this implies $p^2 \mid f(x,z)$, or equivalently that $[x:z]$ is a root of $\frac{1}{p}f(x,z)$. If $\frac{1}{p}f(x,z)$, viewed as a binary form of degree d up to scaling over $\mathbb{F}_p$, has no roots, then C_f is insoluble. This proves the first inequality, since we have shown

$$1 - \rho_{m,d}(p) \geq \frac{1}{p^{d+1}} \left(\frac{N_{d,0}}{p^d + p^{d-1} + \cdots + p + 1} \right) = \frac{1}{p^{d+1}} \left(\frac{(p-1)N_{d,0}}{p^{d+1} - 1} \right).$$

For the second inequality, we use the observation that $N_{d,\mathrm{irr}} \leq N_{d,0}$. We also have that, up to scaling, we may assume that an irreducible degree d form is monic. A standard result in elementary number theory shows

$$N_{d,\mathrm{irr}} = \frac{1}{d} \sum_{e \mid d} \mu\left(\frac{d}{e}\right) p^e,$$

see e.g. [IR90, §7.2, Corollary 2], and this is sufficient to yield the second inequality. □

While Lemma 4.4.3 is not suitable for giving nontrivial upper estimates for $\rho_{m,d}$ as $d \to \infty$, it is sufficient to allow us to conclude $\rho_{m,d}(p) < 1$ for all primes p. In the case where $(m,d) = (3,6)$ and $p \equiv 2 \pmod 3$, Lemma 4.7.1 states that $N_{6,0} \sim \frac{53}{144}p^6$; thus the bound in Lemma 4.4.3 asymptotically becomes

$$1 - \rho_{3,6}(p) \gg \frac{53}{144} p^{-7},$$

which is seen to be sharp by Theorem 4.1.5.

4.5 An exact formula for the $m = 3$ and $d = 6$ case

The goal of this section is to prove Theorem 4.1.5, giving an exact formula for $\rho_{m,d}(p)$ when $m = 3$ and $d = 6$. As in §4.3, the idea is to study when C has solutions modulo p^n which may be lifted via Hensel's lemma. Here however, we must be more careful in dealing with the case that these points may not be smooth. Some of the strategies we employ resemble those of [BCF21] for genus one curves, but here there are far more cases to check. We also comment that this strategy to achieve exact density formulas may not generalize well to

cases of larger m (see Remark 4.5.20).

We lay out the idea of the argument below in §4.5.1, detailing the five cases of interest. In §4.5.2, we give geometric arguments to deal with three (easier) cases. §4.5.3 contains intermediate results which will be used multiple times thereafter, giving a flavor for the type of argument to compute exact local densities. The final two cases are then handled in §4.5.4 and §4.5.5, culminating in the proof of Theorem 4.1.5 in §4.5.5.

4.5.1 Setup

Let $m = 3$, $d = 6$, and F the defining polynomial of C_f for $f(x, z)$ a binary sextic form,

$$F = y^3 - f(x, z) = y^3 - c_6x^6 - c_5x^5z - c_4x^4z^2 - c_3x^3z^3 - c_2x^2z^4 - c_1xz^5 - c_0z^6. \quad (4.5.1)$$

Let $\overline{F} \in \mathbb{F}_p[x, y, z]$ denote the image under the reduction modulo p map. As we will see in Lemma 4.5.2 there are five possible ways that $\overline{F}$ could factor in $\overline{\mathbb{F}_p}[x, z][y]$:

1. $\overline{F}$ is absolutely irreducible;
2. $\overline{F}$ has three distinct linear factors over $\mathbb{F}_p$, i.e. $\overline{F} = \prod_{i=1}^{3}(y - h_i(x, z))$ for binary quadratic forms $h_i(x, z) \in \mathbb{F}_p[x, z]$;
3. $\overline{F}$ has a linear factor over $\mathbb{F}_p$ and a pair of conjugate factors over $\mathbb{F}_{p^2}$, i.e. $\overline{F} = (y - h(x, z))(y - g_1(x, z))(y - g_2(x, z))$ for binary quadratic forms $h(x, z) \in \mathbb{F}_p[x, z]$, and a conjugate pair $g_1, g_2 \in \mathbb{F}_{p^2}[x, z]$;
4. $\overline{F}$ has three conjugate factors over $\mathbb{F}_{p^3}$, $\overline{F} = \prod_{i=1}^{3}(y - g_i(x, z))$;
5. $\overline{F}$ has a triple root, $\overline{F} = (y - h(x, z))^3$ where $h(x, z) \in \mathbb{F}_p[x, z]$.

Remark 4.5.1. More generally, one could study factorization of weighted homogeneous polynomials

$$y^3 + h(x, z)y^2 + g(x, z)y + f(x, z),$$

similar to the generalized binary quartics of [BCF21], and obtain more diverse factorization types. Since we are interested in superelliptic curves, we will stick to the five factorization types above.

We define an auxiliary condition $(*)$, which is satisfied by F if and only if $\overline{c_6} \notin \mathbb{F}_p^3$. Equivalently, we have

$$F \text{ satisfies } (*) \iff y^3 - c_6 \text{ is irreducible in } \mathbb{F}_p[y]. \tag{4.5.2}$$

If F satisfies $(*)$ then C_f has no point at infinity modulo p, as $\overline{F}(1, y, 0) = 0$ has no solutions. It is analogous to the condition $(*)$ as defined in [BCF21] and plays a similar role, making appearances in §4.5.4 and §4.5.5. We denote by $\rho^*(p)$ the local density of curves for which F satisfies condition $(*)$.

The first thing we need to know is how often each of the factorization types 1 — 5 appear for $\overline{F}$. This is computed below for all $\overline{F}$ and for those satisfying condition $(*)$ in Lemma 4.5.2.

Lemma 4.5.2. *Let $\overline{F}$ correspond to the reduction of a superelliptic curve of the form (4.5.1). The table below indicates the frequencies for which each factorization type 1 – 5 appear, as (the reductions of) $c_6, \dots c_0$ range from 0 to $p-1$.*

Factorization type	$p = 3$	$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
1. Abs. irr.	*2160*	$p^3(p^4-1)$	$p^3(p^4-1)$
2. 3 distinct linear over $\mathbb{F}_p$	*0*	$\frac{1}{3}(p^3-1)$	*0*
3. Linear + conj.	*0*	*0*	p^3-1
4. 3 conjugate factors	*0*	$\frac{2}{3}(p^3-1)$	*0*
5. Triple factor	*27*	*1*	*1*
Total	3^7	p^7	p^7

The following table lists the analogous counts of factorization types when condition $(*)$ is satisfied.

Factorization type	$p = 3$	$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
1. Abs. irr.	*0*	$\frac{2}{3}p^2(p-1)(p^4-1)$	*0*
2. 3 distinct linear over $\mathbb{F}_p$	*0*	*0*	*0*
3. Linear + conj.	*0*	*0*	*0*
4. 3 conjugate factors	*0*	$\frac{2}{3}p^2(p-1)$	*0*
5. Triple factor	*0*	*0*	*0*
Total	*0*	$\frac{2}{3}p^6(p-1)$	*0*

Proof. Assume for the moment that $p \neq 3$. If $\overline{F}$ is not absolutely irreducible over $\mathbb{F}_p$, then by Lemma 4.2.3 we must have $\overline{f}(x,z) = ah(x,z)^3$ for $a \in \mathbb{F}_p$ and $h \in \mathbb{F}_p[x,z]$. We may further assume that h has leading term 1. Thus $\overline{F}$ factors as

$$\overline{F} = (y - \alpha h(x,z))(y - \omega\alpha h(x,z))(y - \omega^2\alpha h(x,z))$$

where $\alpha^3 = a$ and ω is a primitive third root of unity defined possibly over $\mathbb{F}_{p^2}$. It is now clear that the five listed possibilities are the only possible factorizations of $\overline{F}$, and the only way to find a triple factor is if $h_0 = 0$, so $\overline{F} = y^3$.

Assume now that $\overline{f} \neq 0$ and consider $p \equiv 1 \pmod 3$. Then $\omega \in \mathbb{F}_p$, so $\overline{F}$ has either 3 linear factors over $\mathbb{F}_p$ or three conjugate factors over $\mathbb{F}_{p^3}$, depending on the value of a, putting us in type 2 or 4. We know that there are $\frac{p-1}{3}$ nonzero cubic residues and $\frac{2(p-1)}{3}$ nonresidues mod p, so we obtain the stated counts by recognizing that there are p^2+p+1 ways to choose h for each nonzero value of a.

Assume now that $p \equiv 2 \pmod 3$. In this case, the cube map is an isomorphism of $\mathbb{F}_p^\times$, but $\omega \notin \mathbb{F}_p$, so we must be in type 3, because a is always in $\mathbb{F}_p^\times$. Hence there are again $(p-1)(p^2+p+1) = p^3 - 1$ ways in which $\overline{F}$ is reducible, this time all landing in type 3.

In either case, we have exhausted the possibilities for which $\overline{F}$ is (absolutely) reducible. Since there were p^3 of these in total, we are left with $p^7 - p^3$ occurrences of type 1.

Condition $(*)$ can only be satisfied in the case that $p \equiv 1 \pmod 3$, because otherwise there exists a root to $y^3 - c_6 \equiv 0 \pmod p$. Since there are $\frac{2}{3}(p-1)$ nonzero cubic nonresidues that could be the residue of c_6, and the other coefficients of $\overline{F}$ may be chosen freely, there are $\frac{2}{3}p^6(p-1)$ total choices of $\overline{F}$ satisfying $(*)$. These clearly cannot come from a triple

factor or distinct linear factors over $\mathbb{F}_p$, so the only possibilities are types 1 or 4. Since we need the x^2 term of h to be nonzero, there are only $\frac{2}{3}p^2(p-1)$ ways to factor in type 4 while satisfying condition $(*)$, and subtracting this from the total gives the frequency of type 1.

Now we consider the case of $p = 3$. Since $\overline{\mathbb{F}_3}$ is characteristic 3, if $\overline{F}$ is reducible, we have $\overline{F} = y^3 - h(x,z)^3 = (y - h(x,z))^3$. Thus there are $3^3 = 27$ ways to choose $h(x,z)$ in this case, all of which give rise to a triple factor. The remaining $3^7 - 3^3 = 2160$ choices of $\overline{F}$ must all be absolutely irreducible over $\mathbb{F}_3$. □

Let ξ_i denote the density of the set of $f(x,z)$ for which $F = y^3 - f(x,z)$ has reduction $\overline{F}$ with factorization type i for $1 \le i \le 5$. Similarly, let ξ_i^* denote the density of $f(x,z)$ for which the associated F also satisfies condition $(*)$. The counts of Lemma 4.5.2 allow us to compute ξ_i and ξ_i^* directly.

Corollary 4.5.3. *The densities ξ_i are given by the table below.*

ξ_i	$p = 3$	$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
ξ_1	*80/81*	$1 - \frac{1}{p^4}$	$1 - \frac{1}{p^4}$
ξ_2	*0*	$\frac{1}{3p^7}(p^3 - 1)$	*0*
ξ_3	*0*	*0*	$\frac{1}{p^7}(p^3 - 1)$
ξ_4	*0*	$\frac{2}{3p^7}(p^3 - 1)$	*0*
ξ_5	*1/81*	$\frac{1}{p^7}$	$\frac{1}{p^7}$

If $p \equiv 1 \pmod 3$ and F satisfies condition $(*)$, the nonzero densities ξ_i^* are

$$\xi_1^* = 1 - \frac{1}{p^4}, \qquad \xi_4^* = \frac{1}{p^4}.$$

Returning to local solubility, suppose the reduction of F as given in (4.5.1) has factorization type i and let σ_i denote the density of F possessing a $\mathbb{Q}_p$ solution. Let σ_i^* denote the density of F with factorization type i satisfying $(*)$ having a $\mathbb{Q}_p$-solution. Then we have

$$\rho(p) = \sum_{i=1}^{5} \xi_i \sigma_i, \tag{4.5.3}$$

$$\rho^*(p) = \xi_1^* \sigma_1^* + \xi_4^* \sigma_4^*. \tag{4.5.4}$$

Thus to obtain an exact formula for the local density $\rho(p)$, we may consider separately the local densities σ_i with prescribed factorization types.

Along the way, we will also need to know the frequency of various factorization types for binary forms of degrees up to 6. In the proofs of Lemmas 4.5.17, 4.5.19, and 4.5.21 for instance, it is often useful to know the the proportion of such forms having types of roots. Namely, having no roots can be used to see that there are no points, while having a simple root implies the existence of a $\mathbb{Q}_p$-point by Hensel lifting arguments. We will also need to know how often roots have higher multiplicities to determine the exact probabilities.

More precisely, we will count nonzero degree d forms over $\mathbb{F}_p$ in two ways: up to scaling by $\mathbb{F}_p^\times$, and monic forms.

Definition 4.5.4 (monic)**.** A degree d binary form $f(x,z)$ is **monic** if $f(1,0)=1$.

It is straightforward to see that there are p^d distinct monic degree d forms $f(x,z)$ over $\mathbb{F}_p$, by writing

$$f(x,z)=\sum_{i=0}^{d} c_i x^i z^{d-i},$$

taking $c_d=1$ and choosing c_i freely for $0\le i<d$. We can then use this to determine that there are $p^d+p^{d-1}+\cdots+p+1$ distinct degree d forms up to scaling by a nonzero constant: if $c_d\neq 0$, then scaling f by $\frac{1}{c_d}$ yields a monic form. More generally, there is a unique way — up to scaling by a nonzero constant — to write

$$f(x,z)=z^k f_0(x,z),$$

where f_0 is a monic degree $d-k$ form for some $0\le k\le d$. Counting the number of such forms gives the desired total.

Since $\mathbb{F}_p[x,z]$ is a unique factorization domain, there is a unique way to factor a degree d form $f(x,z)$, considered up to scaling, into its factors, also considered up to scaling. Similarly, if $f(x,z)$ is monic, it can be factored uniquely into monic factors.

Definition 4.5.5 (factorization type)**.** Let $f(x,z)$ be a degree d considered up to scaling

(resp. monic) binary form with unique factorization

$$f(x,z) = \prod_{i=1}^{r} f_i(x,z)^{a_i},$$

where the irreducible factors $f_i(x,z)$ are also considered up to scaling (resp. monic). The **factorization type** of $f(x,z)$ is the data of the degrees $d_i = \deg f_i$ and multiplicities a_i of the factors. This can be shortened to $(d_1^{a_1} d_2^{a_2} \cdots d_r^{a_r})$.

For convenience (and uniqueness of the type) we adopt a lexicographic ordering, that $d_i \leq d_{i+1}$ for all i and $a_i \leq a_{i+1}$ if $d_i = d_{i+1}$. When $a_i = 1$, it is omitted. If $f(x,z)$ has a linear factor of multiplicity one, its factorization type takes the form $(1 d_2^{a_2} \cdots d_r^{a_r})$. This case will be denoted more compactly as $(1*)$.

The proportion of degree d forms up to scaling (resp. degree d monic forms) possessing certain factorization types, indexed by an integer i, is denoted $\eta_{d,i}$ (resp. $\eta'_{d,i}$ for monic forms). The following lemma is a direct consequence of Lemma 4.7.1, which can be found in §4.7, and will be used repeatedly.

Lemma 4.5.6. *The proportions $\eta_{d,i}$, $\eta'_{d,i}$ are given as follows, for $2 \leq d \leq 6$.*

d	*Fact. type*	$\eta_{d,i}$	$\eta'_{d,i}$
2	*0. No roots*	$\frac{(p-1)p}{2(p^2+p+1)}$	$\frac{p-1}{2p}$
	1. $(1*)$	$\frac{(p+1)p}{2(p^2+p+1)}$	$\frac{p-1}{2p}$
	2. (1^2)	$\frac{p+1}{p^2+p+1}$	$\frac{1}{p}$
3	*0. No roots*	$\frac{(p-1)p}{3(p^2+1)}$	$\frac{(p+1)(p-1)}{3p^2}$
	1. $(1*)$	$\frac{(2p+1)p}{3(p^2+1)}$	$\frac{2(p+1)(p-1)}{3p^2}$
	2. (1^3)	$\frac{1}{p^2+1}$	$\frac{1}{p^2}$

d	*Fact. type*	$\eta_{d,i}$	$\eta'_{d,i}$
4	*0. No roots*	$\frac{(3p^2+p+2)(p-1)p}{8(p^4+p^3+p^2+p+1)}$	$\frac{(3p^2+p+2)(p-1)}{8p^3}$
	1. $(1*)$	$\frac{(5p^2+p+2)(p+1)p}{8(p^4+p^3+p^2+p+1)}$	$\frac{(5p^2+3p+2)(p-1)}{8p^3}$
	2. (1^22)	$\frac{(p+1)(p-1)p}{2(p^4+p^3+p^2+p+1)}$	$\frac{p-1}{2p^2}$
	3. (1^21^2)	$\frac{(p+1)p}{2(p^4+p^3+p^2+p+1)}$	$\frac{p-1}{2p^3}$
	4. (1^4)	$\frac{p+1}{p^4+p^3+p^2+p+1}$	$\frac{1}{p^3}$
5	*0. No roots*	$\frac{(11p^2-5p+6)(p-1)p}{30(p^2+p+1)(p^2-p+1)}$	$\frac{(11p^2-5p+6)(p+1)(p-1)}{30p^4}$
	1. $(1*)$	$\frac{(19p^3+6p^2+4p+1)p}{30(p^2+p+1)(p^2-p+1)}$	$\frac{(19p^3+14p^2+4p-6)(p-1)}{30p^4}$
	2. (1^23)	$\frac{(p+1)(p-1)p}{3(p^2+p+1)(p^2-p+1)}$	$\frac{(p+1)(p-1)}{3p^3}$
	3. (1^32)	$\frac{(p-1)p}{2(p^2+p+1)(p^2-p+1)}$	$\frac{p-1}{2p^3}$
	4. (1^21^3)	$\frac{p}{(p^2+p+1)(p^2-p+1)}$	$\frac{p-1}{p^4}$
	5. (1^5)	$\frac{1}{(p^2+p+1)(p^2-p+1)}$	$\frac{1}{p^4}$
6	*0. No roots*	$\frac{(53p^4+26p^3+19p^2-2p+24)(p-1)p}{144(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{(53p^4+26p^3+19p^2-2p+24)(p-1)}{144p^5}$
	1. $(1*)$	$\frac{(91p^4+26p^3+23p^2+16p-12)(p+1)p}{144(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{(91p^3-27p^2+50p-48)(p+1)(p-1)}{144p^5}$
	2. $(1^24), (1^222)$	$\frac{(3p^2+p+2)(p+1)(p-1)p}{8(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{(3p^2+p+2)(p-1)}{8p^4}$
	3. (1^21^22)	$\frac{(p+1)(p-1)p^2}{4(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{(p-1)^2}{4p^4}$
	4. $(1^21^21^2)$	$\frac{(p+1)(p-1)p}{6(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{(p-1)(p-2)}{6p^5}$
	5. (1^33)	$\frac{(p+1)^2(p-1)p}{3(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{(p+1)(p-1)}{3p^4}$
	6. (1^31^3)	$\frac{(p+1)p}{2(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{p-1}{2p^5}$
	7. (1^42)	$\frac{(p+1)(p-1)p}{2(p^6+p^5+p^4+p^3+p^2+p+1)}$	$\frac{p-1}{2p^4}$
	8. (1^21^4)	$\frac{(p+1)p}{p^6+p^5+p^4+p^3+p^2+p+1}$	$\frac{p-1}{p^5}$
	9. (1^6)	$\frac{p+1}{p^6+p^5+p^4+p^3+p^2+p+1}$	$\frac{1}{p^5}$

4.5.2 Geometric arguments: computing σ_1, σ_2, and σ_3

When $\overline{F}$ is absolutely irreducible, we can leverage the proof of Proposition 4.3.2 to see that $\sigma_1 = 1$ when p is sufficiently large.

Proposition 4.5.7. *Suppose C_f is given by (4.5.1) with $\overline{F}$ absolutely irreducible over $\mathbb{F}_p$. Then the reduction $\overline{C_f}$ has a smooth $\mathbb{F}_p$-point whenever*

(i) $p \equiv 1 \pmod 3$ *and* $p > 43$, *or*

(ii) $p \equiv 2 \pmod 3$ *and* $p > 2$.

In particular, whenever (i) or (ii) above is satisfied we have $\sigma_1 = \sigma_1^* = 1$.

Proof. The curve $\overline{C_f}$ is cut out by $\overline{F}$. Note that the reduction of $f(x, z)$ is not a cube if $\overline{F}$ is absolutely irreducible. Taking $m = 3$ in the proof of Proposition 4.3.2, we have that since $\overline{f}$ is not a cube, the reduction $\overline{C_f}$ is guaranteed to have a smooth $\mathbb{F}_p$-point when $p > (m-1)^2(d-2)^2 - 1 = 63$. Furthermore, the improved Hasse–Weil bound (4.3.3) shows that $\overline{C_f}$ is guaranteed to have a smooth point when $p = 61$. Hence in case (i) we have $\sigma_1 = 1$ and $\sigma_1^* = 1$ as well, since this argument is independent of the $(*)$ condition.

When $p \equiv 2 \pmod 3$, taking $d = 6$ in the proof of Proposition 4.3.4 shows that for $p > 2$ such that $3 \nmid p$, there always exists an $\mathbb{F}_p$ solution of $\overline{F} = 0$ which is liftable by Hensel's lemma. Hence in case (ii) we have $\sigma_1 = 1$ as well. □

When $\overline{F}$ has factorization types 2 or 3, which occur when $\overline{F}$ has at least one factor of the form $y - g(x, z)$ where g is a (nonzero) binary quadratic form, we study the $\mathbb{F}_p$-points on the irreducible components of $\overline{C_f}$. See [BCF21, Proposition 2.6] for the analogous case for genus one curves.

Proposition 4.5.8. *Suppose C_f is given by (4.5.1) and $\overline{F}$ has factorization type 2 modulo p. Then C_f has a $\mathbb{Q}_p$ point, or equivalently, $\sigma_2 = 1$.*

Proof. For $p = 3$ and $p \equiv 2 \pmod 3$ the result is vacuously true, since factorization type 2 does not occur. Thus we may assume $p \equiv 1 \pmod 3$, and in particular $p > 3$.

We have $\overline{F} = \prod_{i=1}^{3}(y - h_i(x, z))$ for distinct binary quadratics h_i, so $\overline{C_f}$ is the union of $\overline{C_i}$: $y = h_i(x, z)$. Each $\overline{C_i}$ has $p + 1$ points in $\mathbb{F}_p$, and each distinct (i, j) pair has at most two intersection points. To see this, suppose (α, β, γ) is on C_1 and C_2, i.e.

$$h_1(\alpha, \gamma) = \beta = h_2(\alpha, \gamma).$$

Thus $(\gamma x - \alpha z)$ is a linear factor of the binary quadratic $h_1 - h_2$, and there are at most two such factors.

With this in hand, we have a maximum of 6 total intersection points. This gives at least $3(p+1) - 2 \cdot 6 = 3(p-3)$ smooth points, so whenever $p > 3$ we can lift one of these $\mathbb{F}_p$ points to a $\mathbb{Q}_p$ point on C, giving $\sigma_2 = 1$. □

Proposition 4.5.9. *Suppose C_f is given by (4.5.1) and $\overline{F}$ has factorization type 3 modulo p. Then C_f has a $\mathbb{Q}_p$ point, or equivalently, $\sigma_3 = 1$.*

Proof. As in the proof of Proposition 4.5.8, the statement is vacuously true for $p = 3$ and all primes $p \equiv 1 \pmod 3$, so we assume $p \equiv 2 \pmod 3$.

Recall that by the proof of Lemma 4.5.2 we have

$$\overline{F} = (y - h(x,z))(y^2 + h(x,z)y + h(x,z)^2),$$

where $h(x,z)$ is a (nonzero) binary quadratic form over $\mathbb{F}_p$. Let

$$\overline{C_1}\colon y = h(x,z), \qquad\qquad \overline{C_2}\colon y^2 + h(x,z)y + h(x,z)^2 = 0.$$

In fact, $\overline{C_2}$ is geometrically reducible, factoring over $\mathbb{F}_{p^2}$, where the third root of unity is defined. This means that after a finite extension, we are in the same situation as in the proof of Proposition 4.5.8, and each of the components has at most two intersection points.

In particular $\overline{C_1}$ has $p+1$ $\mathbb{F}_p$-points and at most 4 $\mathbb{F}_{p^2}$-points of intersection with $\overline{C_2}$, forming (at most) two conjugate pairs. Thus at most two $\mathbb{F}_p$-points of $\overline{C_1}$ intersect with $\overline{C_2}$, so $p - 1 > 0$ of the points on C_1 are smooth solutions to $\overline{F} = 0$, which we can lift to a $\mathbb{Q}_p$-solution. □

Remark 4.5.10. These arguments can be generalized to larger m, if one is willing to exclude small primes p. Suppose m is prime and $d = km$ for $k \geq 1$. Consider a superelliptic curve of the form $C_f\colon y^m = f(x,z)$, where the reduction of f modulo p is nonzero. We have already seen, through the proofs of Propositions 4.3.2 and 4.3.4, that when $\overline{f}$ is not a perfect m-th power, there exists a $\mathbb{Q}_p$ point on C_f for sufficiently large primes p.

If $\overline{f}$ is a perfect m-th power, then over $\overline{\mathbb{F}_p}$, the reduction $\overline{C_f}$ breaks up into m components

$$C_i \colon y = h_i(x, z),$$

where h_i is a (nonzero) binary form of degree $k = \frac{d}{m}$. The argument in the proof of Proposition 4.5.8 shows that each C_i intersects with another C_j in at most k points.

Suppose at least one of the components, say C_1, is defined over $\mathbb{F}_p$, thus excluding factorization type 4 when $(m, d) = (3, 6)$, which will require more care. Since C_1 has $p+1$ $\mathbb{F}_p$-points, we have that $p+1-k(m-1)$ of these points lift by Hensel's lemma. Thus when $p > km - (k+1)$, the curve C_f is guaranteed a $\mathbb{Q}_p$-point.

The caveat is that relatively few superelliptic curves have these factorization types. Only $p^{k+1} - 1$ out of the p^d choices for $\overline{f}(x, z)$ modulo p have that $\overline{f}$ is a nonzero m-th power. If $p \equiv 1 \pmod{m}$, then further $\frac{p-1}{mp}$ of those will have a factor defined over $\mathbb{F}_p$. As $d \to \infty$ for fixed m, these fail to make up a positive proportion.

Considering only factorization types 1 — 3, we are essentially no better off than in §4.3, where using $m = 3$ and $d = 6$ we obtain lower bounds

$$\rho_{3,6}(p) \geq \begin{cases} 1 - \frac{1}{p^4} & p \equiv 1 \pmod 3,\ p > 43 \\ 1 - \frac{1}{p^7} & p \equiv 2 \pmod 3,\ p > 2, \end{cases}$$

via Propositions 4.3.2 and 4.3.4. Thus even just to obtain the improved asymptotics of Theorem 4.1.5, it is necessary to consider factorization types 4 and 5.

4.5.3 Intermediate results

The following intermediate results will be used repeatedly, as will the strategies of their proofs. Throughout, $f(x, z)$ denotes a binary sextic form with coefficients $c_i \in \mathbb{Z}_p$ and C_f the equation cut out by $y^3 - f(x, z)$.

Lemma 4.5.11. *Let $p \equiv 1 \pmod 3$. Suppose $c_4, c_5, c_6 \in p\mathbb{Z}_p$ and $c_3 \in \mathbb{Z}_p$ are fixed, such that the reduction $\overline{c_3}$ is neither a cubic residue nor zero, i.e. $\overline{c_3} \notin \mathbb{F}_p^3$. Let β be the probability that C_f has a $\mathbb{Q}_p$-point of the form $[x : y : 1]$, as c_0, c_1, c_2 range over $\mathbb{Z}_p$. Let α denote the*

same probability, but with $c_0, c_1, c_2 \in p\mathbb{Z}_p$. *We have*

$$\alpha = \frac{(p^3+p+1)}{p^4+p^3+p^2+p+1},$$
$$\beta = \frac{p(p^3+p^2+1)}{p^4+p^3+p^2+p+1}.$$

Proof. The reduction $\overline{C_f}$ is isomorphic to the curve cut out by

$$y^3 \equiv \overline{f}(x,z) \equiv c_3x^3 + c_2x^2z + c_1xz^2 + c_0z^3 \pmod{p}. \tag{4.5.5}$$

We look for a smooth solution $[x : y : 1]$ to (4.5.5), which lifts to a $\mathbb{Q}_p$-point on C_f by Hensel's lemma. Note that there are no solutions of the form $[x : y : 0]$ because $\overline{c_3} \notin \mathbb{F}_p^3$.

The normalization of $\overline{C_f}$ has geometric genus at most 1. Applying the Hasse–Weil bound method to (4.5.5) as in the proof of Proposition 4.3.2, we see that whenever $f(x,z)$ doesn't have a triple root (equivalently $\overline{f} \neq \overline{c_3}(x-\alpha z)^3$ for some $\alpha \in \mathbb{F}_p$), we have

$$\#\overline{C_f}^{\mathrm{sm}}(\mathbb{F}_p) \geq p+1-2\sqrt{p} > 0.$$

The rightmost inequality follows from the fact that $p \geq 7$ since $p \equiv 1 \pmod 3$. Thus we have found our desired $\mathbb{Q}_p$-point whenever $\overline{f} \neq \overline{c_3}(x-\alpha z)^3$.

The proportion of cubics over $\mathbb{F}_p$ with fixed leading coefficient c_3 having a triple root is equal to $\eta'_{3,2} = \frac{1}{p^2}$ (see Lemma 4.5.6). In this case, after a change of variables, we may assume (4.5.5) is of the form $y \equiv c_3x^3 \pmod p$, i.e. $c_0, c_1, c_2 \in p\mathbb{Z}_p$. The probability of C_f having a $\mathbb{Q}_p$-point in this case is precisely α. Thus we have

$$\beta = 1 - \frac{1}{p^2} + \frac{\alpha}{p^2}. \tag{4.5.6}$$

We now assume $c_0, c_1, c_2 \in p\mathbb{Z}_p$, and we are looking to lift solutions of $y^3 \equiv c_3x^3 \pmod p$, whose only $\mathbb{F}_p$-solution is the (singular) point $(0,0)$ by our assumption on c_3. Thus $p \mid x, y$ is necessary, so looking modulo p^2, we see that $p^2 \mid c_0$ is also a necessary condition, which occurs with probability $\frac{1}{p}$ as c_0 runs through $p\mathbb{Z}_p$.

Assuming $p^2 \mid c_0$, we perform a change of variables by replacing x and y by px and py.

Dividing by p^2, the equation for $\overline{C_f}$ is now

$$0 \equiv \frac{c_1}{p}x + \frac{c_0}{p^2} \pmod{p}.$$

If $v_p(c_1) = 1$, then this is merely a linear equation, so for any choice of $y \in \mathbb{Z}_p$, we can find an $\mathbb{F}_p$ solution that lifts to a $\mathbb{Q}_p$-one. This occurs with probability $1 - \frac{1}{p}$, so with probability $\frac{1}{p}$ we have $p^2 \mid c_1$.

Assuming $p^2 \mid c_1$, we again find it is necessary for $p^3 \mid c_0$. Dividing the equation for $\overline{C_f}$ by p^3 instead of p^2 as above, we obtain

$$y^3 \equiv c_3x^3 + \frac{c_2}{p}x^2 + \frac{c_1}{p^2}x + \frac{c_0}{p^3} \pmod{p},$$

which puts us back in the case of β, where $c_0, c_1, c_2 \in \mathbb{Z}_p$. That is, we have shown

$$\begin{aligned} \alpha &= \frac{1}{p}\left(1 - \frac{1}{p} + \frac{\beta}{p^2}\right) \\ &= \frac{1}{p} + \frac{1}{p^2} + \frac{\beta}{p^3}. \end{aligned} \tag{4.5.7}$$

Combining (4.5.6) and (4.5.7) and solving simultaneously, we obtain the claimed values. □

The strategy employed in the proof of Lemma 4.5.11 — making successive reductions until we reach a case we know and solving a system of equations to determine desired probabilities — will be used repeatedly. For results with longer proofs, it is convenient to organize the argument with a table. We illustrate this below with the computation for α.

			$v(c_6)$	$v(c_5)$	$v(c_4)$	$v(c_3)$	$v(c_2)$	$v(c_1)$	$v(c_0)$
$\alpha =$	$\alpha_a =$	$\frac{1}{p}\alpha_b$	≥ 1	≥ 1	≥ 1	$= 0$	≥ 1	≥ 1	≥ 1
	$\alpha_b =$	$1 - \frac{1}{p} + \frac{1}{p}\alpha_c$	≥ 1	≥ 1	≥ 1	$= 0$	≥ 1	≥ 1	≥ 2
	$\alpha_c =$	$\frac{1}{p}\alpha_d$	≥ 1	≥ 1	≥ 1	$= 0$	≥ 1	≥ 2	≥ 2
	$\alpha_d =$	α_e	≥ 1	≥ 1	≥ 1	$= 0$	≥ 1	≥ 2	≥ 3
	$\alpha_e =$	β	≥ 4	≥ 3	≥ 2	$= 0$	≥ 0	≥ 0	≥ 0

The first step in the table above was recognizing that $p^2 \mid c_0$ is necessary for a solution to lift. In the second step, we assume $v(c_0) \geq 2$ and compute the probability of a liftable

solution when $v(c_1) = 1$, moving to the next line if $p^2 \mid c_1$, and so on. One sees that combining the steps in the table, we achieve the same formula for α in terms of β as (4.5.7).

Repeating the argument of the proof of Lemma 4.5.11, we obtain similar results when c_3 is fixed of valuation 1 or 2. We will use all of these later as well. Note that the probabilities depend on the conjugacy class of p modulo 3, owing to the fact that the probability of a nonzero element of $\mathbb{F}_p$ being a cubic residue differs in each case.

Lemma 4.5.12. *Suppose $c_3, c_4, c_5, c_6 \in \mathbb{Z}_p$ are fixed with p-adic valuation given below. Let $\alpha', \beta', \alpha'', \beta''$ denote the probabilities that C_f has a $\mathbb{Q}_p$-point of the form $[x : y : 1]$ as c_0, c_1, c_2 vary over $\mathbb{Z}_p$ with the specified valuation(s).*

$v(c_6)$	$v(c_5)$	$v(c_4)$	$v(c_3)$	$v(c_2)$	$v(c_1)$	$v(c_0)$		
≥ 2	≥ 2	≥ 2	$= 1$	≥ 1	≥ 1	≥ 1	$\alpha' =$	$\begin{cases} \frac{2p^3+2p^2+3}{3(p^3+p^2+p+1)} = \frac{5}{8}, & p = 3 \\ \frac{2p^4+2p^3+3p+1}{3(p^4+p^3+p^2+p+1)}, & p \equiv 1 \pmod 3 \\ \frac{2p^4+2p^3+3p+3}{3(p^4+p^3+p^2+p+1)}, & p \equiv 2 \pmod 3 \end{cases}$
≥ 2	≥ 2	≥ 2	$= 1$	≥ 1	≥ 0	≥ 0	$\beta' =$	$\begin{cases} \frac{3p^3+2p^2+2p}{3(p^3+p^2+p+1)} = \frac{7}{8}, & p = 3 \\ \frac{3p^4+p^3+2p^2+2p}{3(p^4+p^3+p^2+p+1)}, & p \equiv 1 \pmod 3 \\ \frac{3p^4+3p^3+2p^2+2p}{3(p^4+p^3+p^2+p+1)}, & p \equiv 2 \pmod 3 \end{cases}$
≥ 3	≥ 3	≥ 3	$= 2$	≥ 2	≥ 2	≥ 2	$\alpha'' =$	$\begin{cases} \frac{2p^3+2p^2+3p}{3(p^3+p^2+p+1)} = \frac{27}{40}, & p = 3 \\ \frac{2p^4+2p^3+p^2+3p}{3(p^4+p^3+p^2+p+1)}, & p \equiv 1 \pmod 3 \\ \frac{2p^4+2p^3+3p^2+3p}{3(p^4+p^3+p^2+p+1)}, & p \equiv 2 \pmod 3 \end{cases}$
≥ 3	≥ 3	≥ 3	$= 2$	≥ 3	≥ 3	≥ 3	$\beta'' =$	$\begin{cases} \frac{3p^3+2p+2}{3(p^3+p^2+p+1)} = \frac{89}{120}, & p = 3 \\ \frac{p^4+3p^3+2p+2}{3(p^4+p^3+p^2+p+1)}, & p \equiv 1 \pmod 3 \\ \frac{3p^4+3p^3+2p+2}{3(p^4+p^3+p^2+p+1)}, & p \equiv 2 \pmod 3 \end{cases}$

(4.5.8)

(4.5.9)

(4.5.10)

(4.5.11)

Proof. Starting with α', in order for there to be a liftable $\mathbb{F}_p$-point of the form $[x : y : 1]$, we need $y \equiv 0 \pmod{p}$, and a root of the polynomial $\frac{1}{p}(c_3x^3 + c_2x^2 + c_1x + c_0) \pmod{p}$. There is an $\eta'_{3,1} = \frac{2}{3}(1 - \frac{1}{p^2})$ chance of the existence of a simple root, an $\eta'_{3,0} = \frac{1}{3}(1 - \frac{1}{p^2})$ chance of no roots, and an $\eta'_{3,2} = \frac{1}{p^2}$ chance of a triple root (see Lemma 4.5.6). If we have a triple root, we may assume it is at $x \equiv 0 \pmod{p}$ after a change of variables, allowing us to assume $v(c_2), v(c_1), v(c_0) \geq 2$.

Considering the resulting polynomial mod p^3, we have that x is a root if and only if $p^3 \mid c_0$, which occurs with probability $\frac{1}{p}$. Changing variables by replacing x, y by px, py and dividing by p^3 gives us that $c_6, c_5, c_4 \in p^2\mathbb{Z}_p$ (though their valuations may increase), and $v(c_0), v(c_1) \geq 0$, while $v(c_2) \geq 1$ and c_3 remains unchanged. This is precisely the case of β', giving us

$$\alpha' = \eta'_{3,1} + \frac{\beta'}{p^3} = \frac{2}{3}\left(1 - \frac{1}{p^2}\right) + \frac{\beta'}{p^3},$$

regardless of the choice of prime p.

Now we compute β'. If $v(c_1) = 0$ then we can always find a smooth solution to $c_1x + c_0 \equiv 0 \pmod{p}$, as a linear polynomial always has a simple root. If $v(c_1) \geq 1$ then mod p we have $F(x, y, 1) \equiv y^3 - c_0$. Suppose $v(c_0) = 0$, for if not we are in the case of α'. If $p \equiv 1 \pmod{3}$ this has a liftable solution with probability $1/3$, as $1/3$ of the residue classes in $\mathbb{F}_p^\times$ are cubic residues. If $p \equiv 2 \pmod{3}$, this probability is 1, since every nonzero residue is a cube. If $p = 3$, then the change of variables $y \mapsto y + a$, where $a \equiv c_0 \pmod{p}$ gives the new equation

$$F(x, y, 1) = y^3 - c_3x^3 - c_2x^2 - c_1x - c_0 + a^3,$$

and since $c_0 \equiv a^3 \pmod{p}$ we have that $p \mid c_0$ after a change of variables. Hence, we have

$$\beta' = \begin{cases} (1 - \frac{1}{p}) + \frac{1}{p}(\frac{1}{3}(1 - \frac{1}{p}) + \frac{1}{p}\alpha'), & p \equiv 1 \pmod{3} \\ (1 - \frac{1}{p}) + \frac{1}{p}((1 - \frac{1}{p}) + \frac{1}{p}\alpha'), & p \equiv 2 \pmod{3} \\ (1 - \frac{1}{p}) + \frac{1}{p}\alpha', & p = 3. \end{cases}$$

Solving these equations for α' and β' gives the values in the tables.

To compute α'', we proceed as in the calculation for α'. We can compute the probability

that $\frac{1}{p^2}(c_3x^3 + c_2x^2 + c_1x + c_0)$ has a simple root or triple root, and notice that if there is a triple root, it can be moved to $x \equiv 0 \pmod{p}$, putting us in the case of β''. Thus

$$\alpha'' = \eta'_{3,1} + \frac{\beta''}{p^2} = \frac{2}{3}\left(1 - \frac{1}{p^2}\right) + \frac{\beta''}{p^2}.$$

For β'', we immediately make the change of variables $x \mapsto px, y \mapsto py$ and divide by p^3. This doesn't change c_3, but puts the valuations of c_2, c_1, c_2 at *at least* 2, 1, and 0 respectively. If $p \neq 3$ and $v(c_0) = 0$, then we can compute the probability that $y^3 = c_0$ has a solution depending on the residue class of p. If $p \mid c_0$ then we look mod p^2, where our polynomial becomes linear. If $v(c_1) \geq 2$ then we must have $p^2 \mid c_0$ in order to have a solution, putting us back in the case of α''.

If $p = 3$ then we can take the same approach as for β'. After changing variables in y, we may assume that $p \mid c_0$, and then follow the same argument as $p \neq 3$. Thus the values of β'' in terms of α'' become

$$\beta'' = \begin{cases} \frac{1}{3}(1 - \frac{1}{p}) + \frac{1}{p}((1 - \frac{1}{p}) + \frac{1}{p^2}\alpha''), & p \equiv 1 \pmod 3 \\ 1 - \frac{1}{p} + \frac{1}{p}((1 - \frac{1}{p}) + \frac{1}{p^2}\alpha''), & p \equiv 2 \pmod 3 \\ 1 - \frac{1}{p} + \frac{1}{p^2}\alpha'', & p = 3. \end{cases}$$

Solving the equations for α'' and β'' gives the values stated in the table. □

Remark 4.5.13. The probabilities in Lemmas 4.5.11 and 4.5.12 are independent of c_4, c_5, and c_6, even though they may be changed in the second parts of the proofs. This is key, and also noted in the proof of [BCF21, Lemma 2.8].

We conclude this subsection with another result which will be used repeatedly in what follows. While it is independent from the later results, we will make reference in the proof to quantities which will be defined and determined in §4.5.5, in an effort to keep the paper compact.

Lemma 4.5.14. *Fix a prime $p > 31$, or $p > 2$ satisfying $p \equiv 2 \pmod 3$. Suppose c_4, c_5, c_6 are fixed with $c_5, c_6 \in p^3\mathbb{Z}_p$ (resp. $p^2\mathbb{Z}_p$) and $v_p(c_4) = 2$ (resp. $v_p(c_4) = 1$). Let μ (resp. μ')*

denote the proportion of f for which C_f has a $\mathbb{Q}_p$-point of the form $[x : y : 1]$ as c_0, c_1, c_2, c_3 vary over $p^2\mathbb{Z}_p$ (resp. $p\mathbb{Z}_p$). Then

$$\mu = \begin{cases} \frac{45p^{11}-6p^{10}+5p^9-30p^8+69p^7-29p^6-39p^5+81p^4-120p^3+60p^2+108p-72}{72p^{11}}, & p \equiv 1 \pmod 3 \\ \frac{\left(5p^{10}-3p^9+2p^7+3p^6-16p^5+25p^4-16p^3-8p^2+20p-8\right)(p+1)}{8p^{11}}, & p \equiv 2 \pmod 3 \end{cases} \tag{4.5.12}$$

$\mu' = (4.8.6)$.

Proof. Consider first μ, so let $v(c_4) = 2$, $c_5, c_6 \in p^3\mathbb{Z}_p$, and c_0, c_1, c_2, c_3 vary in $p^2\mathbb{Z}_p$. A necessary condition for $[x : y : 1]$ to satisfy $F = 0$ is $p \mid y$, hence $\frac{1}{p^2}\left(c_3x^3 + c_2x^2 + c_1x + c_0\right) \equiv 0 \pmod p$. Thus the probability depends on how this quartic factors modulo p, the proportions of which are given by $\eta'_{4,i}$ from Lemma 4.5.6.

If $\frac{1}{p^2}\left(c_3x^3 + c_2x^2 + c_1x + c_0\right)$ has no roots modulo p, then there can necessarily be no liftable solution. If it has a root of multiplicity 1, then we can lift it to a $\mathbb{Q}_p$-solution. If it has a double root, then after composing with an automorphism of $\mathbb{P}^1$, we may assume the root occurs at $[x : z] = [0 : 1]$, i.e. we have $v(c_0), v(c_1) \geq 3$ while $v(c_2) = 2$. Thus we are precisely in the case of θ_2, to be defined in §4.5.5 and computed in Lemma 4.5.21. Similarly, if the quartic has two double roots, the probability of at least one lifting is given by θ_3. If it has a quadruple root, the probability of it lifting is given by θ_7, which is valid for all primes $p > 31$ or $p > 2$ if $p \equiv 2 \pmod 3$. Thus we have

$$\mu = \eta'_{4,1} + \eta'_{4,2}\theta_2 + \eta'_{4,3}\theta_3 + \eta'_{4,4}\theta_7 \tag{4.5.13}$$

which gives the value stated in (4.5.12).

For μ', a similar analysis shows that

$$\mu' = \eta'_{4,1} + \eta'_{4,2}\tau_2 + \eta'_{4,3}\tau_3 + \eta'_{4,4}\tau_7 \tag{4.5.14}$$

where again the τ_i are to be defined in §4.5.5 and computed in Lemma 4.5.19. This gives the value of μ' which given in (4.8.6). We comment that while none of the τ_i use μ' as

defined here, the value of μ is used in the computation of τ_7, so this rational function for μ' is valid for all primes $p > 31$ or $p > 2$ if $p \equiv 2 \pmod 3$. □

4.5.4 Three conjugate factors: computing σ_4

By Lemma 4.5.2 and Corollary 4.5.3, this type only occurs when $p \equiv 1 \pmod 3$, so we assume this for the remainder of §4.5.4. If $\overline{F}$ has three distinct conjugate factors, none of which are defined over $\mathbb{F}_p$, then the proof of Lemma 4.5.2 shows that

$$\overline{F}(x, y, z) = y^3 - ah_0(x, z)^3,$$

where $a \notin (\mathbb{F}_p^\times)^3$ is nonzero and $h_0(x, z)$ is a binary quadratic form defined over $\mathbb{F}_p$ up to scaling. Note also that $(*)$ is satisfied whenever h above is monic.

It is thus clear that $\overline{F}$ has no $\mathbb{F}_p$-solutions for which $h_0(x, z) \neq 0$. However, if $h_0(x_0, z_0) = 0$, the point $(x_0, 0, z_0)$ is not a smooth point of $\overline{F}$. After considering the possible factorization types of $h_0(x, z)$ we obtain the following value for σ_4 when p is sufficiently large.

Proposition 4.5.15. *Suppose C_f is given by (4.5.1) and $\overline{F}$ has factorization type 4 modulo p for a prime $p > 43$. Then the proportions of f and f satisfying $(*)$ for which $C_f(\mathbb{Q}_p) \neq \emptyset$ are*

$$\sigma_4 = (4.8.3)$$
$$\sigma_4^* = (4.8.4).$$

The proof is given in §4.5.4, after studying the factorization types of the binary quadratic form $h_0(x, z)$ individually.

$h_0(x, z)$ has no roots in $\mathbb{F}_p$.

If this is the case, then there are no $\mathbb{Q}_p$-points, because there are no $\mathbb{F}_p$ solutions to $h_0(x, z) = 0$, which is necessary by the above argument.

The probability of $h_0(x, z)$ having no roots is $\eta_{2,0} = \frac{p(p-1)^2}{2(p^3-1)}$. If F satisfies $(*)$, then we may as well assume $h_0(x, z)$ is monic, and the probability of it having no roots is $\eta'_{2,0} = \frac{p-1}{2p}$.

$h_0(x,z)$ has distinct roots in $\mathbb{F}_p$.

The probability of this occurring is $\eta_{2,1} = \frac{p(p^2-1)}{2(p^3-1)}$, and $\eta'_{2,1} = \frac{p-1}{2p}$ in the case of condition $(*)$. After composing with an automorphism of $\mathbb{P}^1$, we may assume the roots of h_0 are located at $[x:z] = [1:0]$ and $[0:1]$, so we have $h_0(x,z) = xz$. Thus we have $\overline{F}(x,y,z) = y^3 - ax^3z^3$, where $a \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^3$. We now need to compute the probabilities that $[0:0:1]$ and $[1:0:0]$ lift to $\mathbb{Q}_p$-points. This is analogous to [BCF21, §2.3.2], and follows from Lemma 4.5.11 applied to each root.

Corollary 4.5.16. *Suppose $\overline{F}$ has factorization type 4, with $h_0(x,z)$ having distinct linear factors mod p. Then the probability that F has a $\mathbb{Q}_p$-solution is given by*

$$1 - (1-\alpha)^2 = \frac{(p^3+p+1)(2p^4+p^3+2p^2+p+1)}{(p^4+p^3+p^2+p+1)^2}$$

where α is as defined in Lemma 4.5.11.

Proof. Suppose $F(x,y,z) \equiv y^3 - ah_0(x,z)^3 \pmod{p}$, where $a \notin \mathbb{F}_p^3$, such that $h_0(x,z)$ has distinct linear factors mod p. After a change of coordinates, we may assume that $h_0(x,z) = xz$, giving us

$$\overline{F}(x,y,z) = y^3 - ax^3z^3.$$

The only $\mathbb{F}_p$-points of $\overline{F} \equiv 0$ are at $[1:0:0]$ and $[0:0:1]$, both of which are singular.

Since $c_0, c_1, c_2, c_4, c_5, c_6 \in p\mathbb{Z}_p$ and $c_3 \equiv a \notin \mathbb{F}_p^3$, for the point $[0:0:1]$ we are in the case of Lemma 4.5.11. The probability that $[0:0:1]$ lifts to a $\mathbb{Q}_p$-point is thus α. Note that by Remark 4.5.13, this only depends on the choices of c_0, c_1, c_2. Similarly, but with the roles of x and z reversed, the probability that $[1:0:0]$ lifts is also α, and only depends on c_4, c_5, c_6. Thus the two probabilities are independent, allowing us to compute the probability that at least one of the points lifts by $1-(1-\alpha)^2$. □

$h_0(x,z)$ has a double root

We now need to carry out the analysis for when $h_0(x,z)$ has a double root. This occurs with probability $\eta_{2,2} = \frac{p^2-1}{p^3-1}$ and in the case of $(*)$, $\eta'_{2,2} = \frac{1}{p}$. This case requires more work, which we organize into the following lemma.

Lemma 4.5.17. *Assume $p > 3$ and suppose $\overline{F}$ has factorization type 4, with $h_0(x, z)$ having a double root modulo p. Then the probability that F has a $\mathbb{Q}_p$-solution is given by λ, where*

$$\lambda = \frac{1}{p^{15}}\rho^*(p) + (p-1)\Big(72p^{25} + 72p^{23} + 72p^{22} + 24p^{21} - 24p^{20} + 36p^{19} - 84p^{18} + 72p^{17} - 27p^{16} + 18p^{15} - 13p^{14} - 12p^{13} - 36p^{12} + 25p^{11} - 55p^{10} + 12p^9 - 115p^8 + 105p^7 - 178p^6 + 73p^5 - 35p^4 + 67p^3 - 93p^2 + 36p - 12\Big)\Big/\Big(72p^{22}(p^5 - 1)\Big). \tag{4.5.15}$$

Proof. After a change of variables, we may assume $h_0(x, z) = x^2$, so we have $\overline{F}(x, y, z) = y^3 - ax^6$, where $a \notin \mathbb{F}_p^3$. That is, we have $c_6 \in \mathbb{Z}_p$ such that $c_6 \equiv a \pmod{p}$ and $c_0, ..., c_5 \in p\mathbb{Z}_p$. The only $\mathbb{F}_p$-point of $\overline{F}$ is the singular point at $[0 : 0 : 1]$ since $a \notin \mathbb{F}_p^3$. Thus λ is the probability that this point lifts.

The table below lists the valuations of the coefficients of f. For each line, we compute the probability that the singular point lifts or not, and then move on to the next line. The probability for moving to the next line will always be $\frac{1}{p}$. This will give rise to a linear relation between λ and ρ^*, the probability that F has a $\mathbb{Q}_p$-point when its leading coefficient is not a cube mod p.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\lambda =$	$\lambda_a =$	$\frac{1}{p}\lambda_b$	$=0$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1
	$\lambda_b =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\lambda_c$	$=0$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 2
	$\lambda_c =$	$\frac{1}{p}\lambda_d$	$=0$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 2	≥ 2
	$\lambda_d =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\lambda_e$	$=3$	≥ 3	≥ 2	≥ 1	≥ 0	≥ 0	≥ 0
	$\lambda_e =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\lambda_f$	$=3$	≥ 3	≥ 2	≥ 1	≥ 1	≥ 0	≥ 0
	$\lambda_f =$	$\Phi(p)+\frac{1}{p}\lambda_g$	$=3$	≥ 3	≥ 2	≥ 1	≥ 1	≥ 1	≥ 0
	$\lambda_g =$	$\left(1-\frac{1}{p}\right)\alpha'+\frac{1}{p}\lambda_h$	$=3$	≥ 3	≥ 2	≥ 1	≥ 1	≥ 1	≥ 1
	$\lambda_h =$	$\left(1-\frac{1}{p}\right)\left(\frac{p-1}{2p}+\frac{1}{p^2}\right)+\frac{1}{p}\lambda_i$	$=3$	≥ 3	≥ 2	≥ 2	≥ 1	≥ 1	≥ 1
	$\lambda_i =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\lambda_j$	$=3$	≥ 3	≥ 2	≥ 2	≥ 2	≥ 1	≥ 1
	$\lambda_j =$	$\frac{1}{p}\lambda_k$	$=3$	≥ 3	≥ 2	≥ 2	≥ 2	≥ 2	≥ 1
	$\lambda_k =$	$\left(1-\frac{1}{p}\right)\mu+\frac{1}{p}\lambda_\ell$	$=3$	≥ 3	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2
	$\lambda_\ell =$	$\left(1-\frac{1}{p}\right)\alpha''+\frac{1}{p}\lambda_m$	$=3$	≥ 3	≥ 3	≥ 2	≥ 2	≥ 2	≥ 2
	$\lambda_m =$	$\left(1-\frac{1}{p}\right)\left(\frac{p-1}{2p}+\frac{(p+2)(2p^2-3p+3)}{6p^3}\right)+\frac{1}{p}\lambda_n$	$=3$	≥ 3	≥ 3	≥ 3	≥ 2	≥ 2	≥ 2
	$\lambda_n =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\lambda_o$	$=3$	≥ 3	≥ 3	≥ 3	≥ 3	≥ 2	≥ 2
	$\lambda_o =$	$\frac{1}{p}\lambda_p$	$=3$	≥ 3	≥ 3	≥ 3	≥ 3	≥ 3	≥ 2
	$\lambda_p =$	ρ^*	$=0$	≥ 0	≥ 0	≥ 0	≥ 0	≥ 0	≥ 0

Putting together the steps above gives (4.5.15). Each step is justified below.

(a) The only possible point reduces to $[0:0:1]$, so $p \mid x, y$. Reducing $F(x, y, z)$ mod p^2 reveals that $v(c_0) \geq 2$ is necessary.

(b) If $v(c_1) = 1$, which occurs with probability $1 - \frac{1}{p}$ then we can fix $y \in p\mathbb{Z}_p$ and look for solutions to $F(x, y, 1)$ as a function of x. While it is clear $p \mid x$ is necessary, we have $v(F'(x, y, 1)) = 1$, so we need to look for solutions mod p^3. Looking modulo p^3, we have the linear equation $c_1x + c_0 \equiv 0 \pmod{p^3}$, which we can solve, finding something that lifts. If $v(c_1) = 2$ then we move to the next line.

(c) Again we have $p \mid x, y$, so we reduce mod p^3 and find that it is necessary to have $p^3 \mid c_0$. This occurs with probability $\frac{1}{p}$. Before moving to the next line we replace both x and y with px and py, then divide by p^3.

(d) With probability $1 - \frac{1}{p}$ we have $v(c_2) = 0$, in which case $\overline{C_f}$ is isomorphic to

$$y^3 \equiv c_2x^2z + c_1xz^2 + c_0z^3 \pmod{p}$$

and its normalization has geometric genus at most 1. Since $\overline{f} \neq ah^3$ for $a \in \mathbb{F}_p$ and $h \in \mathbb{F}_p[x,z]$, we apply the Hasse–Weil bound (see the proof of Proposition 4.3.2) to find

$$\#\overline{C_f}^{\mathrm{sm}}(\mathbb{F}_p) \geq p + 1 - 2\sqrt{p} > 1,$$

where the rightmost inequality holds for all primes $p > 4$. $\overline{C_f}$ has only the point $[1:0:0]$ above infinity, so there must exist some smooth $\mathbb{F}_p$-point $[x:y:1]$ which lifts to a $\mathbb{Q}_p$-point of C_f. If $v(c_2) \geq 1$ we move to the next line.

(e) With probability $1 - \frac{1}{p}$ we have $v(c_1) = 0$ and the reduced equation is $\overline{F}(x,y,1) = y^3 - c_1x - c_0$, which is linear in x and thus has a solution with $y \in p\mathbb{Z}_p$. With probability $\frac{1}{p}$ we have $v(c_1) \geq 1$ and move to the next line.

(f) The reduced equation is now $\overline{F} = y^3 - c_0$. The probability that c_0 is a nonzero cubic residue is $\Phi(p) = \frac{1}{3}\left(1 - \frac{1}{p}\right)$ (see Proposition 4.3.6 for the definition). If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(g) With probability $1 - \frac{1}{p}$ we have $v(c_3) = 1$ and we are in the case of α'. See (4.5.8) from Lemma 4.5.12. With probability $\frac{1}{p}$ we move to the next line.

(h) With probability $1 - \frac{1}{p}$ we have $v(c_2) = 1$. It is clear that for any solution, we must have $p \mid y$ and $\frac{1}{p}(c_2x^2 + c_1x + c_0) \equiv 0 \pmod{p}$. The quadratic $\frac{1}{p}(c_2x^2 + c_1x + c_0)$ has no roots with probability $\eta'_{2,0} = \frac{1}{2}\frac{(p-1)}{p}$ and distinct roots with probability $\eta'_{2,1} = \frac{1}{2}\frac{(p-1)}{p}$. In the case of distinct roots, one can check that either root lifts to the x-coordinate of a $\mathbb{Q}_p$-point with $y \in p\mathbb{Z}_p$. A double root occurs with probability $\eta'_{2,2} = \frac{1}{p}$, and the probability of a solution lifting is equal to τ_2, to be defined later shown to be $\tau_2 = \frac{1}{p}$ in Lemma 4.5.19. Thus we have

$$\lambda_h = \left(1 - \frac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\tau_2\right) + \frac{1}{p}\lambda_i = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{1}{p^2}\right) + \frac{1}{p}\lambda_i.$$

(i) Reducing mod p we see that any solution must have $p \mid y$. If $v(c_1) = 1$ then $\frac{1}{p}(c_1x + c_0)$ is linear in x and has a solution modulo p. A straightforward check shows that an

x-value solving this equation modulo p lifts to a solution of $F(x,y,1) \equiv 0 \pmod{p^3}$ with $p \mid y$, and hence to a $\mathbb{Q}_p$-solution by Hensel's lemma. With probability $\frac{1}{p}$ we move to the next line.

(j) Reducing mod p^2, we have $c_0 \in p^2\mathbb{Z}_p$ is necessary to obtain a $\mathbb{Q}_p$-solution. This occurs with probability $\frac{1}{p}$, and we move to the next line.

(k) With probability $1 - \frac{1}{p}$ we have $v(c_4) = 2$ and we are in the case of μ from Lemma 4.5.14. With probability $\frac{1}{p}$ we move to the next line.

(ℓ) With probability $1 - \frac{1}{p}$ we have $v(c_3) = 2$ and we are in the case of α''. See (4.5.10) from Lemma 4.5.12. With probability $\frac{1}{p}$ we move to the next line.

(m) With probability $1-\frac{1}{p}$ we have $v(c_2) = 2$. It is clear that for any solution, we must have $p \mid y$ and $\frac{1}{p^2}(c_2x^2 + c_1x + c_0) \equiv 0 \pmod{p}$. The quadratic $\frac{1}{p^2}(c_2x^2 + c_1x + c_0)$ has no roots with probability $\eta'_{2,0} = \frac{1}{2}\frac{(p-1)}{p}$ and distinct roots with probability $\eta'_{2,1} = \frac{1}{2}\frac{(p-1)}{p}$. In the case of distinct roots, one can check that either root lifts to the x-coordinate of a $\mathbb{Q}_p$-point with $y \in p\mathbb{Z}_p$. A double root occurs with probability $\eta'_{2,2} = \frac{1}{p}$, and the probability of a solution lifting is equal to θ_2, to be defined later shown to be $\theta_2 = \frac{(p+2)(2p^2-3p+3)}{6p^2}$ in Lemma 4.5.21. Thus we have

$$\lambda_m = \left(1 - \tfrac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\theta_2\right) + \tfrac{1}{p}\lambda_n = \left(1 - \tfrac{1}{p}\right)\left(\tfrac{p-1}{2p} + \tfrac{(p+2)(2p^2-3p+3)}{6p^3}\right) + \tfrac{1}{p}\lambda_n.$$

(n) If $v(c_1) = 2$ then we can lift a root of $\frac{1}{p^2}(c_1x + c_0) \equiv 0 \pmod{p}$ to a solution. If not, we move to the next line.

(o) We have $p \mid y$, so reducing modulo p^3 shows that $c_0 \in p^3\mathbb{Z}_p$ is necessary, which occurs with probability $\frac{1}{p}$. Replacing y by py and dividing by p^3 moves us to the next line.

(p) Recalling that c_6 is not congruent to a cubic residue mod p, we are in the case of ρ^*, because we have assumed no conditions on the coefficients except the $(*)$ condition.

□

Completing the proof of Proposition 4.5.15

Proof of Proposition 4.5.15. Lemma 4.5.17 gives us a linear relation between $\rho^*(p)$ and λ. Here we give another such relation, and solve the system for $\rho^*(p)$ and λ. Recall

$$\rho^*(p) = \xi_1^* + \xi_4^*\sigma_4^*$$

since $\sigma_1^* = 1$ when $p > 43$. We have given the values of ξ_i^* in Corollary 4.5.3. We break σ_4^* down into the cases where $h_0(x, z)$ has no roots, distinct simple roots, or a double root, giving us

$$\begin{aligned}\sigma_4^* &= \eta'_{2,1}(1-(1-\alpha)^2) + \eta'_{2,2}\lambda \\ &= \left(\frac{p-1}{2p}\right)\left(1-(1-\alpha)^2\right) + \frac{1}{p}\lambda\end{aligned}$$

by Corollary 4.5.16. Combining these, we have the relation

$$\rho^*(p) = \xi_1^* + \xi_4^*\left(\left(\frac{p-1}{2p}\right)\left(1-(1-\alpha)^2\right) + \frac{1}{p}\lambda\right).$$

We also write σ_4 as

$$\begin{aligned}\sigma_4 &= \eta_{2,1}(1-(1-\alpha)^2) + \eta_{2,2}\lambda \\ &= \left(\frac{1}{2}\frac{p(p^2-1)}{p^3-1}\right)\left(1-(1-\alpha)^2\right) + \left(\frac{p^2-1}{p^3-1}\right)\lambda.\end{aligned}$$

Using the above relations and (4.5.15) from Lemma 4.5.17, we have four equations relating $\sigma_4, \sigma_4^*, \rho^*, \lambda$, which may be solved using computer algebra software to produce (4.8.2) – (4.8.7). For an implementation using Sage [Sag21], see the GitHub repository associated to this paper [BK21b, `SEC_rho36_23Aug21.ipynb`]. □

4.5.5 Triple factors: computing σ_5

Suppose $p \neq 3$. Then if $\overline{F}$ has factorization type 5, we have $F \equiv y^3 \pmod{p}$, so the coefficients of $f(x, z)$ are all divisible by p.

For any solution, that is, for any $[x_0 : y_0 : z_0]$ such that $F(x_0, y_0, z_0) = 0$, we have that $y_0^3 = f(x_0, z_0)$. Since we are assuming that $[x_0 : y_0 : z_0]$ is a solution, we also have that $0 = y_0^3 - f(x_0, z_0) = y_0^3 \pmod{p}$, and thus $p \mid y_0^3$ so we have that $p^3 \mid y_0^3$. Since we have $y_0^3 = f(x_0, z_0)$, then $p^3 \mid f(x_0, z_0)$.

Writing $f_1 = \frac{1}{p} f$, we see that each solution $[x_0 : y_0 : z_0]$ satisfies $f_1(x_0, z_0) \equiv y_0 \equiv 0 \pmod{p}$. Thus we will consider the different possible factorizations of $f_1(x, z)$ modulo p. If $f_1(x, z) \equiv 0 \pmod{p}$ then all the coefficients of f are divisible by p^2 and so we can write $f_2 = \frac{1}{p^2} f$. Now each solution $[x_0 : y_0 : z_0]$ must satisfy $f_2(x_0, z_0) \equiv y_0 \equiv 0 \pmod{p}$ and so we consider the different possible factorizations of $f_2(x, z)$ modulo p.

Now if $f_2(x, z) \equiv 0 \pmod{p}$, then all of the coefficients of $f(x, z)$ are divisible by p^3. In this case we can replace y by py and divide through by p^3 and obtain another arbitrary superelliptic curve with $m = 3$ and $d = 6$, namely, $y^3 = \frac{1}{p} f_2(x, z)$ with coefficients in $\mathbb{Z}_p$ in which case, the probability of solubility is ρ. This occurs with probability $\frac{1}{p^{14}}$.

For $i = 0, \ldots, 9$, we denote by $\eta_{6,i}$ the probability of each possible factorization type for a binary sextic modulo p (see Lemma 4.5.6), and we denote by τ_i (respectively θ_i) the probability of solubility of f_1 (respectively f_2) with factorization type i modulo p. Thus we have:

$$\sigma_5 = \frac{1}{p^{14}}\rho + \left(1 - \frac{1}{p^7}\right) \sum_{i=0}^{9} \eta_{6,i}\tau_i + \left(\frac{p^7 - 1}{p^{14}}\right) \sum_{i=0}^{9} \eta_{6,i}\theta_i.$$

In order to compute the τ_i and θ_i, we make the following definitions. Let σ_5' be the probability that $F(x, y, z)$ has a $\mathbb{Q}_p$-solution when $v(c_6) = 1$ and $v(c_i) \geq 1$ for $0 \leq i \leq 5$. Take σ_5'' to be the probability that $F(x, y, z)$ has a $\mathbb{Q}_p$-solution when $v(c_6) = 2$ and $v(c_i) \geq 2$ for $0 \leq i \leq 5$.

Proposition 4.5.18. *Suppose C_f is given by (4.5.1) and $\overline{F}$ has factorization type 5 modulo p for a prime $p > 43$ or $p > 2$ with $p \equiv 2 \pmod{3}$. Then the proportion of f for which $C_f(\mathbb{Q}_p) \neq \emptyset$ is a rational function in p given explicitly by*

$$\sigma_5 = (4.8.5).$$

The proportions σ_5' and σ_5'' defined above are also rational functions in p,

$$\sigma_5' = (4.8.8),$$
$$\sigma_5'' = (4.8.9).$$

The proofs of these equalities are spread across the remainder of this section. σ_5' is computed in the proof Lemma 4.5.19, along with the values of τ_i. σ_5'' is computed in the proof of Lemma 4.5.21, along with the θ_i values. The proof is completed in §4.5.5 with the computation of σ_5, along with $\rho_{3,6}$.

Lemma 4.5.19. *The τ_i values are tabulated below. These hold for all primes $p > 31$, and for $p > 3$ if $p \equiv 2 \pmod 3$.*

$$\tau_0 = 0 \qquad \tau_5 = \begin{cases} \frac{3p^3+p^2+2p+2}{3(p^4+p^3+p^2+p+1)}, & p \equiv 1 \pmod 3 \\ \frac{(3p^2+2)(p+1)}{3(p^4+p^3+p^2+p+1)}, & p \equiv 2 \pmod 3 \end{cases}$$

$$\tau_1 = 1 \qquad \tau_6 = 1 - (1-\tau_5)^2 = (4.8.10)$$

$$\tau_2 = \frac{1}{p} \qquad \tau_7 = (4.8.11)$$

$$\tau_3 = 1 - (1-\tau_2)^2 = \frac{2p-1}{p^2} \qquad \tau_8 = 1 - (1-\tau_2)(1-\tau_7) = (4.8.12)$$

$$\tau_4 = 1 - (1-\tau_2)^3 = \frac{3p^2-3p+1}{p^3} \qquad \tau_9 = (4.8.13)$$

Proof. Recall that $f_1 = \frac{1}{p} f$ and assume $f_1 \not\equiv 0 \pmod p$. We consider the possible factorization types of f_1 as a binary sextic form, given by the index i in the $d = 6$ row of Lemma 4.5.6, and compute the probabilities τ_i of a root $f_1(x, z) \equiv 0$ lifting to a $\mathbb{Q}_p$-point of C_f.

No roots: τ_0

If $f_1(x, z) \equiv 0 \pmod p$ has no roots in $\mathbb{F}_p$, then $f(x, z) \equiv 0 \pmod{p^2}$ has no solutions and thus $f(x, z) \equiv 0 \pmod{p^3}$ has no solutions, so $\tau_0 = 0$.

Simple roots: τ_1

If $f_1(x,z) \equiv 0 \pmod{p}$ has a simple root in $\mathbb{F}_p$, it lifts to a $\mathbb{Q}_p$-point on C_f of the form $[x_0 : y_0 : z_0]$ with $p \mid y_0$ (see also λ_i in the proof of Lemma 4.5.17), so $\tau_1 = 1$.

Double roots: τ_2**,** τ_3**,** ***and*** τ_4

If $f_1(x,z) \equiv 0 \pmod{p}$ has a double root in $\mathbb{F}_p$, we can assume this root occurs at $[0:1]$ and the valuations of the coefficients are as in the first line of the following table.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\tau_2 =$	$\tau_{2a} =$	$\frac{1}{p}\tau_{2b}$	≥ 1	≥ 1	≥ 1	≥ 1	$= 1$	≥ 2	≥ 2
	$\tau_{2b} =$	1	≥ 4	≥ 3	≥ 2	≥ 1	$= 0$	≥ 0	≥ 0

(a) Since $p \mid x$, reducing modulo p^3 reveals that $p \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace x, y by px, py and divide by p^3.

(b) The justification is identical to that of λ_d.

Thus we have $\tau_2 = \frac{1}{p}$.

If $f_1(x,z)$ has two double roots in $\mathbb{F}_p$, then after composing with an automorphism of $\mathbb{P}^1$, they occur at $[0:1]$ and $[1:0]$, and we have $v(c_0), v(c_1), v(c_5), v(c_6) \geq 2$ and $v(c_2) = v(c_4) = 1$. The probability, τ_2, that the root at $[0:1]$ lifts to a $\mathbb{Q}_p$-point depends only on c_0; the same argument with c_6 shows that τ_2 is the probability $[1:0]$ lifts and thus the two are independent. This allows us to write

$$\tau_3 = 1 - (1 - \tau_2)^2 = \frac{2p-1}{p^2}.$$

If $f_1(x,z)$ has three double roots in $\mathbb{F}_p$, then after composing with an automorphism of $\mathbb{P}^1$, we may assume they occur at $[0:1]$, $[1:1]$, and $[1:0]$. To extend the independence argument above to these three roots, we need to argue that the probability of $[1:1]$ lifting is still τ_2, even if we assume the points at $[0:1]$ and $[1:0]$ do not lift. To see this, we recognize that $f(1,1) = \sum_{i=0}^{d} c_i$, and our assumption that f_1 has a double root at $[1:1]$

is equivalent to requiring $v\left(\sum_{i=0}^{d} c_i\right) \geq 2$. Running through the proof of τ_2 shows that we need only for $v\left(\sum_{i=0}^{d} c_i\right) \geq 3$, which occurs with probability $\frac{1}{p}$, independent of the valuations of c_0, c_1, c_5, c_6 (i.e. independent of the lifting behavior at $[0:1]$ and $[1:0]$). Therefore

$$\tau_4 = 1 - (1-\tau_2)^3 = \frac{3p^2 - 3p + 1}{p^3}.$$

Triple roots: τ_5 ***and*** τ_6

If $f_1(x,z) \equiv 0 \pmod{p}$ has a triple root in $\mathbb{F}_p$ we can assume the valuations of the coefficients are as in line 1 of the following table.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\tau_5 =$	$\tau_{5a} =$	$\frac{1}{p}\tau_{5b}$	≥ 1	≥ 1	≥ 1	$= 1$	≥ 2	≥ 2	≥ 2
	$\tau_{5b} =$	β'	≥ 4	≥ 3	≥ 2	$= 1$	≥ 1	≥ 0	≥ 0

(a) Since $p \mid x$, reducing modulo p^3 reveals that $p \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace x, y by px, py and divide by p^3.

(b) We are in the situation of $\beta' =$ (4.5.9); see Lemma 4.5.12.

In the case of τ_5, $f(x,z)$ has one triple root and no other roots, therefore any $\mathbb{Q}_p$ point must come from lifting the triple root which happens with probability $\frac{1}{p}\beta'$, thus giving $\tau_5 = \frac{1}{p}\beta'$, which is equal to the stated expression.

In the case of τ_6, $f(x,z)$ has two triple roots. We assumed that one triple root was at $[x:z] = [0:1]$ and we could similarly assume the other triple root is at $[1:0]$. The probabilities of these lifting are independent because the computation of the former involves coefficients c_2, c_1, c_0 and the second involves coefficients c_4, c_5, c_6. Thus each point lifts to a $\mathbb{Q}_p$ point with probability $\frac{1}{p}\beta'$, and hence

$$\tau_6 = 1 - (1-\tau_5)^2 = (4.8.10).$$

Quadruple roots τ_7 and τ_8

If $f_1(x,z) \equiv 0 \pmod{p}$ has a quadruple root in $\mathbb{F}_p$, we can assume the the root occurs at $[0:1]$ and the coefficients have valuations as listed in the first line of the following table.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\tau_7 =$	$\tau_{7a} =$	$\frac{1}{p}\tau_{7b}$	≥ 1	≥ 1	$= 1$	≥ 2	≥ 2	≥ 2	≥ 2
	$\tau_{7b} =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\tau_{7c}$	≥ 4	≥ 3	$= 2$	≥ 2	≥ 1	≥ 0	≥ 0
	$\tau_{7c} =$	$\Phi(p)+\frac{1}{p}\tau_{7d}$	≥ 4	≥ 3	$= 2$	≥ 2	≥ 1	≥ 1	≥ 0
	$\tau_{7d} =$	$\left(1-\frac{1}{p}\right)\left(\frac{p-1}{2p}+\frac{1}{p^2}\right)+\frac{1}{p}\tau_{7e}$	≥ 4	≥ 3	$= 2$	≥ 2	≥ 1	≥ 1	≥ 1
	$\tau_{7e} =$	$\left(1-\frac{1}{p}\right)+\frac{1}{p}\tau_{7f}$	≥ 4	≥ 3	$= 2$	≥ 2	≥ 2	≥ 1	≥ 1
	$\tau_{7f} =$	$\frac{1}{p}\tau_{7g}$	≥ 4	≥ 3	$= 2$	≥ 2	≥ 2	≥ 2	≥ 1
	$\tau_{7g} =$	μ	≥ 4	≥ 3	$= 2$	≥ 2	≥ 2	≥ 2	≥ 2

(a) Since $p \mid x$, reducing modulo p^3 reveals that $p \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace x, y by px, py and divide by p^3.

(b) With probability $1-\frac{1}{p}$ we have $v(c_1) = 0$ and the reduced equation is $\overline{F}(x,y,1) = y^3 - c_1x - c_0$, which is linear in x and thus has a solution with $y \in p\mathbb{Z}_p$. With probability $\frac{1}{p}$ we have $v(c_1) \geq 1$ and move to the next line.

(c) The reduced equation is now $\overline{F} = y^3 - c_0$. The probability that c_0 is a nonzero cubic residue is

$$\Phi(p) = \begin{cases} \frac{1}{3}\left(1-\frac{1}{p}\right), & p \equiv 1 \pmod 3 \\ 1-\frac{1}{p}, & p \equiv 2 \pmod 3 \end{cases}$$

(see Proposition 4.3.6 for the definition of $\Phi(p)$). If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(d) With probability $1-\frac{1}{p}$ we have $v(c_2) = 1$. It is clear that for any solution, we must have $p \mid y$ and $\frac{1}{p}(c_2x^2+c_1x+c_0) \equiv 0 \pmod{p}$. The quadratic $\frac{1}{p}(c_2x^2+c_1x+c_0)$ has no roots with probability $\eta'_{2,0} = \frac{1}{2}\frac{(p-1)}{p}$ and distinct roots with probability $\eta'_{2,1} = \frac{1}{2}\frac{(p-1)}{p}$. In the case of distinct roots, one can check that either root lifts to the x-coordinate

of a $\mathbb{Q}_p$-point with $y \in p\mathbb{Z}_p$. A double root occurs with probability $\eta'_{2,2} = \frac{1}{p}$, and the probability of a solution lifting is equal to $\tau_2 = \frac{1}{p}$. Thus we have

$$\tau_{7d} = \left(1 - \frac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\tau_2\right) + \frac{1}{p}\tau_{7e} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{1}{p^2}\right) + \frac{1}{p}\tau_{7e}.$$

(e) Modulo p^2 we have $\frac{1}{p}(c_1 x + c_0)$, so if $v_p(c_1) = 1$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(f) Reducing modulo p^2, we see that $p^2 \mid c_0$ is necessary to get a $\mathbb{Q}_p$ solution. This happens with probability $\frac{1}{p}$ and so we move to the next line.

(g) We are now in the case of $\mu =$ (4.5.12) from Lemma 4.5.14.

In the case of τ_7 there is only a quadruple root so any $\mathbb{Q}_p$-point must come from lifting a quadruple root which happens with probability τ_7, computed to be (4.8.11).

In the case of τ_8, there is a quadruple root and a double root. We can make the usual argument about independence of these lifting based on which coefficients were used for the argument. Then

$$\tau_8 = 1 - (1 - \tau_7)(1 - \tau_2) = (4.8.12).$$

Sextuple roots: τ_9 and σ'_5

If $f_1(x, z) \equiv 0 \pmod{p}$ has a sextuple root in $\mathbb{F}_p$, we can assume this root occurs at $[0 : 1]$ and the valuations of the coefficients are as in the first line of the following table.

		c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\tau_9 =$	$\tau_{9a} = \frac{1}{p}\tau_{9b}$	$= 1$	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2
	$\tau_{9b} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\tau_{9c}$	$= 4$	≥ 4	≥ 3	≥ 2	≥ 1	≥ 0	≥ 0
	$\tau_{9c} = \Phi(p) + \frac{1}{p}\tau_{9d}$	$= 4$	≥ 4	≥ 3	≥ 2	≥ 1	≥ 1	≥ 0
	$\tau_{9d} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{1}{p^2}\right) + \frac{1}{p}\tau_{9e}$	$= 4$	≥ 4	≥ 3	≥ 2	≥ 1	≥ 1	≥ 1
	$\tau_{9e} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\tau_{9f}$	$= 4$	≥ 4	≥ 3	≥ 2	≥ 2	≥ 1	≥ 1
	$\tau_{9f} = \frac{1}{p}\tau_{9g}$	$= 4$	≥ 4	≥ 3	≥ 2	≥ 2	≥ 2	≥ 1
	$\tau_{9g} = \left(1 - \frac{1}{p}\right)\alpha'' + \frac{1}{p}\tau_{9h}$	$= 4$	≥ 4	≥ 3	≥ 2	≥ 2	≥ 2	≥ 2
	$\tau_{9h} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{\theta_2}{p}\right) + \frac{1}{p}\tau_{9i}$	$= 4$	≥ 4	≥ 3	≥ 3	≥ 2	≥ 2	≥ 2
	$\tau_{9i} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\tau_{9j}$	$= 4$	≥ 4	≥ 3	≥ 3	≥ 3	≥ 2	≥ 2
	$\tau_{9j} = \frac{1}{p}\tau_{9k}$	$= 4$	≥ 4	≥ 3	≥ 3	≥ 3	≥ 3	≥ 2
	$\tau_{9k} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\tau_{9\ell}$	$= 1$	≥ 1	≥ 0	≥ 0	≥ 0	≥ 0	≥ 0
	$\tau_{9\ell} = \Phi(p) + \left(1 - \Phi(p) - \frac{1}{p}\right)\beta + \frac{1}{p}\tau_{9m}$	$= 1$	≥ 1	≥ 1	≥ 0	≥ 0	≥ 0	≥ 0
	$\tau_{9m} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\tau_{9n}$	$= 1$	≥ 1	≥ 1	≥ 1	≥ 0	≥ 0	≥ 0
	$\tau_{9n} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\tau_{9o}$	$= 1$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 0	≥ 0
	$\tau_{9o} = \Phi(p) + \frac{1}{p}\tau_{9p}$	$= 1$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 0
	$\tau_{9p} = \sigma_5'$	$= 1$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1

(a) Since $p \mid x$, reducing modulo p^3 reveals that $p^3 \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace x, y by px, py and divide by p^3.

(b) With probability $1 - \frac{1}{p}$ we have $v(c_1) = 0$ and the reduced equation is $\overline{F}(x, y, 1) = y^3 - c_1 x - c_0$, which is linear in x and thus has a solution with $y \in p\mathbb{Z}_p$. With probability $\frac{1}{p}$ we have $v(c_1) \geq 1$ and move to the next line.

(c) The reduced equation is now $\overline{F} = y^3 - c_0$. The probability that c_0 is a nonzero cubic residue is $\Phi(p)$. If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(d) The justification is identical to τ_{7d}, producing

$$\tau_{9d} = \left(1 - \frac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\tau_2\right) + \frac{1}{p}\tau_{9e} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{1}{p^2}\right) + \frac{1}{p}\tau_{9e}.$$

(e) Modulo p^2 we have $\frac{1}{p}(c_1 x + c_0)$, so if $v_p(c_1) = 1$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(f) Reducing modulo p^2, we see that $p^2 \mid c_0$ is necessary to get a $\mathbb{Q}_p$ solution. This happens with probability $\frac{1}{p}$ and so we move to the next line.

(g) If $v(c_3) = 2$, then we are in the situation of $\alpha'' = (4.5.10)$ from Lemma 4.5.12. This happens with probability $1 - 1/p$, so with probability $1/p$ we have $v(c_3) \geq 3$ and we move to the next line.

(h) With probability $1-\frac{1}{p}$ we have $v(c_2) = 2$. It is clear that for any solution, we must have $p \mid y$ and $\frac{1}{p^2}(c_2x^2 + c_1x + c_0) \equiv 0 \pmod{p}$. The quadratic $\frac{1}{p^2}(c_2x^2 + c_1x + c_0)$ has no roots with probability $\eta'_{2,0} = \frac{1}{2}\frac{(p-1)}{p}$ and distinct roots with probability $\eta'_{2,1} = \frac{1}{2}\frac{(p-1)}{p}$. In the case of distinct roots, one can check that either root lifts to the x-coordinate of a $\mathbb{Q}_p$-point with $y \in p\mathbb{Z}_p$. A double root occurs with probability $\eta'_{2,2} = \frac{1}{p}$, and the probability of a solution lifting is equal to θ_2, given in Lemma 4.5.21. Thus we have

$$\tau_{9h} = \left(1 - \frac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\theta_2\right) + \frac{1}{p}\tau_{9i} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{\theta_2}{p}\right) + \frac{1}{p}\tau_{9i}.$$

(i) Modulo p^3 we have $\frac{1}{p^2}(c_1x + c_0)$, so if $v_p(c_1) = 2$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(j) Reducing modulo p^3 reveals that $p^3 \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace y by py and divide by p^3.

(k) With probability $1 - \frac{1}{p}$ we have $v(c_4) = 0$, in which case the normalization of $\overline{C_f}$ is seen to have geometric genus at most 3. Since $\overline{f} \neq ah^3$ for $a \in \mathbb{F}_p$ and $h \in \mathbb{F}_p[x, z]$, we apply the Hasse–Weil bound (see the proof of Proposition 4.3.2) to find

$$\#\overline{C_f}^{\mathrm{sm}}(\mathbb{F}_p) \geq p + 1 - 6\sqrt{p} > 1,$$

where the rightmost inequality holds for all primes $p > 31$. $\overline{C_f}$ has only the point $[1 : 0 : 0]$ above infinity, so there must exist some smooth $\mathbb{F}_p$-point $[x : y : 1]$ which lifts to a $\mathbb{Q}_p$-point of C_f. If $p \equiv 2 \pmod{3}$, it suffices to take $p > 2$ (see the proof of Proposition 4.3.4). If $v(c_4) \geq 1$ we move to the next line.

(ℓ) With probability $1 - \frac{1}{p}$ we have $v(c_3) = 0$, in which case the normalization of $\overline{C_f}$ is seen to have geometric genus at most 1. If $p \equiv 1 \pmod 3$ and $c_3 \in \left(\mathbb{F}_p^\times\right)^3$ is a nonzero cubic residue, then whenever $\overline{f} \neq c_3(x - \alpha z)$ for $\alpha \in \mathbb{F}_p[x, z]$, we apply the Hasse–Weil bound (see the proof of Proposition 4.3.2) to find

$$\#\overline{C_f}^{\mathrm{sm}}(\mathbb{F}_p) \geq p + 1 - 2\sqrt{p} > 3,$$

where the rightmost inequality holds for all primes $p > 7$. In this case, $\overline{C_f}$ must possess a smooth $\mathbb{F}_p$-point $[x : y : 1]$ which then lifts to a $\mathbb{Q}_p$-point of C_f. On the other hand, if $\overline{f} = c_3(x - \alpha z)$ then the fact that c_3 is a cubic residue produces a liftable solution. If c_3 is not a cubic residue, the probability of solution is given by β. If $p \equiv 2 \pmod 3$, it suffices to take $p > 2$ (see the proof of Proposition 4.3.2). In either case, we have

$$\tau_{9\ell} = \Phi(p) + \left(1 - \Phi(p) - \frac{1}{p}\right)\beta + \frac{1}{p}\tau_{9m},$$

which is well defined when $p \equiv 2 \pmod 3$ even though β is not, since $1 - \Phi(p) - \frac{1}{p} = 0$.

(m) The justification is identical to that of λ_d.

(n) The justification is identical to that of line (b).

(o) The justification is identical to that of line (c).

(p) This is the definition of σ_5'.

The table above gives us a relation between τ_9 and σ_5', while the definition of σ_5' gives another:

$$\sigma_5' = \sum_{i=0}^{9} \eta_{6,i}' \tau_i.$$

Solving the two simultaneously give the values of $\tau_9 =$ (4.8.13) and $\sigma_5' =$ (4.8.8). □

Remark 4.5.20. The independence argument used in the computation of τ_4 in terms of τ_2 makes use of the 3-transitivity of $\operatorname{Aut}\mathbb{P}^1$. This argument breaks down if attempting to lift more than three such roots independently, suggesting that more care may be needed to compute $\rho_{m,d}(p)$ exactly when $d \geq 8$.

Lemma 4.5.21. *The θ_i values are tabulated below. These hold for all primes $p > 31$, and for $p > 3$ if $p \equiv 2 \pmod 3$.*

$$\theta_0 = 0 \qquad \theta_5 = \begin{cases} \frac{p^4+3p^3+2p+2}{3(p^4+p^3+p^2+p+1)}, & p \equiv 1 \pmod 3 \\ \frac{(3p^3+2)(p+1)}{3(p^4+p^3+p^2+p+1)}, & p \equiv 2 \pmod 3 \end{cases}$$

$$\theta_1 = 1 \qquad \theta_6 = (4.8.16)$$

$$\theta_2 = \begin{cases} \frac{(2p^2-3p+3)(p+2)}{6p^3}, & p \equiv 1 \pmod 3 \\ \frac{(2p^2-3p+2)(p+1)}{2p^3}, & p \equiv 2 \pmod 3 \end{cases} \qquad \theta_7 = (4.8.17)$$

$$\theta_3 = 1 - (1-\theta_2)^2 = (4.8.14) \qquad \theta_8 = (4.8.18)$$

$$\theta_4 = 1 - (1-\theta_2)^3 = (4.8.15) \qquad \theta_9 = (4.8.19)$$

Proof. Recall that $f_2 = \frac{1}{p^2} f$ and assume $f_2 \not\equiv 0 \pmod p$. We consider the possible factorization types of f_2 as a binary sextic form, given by the index i in the $d = 6$ row of Lemma 4.5.6, and compute the probabilities θ_i of a root $f_2(x, z) \equiv 0$ lifting to a $\mathbb{Q}_p$-point of C_f.

No roots: θ_0

If $f_2(x, z) \equiv 0 \pmod p$ has no roots in $\mathbb{F}_p$, then $f(x, z) \equiv 0 \pmod{p^3}$ has no solutions, so $\theta_0 = 0$.

Simple roots: θ_1

If $f_2(x, z) \equiv 0 \pmod p$ has a simple root in $\mathbb{F}_p$, it lifts to a $\mathbb{Q}_p$-point on C_f of the form $[x_0 : y_0 : z_0]$ with $p \mid y_0$, so $\theta_1 = 1$.

Double roots: θ_2, θ_3, *and* θ_4

If $f_2(x, z) \pmod p$ has a double root in $\mathbb{F}_p$, after composition with an automorphism of $\mathbb{P}^1$, we can assume the root occurs at $[0 : 1]$. Replacing x, y by px, py and dividing by p^3 we obtain the valuations of the coefficients listed in the first line of the following table.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\theta_2 =$	$\theta_{2a} =$	$\Phi(p) + \frac{1}{p}\theta_{2b}$	≥ 5	≥ 4	≥ 3	≥ 2	$= 1$	≥ 1	≥ 0
	$\theta_{2b} =$	$\frac{1}{2}\left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{2c}$	≥ 5	≥ 4	≥ 3	≥ 2	$= 1$	≥ 1	≥ 1
	$\theta_{2c} =$	$\frac{1}{p}\theta_{2d}$	≥ 5	≥ 4	≥ 3	≥ 2	$= 1$	≥ 2	≥ 2
	$\theta_{2d} =$	1	≥ 8	≥ 6	≥ 4	≥ 2	$= 0$	≥ 0	≥ 0

(a) After the change of variables, reduced equation is $\overline{F} = y^3 - c_0$. The probability that c_0 is a nonzero cubic residue is $\Phi(p)$. If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(b) In this case, we consider the quadratic $\frac{1}{p}(c_2x^2 + c_1x + c_0)$ over $\mathbb{F}_p$. If it has a simple root, which happens with probability $\eta'_{2,1} = \frac{1}{2}\left(1 - \frac{1}{p}\right)$, these lift to $\mathbb{Q}_p$ points with $y \in p\mathbb{Z}_p$. If it has no roots, the equation is insoluble, and if the quadratic has a double root, which happens with probability $\eta'_{2,2} = \frac{1}{p}$, we can shift it to $[0 : 1]$, giving the valuations in the next line.

(c) Reducing modulo p^3 reveals that $p^3 \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace x, y by px, py and divide by p^3.

(d) The justification is identical to that of λ_d.

This gives the expression for θ_2 in the statement. The same independence arguments as for τ_2 and τ_3 in the proof of Lemma 4.5.19 apply here to give

$$\theta_3 = 1 - (1 - \theta_2)^2 = (4.8.14).$$

For θ_4, we need to modify the argument from τ_4 slightly. We observe that for $p > 2$ if $c_1, \ldots, c_6$ are fixed (satisfying the conditions above) then as c_0 varies, the probability of a lift is precisely θ_2. This is already clear for steps θ_{2a} and θ_{2c} above. To see why this holds for θ_{2b}, we consider the quadratic

$$x^2 + \frac{c_1}{c_2}x + \frac{c_0}{c_2},$$

whose discriminant $\frac{c_1^2}{c_2^2} - 4\frac{c_0}{c_2}$ determines its factorization type. This discriminant is linear in c_0, so for fixed c_1, c_2, as c_0 runs through $p\mathbb{Z}_p$, it will take quadratic residue/nonresidue values with probability $\frac{p-1}{2p}$, and be divisible by p with probability $\frac{1}{p}$.

Hence, we see that for $p \neq 2$, we can view θ_2 as depending only on the value of c_0. Thus, as in the determination of τ_4 in the proof of Lemma 4.5.19, we see that after moving the roots to $[0:1], [1:1]$, and $[1:0]$, the lifting behavior at $[1:1]$ is independent of the other points, making

$$\theta_4 = 1 - (1-\theta_2)^3 = (4.8.15).$$

In the case of $p = 2$ — which will be needed in §4.5.6 — we observe that the proof of θ_2 above shows that lifting $[0:1]$ depends only on c_0, c_1, and the valuation of c_2. thus the lifting behavior of $[1:0]$ depends only on c_5, c_6, and the valuation of c_4. For θ_4, the other double root is located at $[1:1]$, and the lifting argument depends on

$$f(1,1) = \sum_{i=0}^{6} c_i \quad \text{and} \quad f'(1,1) = \sum_{i=0}^{6} i c_i.$$

The latter can be controlled by c_3, while the former may be controlled by writing $c_2 = 4 + 8c_2'$ for some $c_2' \in \mathbb{Z}_2$ and letting c_2' vary. This is independent of c_0, c_1, c_5, c_6, and so we have that $\theta_4 = 1 - (1-\theta_2)^3 = (4.8.15)$ for $p = 2$ as well.

Triple roots: θ_5 *and* θ_6

If $f_2(x,z) \pmod p$ has a triple root in $\mathbb{F}_p$, after composition with an automorphism of $\mathbb{P}^1$, we can assume the root occurs at $[0:1]$. Replacing x, y by px, py and dividing by p^3 we obtain the valuations of the coefficients listed in the first line of the following table.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\theta_5 =$	$\theta_{5a} =$	$\Phi(p) + \frac{1}{p}\theta_{5b}$	≥ 5	≥ 4	≥ 3	$= 2$	≥ 2	≥ 1	≥ 0
	$\theta_{5b} =$	$\left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{5c}$	≥ 5	≥ 4	≥ 3	$= 2$	≥ 2	≥ 1	≥ 1
	$\theta_{5c} =$	$\frac{1}{p}\theta_{5d}$	≥ 5	≥ 4	≥ 3	$= 2$	≥ 2	≥ 2	≥ 1
	$\theta_{5d} =$	α''	≥ 5	≥ 4	≥ 3	$= 2$	≥ 2	≥ 2	≥ 2

(a) After the change of variables, reduced equation is $\overline{F} = y^3 - c_0$. The probability that

c_0 is a nonzero cubic residue is $\Phi(p)$. If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(b) Modulo p^2 we have $\frac{1}{p}(c_1 x + c_0)$, so if $v_p(c_1) = 1$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(c) Reducing modulo p^2 reveals that $p^2 \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$, and we move to the next line.

(d) We are in the situation of α'' = (4.5.10) from Lemma 4.5.12.

This gives the expression for θ_5 in the statement. The same independence argument as for τ_5 and τ_6 in the proof of Lemma 4.5.19 apply to give

$$\theta_6 = 1 - (1 - \theta_5)^2 = (4.8.16).$$

Quadruple roots: θ_7 *and* θ_8

If $f_2(x, z) \pmod p$ has a quadruple root in $\mathbb{F}_p$, after composition with an automorphism of $\mathbb{P}^1$, we can assume the root occurs at $[0 : 1]$. Replacing x, y by px, py and dividing by p^3 we obtain the valuations of the coefficients listed in the first line of the following table.

			c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\theta_7 =$	$\theta_{7a} =$	$\Phi(p) + \frac{1}{p}\theta_{7b}$	≥ 5	≥ 4	$= 3$	≥ 3	≥ 2	≥ 1	≥ 0
	$\theta_{7b} =$	$\left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{7c}$	≥ 5	≥ 4	$= 3$	≥ 3	≥ 2	≥ 1	≥ 1
	$\theta_{7c} =$	$\frac{1}{p}\theta_{7d}$	≥ 5	≥ 4	$= 3$	≥ 3	≥ 2	≥ 2	≥ 1
	$\theta_{7d} =$	$\left(1 - \frac{1}{p}\right)\left(\frac{1}{2}\left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_2\right) + \frac{1}{p}\theta_{7e}$	≥ 5	≥ 4	$= 3$	≥ 3	≥ 2	≥ 2	≥ 2
	$\theta_{7e} =$	$\left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{7f}$	≥ 5	≥ 4	$= 3$	≥ 3	≥ 3	≥ 2	≥ 2
	$\theta_{7f} =$	$\frac{1}{p}\theta_{7g}$	≥ 5	≥ 4	$= 3$	≥ 3	≥ 3	≥ 3	≥ 2
	$\theta_{7g} =$	1	≥ 2	≥ 1	$= 0$	≥ 0	≥ 0	≥ 0	≥ 0

(a) The reduced equation is $\overline{F} = y^3 - c_0$. The probability that c_0 is a nonzero cubic residue is $\Phi(p)$. If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(b) Modulo p^2 we have $\frac{1}{p}(c_1 x + c_0)$, so if $v_p(c_1) = 1$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(c) Reducing modulo p^2 reveals that $p^2 \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$, and we move to the next line.

(d) With probability $1-\frac{1}{p}$ we have $v(c_2) = 2$. It is clear that for any solution, we must have $p \mid y$ and $\frac{1}{p^2}(c_2x^2 + c_1x + c_0) \equiv 0 \pmod{p}$. The quadratic $\frac{1}{p^2}(c_2x^2 + c_1x + c_0)$ has no roots with probability $\eta'_{2,0} = \frac{1}{2}\frac{(p-1)}{p}$ and distinct roots with probability $\eta'_{2,1} = \frac{1}{2}\frac{(p-1)}{p}$. In the case of distinct roots, one can check that either root lifts to the x-coordinate of a $\mathbb{Q}_p$-point with $y \in p\mathbb{Z}_p$. A double root occurs with probability $\eta'_{2,2} = \frac{1}{p}$, and the probability of a solution lifting is equal to θ_2. Thus we have

$$\theta_{7d} = \left(1 - \frac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\theta_2\right) + \frac{1}{p}\theta_{7e} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{\theta_2}{p}\right) + \frac{1}{p}\theta_{7e}.$$

(e) Modulo p^3 we have $(c_1x + c_0)$, so if $v_p(c_1) = 2$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(f) Reducing modulo p^3 reveals that $p^3 \mid c_0$ is necessary, which occurs with probability $\frac{1}{p}$. Before moving to the next line, we replace y by py and divide by p^3.

(g) The justification is identical to that of τ_{9k}.

This gives the expression for θ_7 in (4.8.17). The same argument as for τ_7 and τ_8 in the proof of Lemma 4.5.19 applies here to give

$$\theta_8 = 1 - (1 - \theta_7)(1 - \theta_2) = (4.8.18).$$

Sextuple roots: θ_9

If $f_2(x, z) \pmod{p}$ has a sextuple root in $\mathbb{F}_p$, after composition with an automorphism of $\mathbb{P}^1$, we can assume the root occurs at $[0 : 1]$. Replacing x, y by px, py and dividing by p^3 we obtain the valuations of the coefficients listed in the first line of the following table.

		c_6	c_5	c_4	c_3	c_2	c_1	c_0
$\theta_9 =$	$\theta_{9a} = \Phi(p) + \frac{1}{p}\theta_{9b}$	$= 5$	≥ 5	≥ 4	≥ 3	≥ 2	≥ 1	≥ 0
	$\theta_{9b} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{9c}$	$= 5$	≥ 5	≥ 4	≥ 3	≥ 2	≥ 1	≥ 1
	$\theta_{9c} = \frac{1}{p}\theta_{9d}$	$= 5$	≥ 5	≥ 4	≥ 3	≥ 2	≥ 2	≥ 1
	$\theta_{9d} = \left(1 - \frac{1}{p}\right)\left(\frac{1}{2}\left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_2\right) + \frac{1}{p}\theta_{9e}$	$= 5$	≥ 5	≥ 4	≥ 3	≥ 2	≥ 2	≥ 2
	$\theta_{9e} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{9f}$	$= 5$	≥ 5	≥ 4	≥ 3	≥ 3	≥ 2	≥ 2
	$\theta_{9f} = \frac{1}{p}\theta_{9g}$	$= 5$	≥ 5	≥ 4	≥ 3	≥ 3	≥ 3	≥ 2
	$\theta_{9g} = \Phi(p) + \left(1 - \Phi(p) - \frac{1}{p}\right)\beta + \frac{1}{p}\theta_{9h}$	$= 2$	≥ 2	≥ 1	≥ 0	≥ 0	≥ 0	≥ 0
	$\theta_{9h} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{9i}$	$= 2$	≥ 2	≥ 1	≥ 1	≥ 0	≥ 0	≥ 0
	$\theta_{9i} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{9j}$	$= 2$	≥ 2	≥ 1	≥ 1	≥ 1	≥ 0	≥ 0
	$\theta_{9j} = \Phi(p) + \frac{1}{p}\theta_{9k}$	$= 2$	≥ 2	≥ 1	≥ 1	≥ 1	≥ 1	≥ 0
	$\theta_{9k} = \left(1 - \frac{1}{p}\right)\mu' + \frac{1}{p}\theta_{9\ell}$	$= 2$	≥ 2	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1
	$\theta_{9\ell} = \left(1 - \frac{1}{p}\right)\alpha' + \frac{1}{p}\theta_{9m}$	$= 2$	≥ 2	≥ 2	≥ 1	≥ 1	≥ 1	≥ 1
	$\theta_{9m} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{1}{p^2}\right) + \frac{1}{p}\theta_{9n}$	$= 2$	≥ 2	≥ 2	≥ 2	≥ 1	≥ 1	≥ 1
	$\theta_{9n} = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\theta_{9o}$	$= 2$	≥ 2	≥ 2	≥ 2	≥ 2	≥ 1	≥ 1
	$\theta_{9o} = \frac{1}{p}\theta_{9p}$	$= 2$	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2	≥ 1
	$\theta_{9p} = \sigma_5''$	$= 2$	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2

(a) The reduced equation is now $\overline{F} = y^3 - c_0$. The probability that c_0 is a nonzero cubic residue is $\Phi(p)$. If $p \nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0) = 1$ and we move to the next line.

(b) Modulo p^2 we have $\frac{1}{p}(c_1 x + c_0)$, so if $v_p(c_1) = 1$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(c) Reducing modulo p^2, we see that $p^2 \mid c_0$ is necessary to get a $\mathbb{Q}_p$ solution. This happens with probability $\frac{1}{p}$ and so we move to the next line.

(d) The justification is identical to θ_{7d}, producing

$$\theta_{9d} = \left(1 - \frac{1}{p}\right)\left(\eta'_{2,1} + \eta'_{2,2}\theta_2\right) + \frac{1}{p}\theta_{9e} = \left(1 - \frac{1}{p}\right)\left(\frac{p-1}{2p} + \frac{\theta_2}{p}\right) + \frac{1}{p}\theta_{9e}.$$

(e) Modulo p^3 we have $\frac{1}{p^2}(c_1 x + c_0)$, so if $v_p(c_1) = 2$, which happens with probability $1 - \frac{1}{p}$, then there is a solution that lifts to $\mathbb{Q}_p$.

(f) Reducing modulo p^3, we see that $p^3 \mid c_0$ is necessary to get a $\mathbb{Q}_p$ solution. This

happens with probability $\frac{1}{p}$. Before moving to the next line, we replace y by py and divide by p^3.

(g) The justification is identical to that of $\tau_{9\ell}$.

(h) The justification is identical to that of λ_d.

(i) With probability $1-\frac{1}{p}$ we have $v(c_1)=0$ and the reduced equation is $\overline{F}(x,y,1)=y^3-c_1x-c_0$, which is linear in x and thus has a solution with $y\in p\mathbb{Z}_p$. With probability $\frac{1}{p}$ we have $v(c_1)\geq 1$ and move to the next line.

(j) The reduced equation is now $\overline{F}=y^3-c_0$. The probability that c_0 is a nonzero cubic residue is $\Phi(p)$. If $p\nmid c_0$ is not a cubic residue, then no point lifts. With probability $\frac{1}{p}$ we have $v(c_0)=1$ and we move to the next line.

(k) If $v(c_4)=1$ we are in the situation of $\mu'=$ (4.8.6) from Lemma 4.5.14. This happens with probability $1-\frac{1}{p}$, so with probability $\frac{1}{p}$ we have $v(c_4)\geq 2$ and we move to the next line.

(ℓ) If $v(c_3)=1$, then we are in the situation of $\alpha'=$ (4.5.10) from Lemma 4.5.12. This happens with probability $1-\frac{1}{p}$, so with probability $\frac{1}{p}$ we have $v(c_3)\geq 2$ and we move to the next line.

(m) The justification is identical to τ_{9d} of Lemma 4.5.19, producing

$$\theta_{9m}=\left(1-\frac{1}{p}\right)\left(\eta'_{2,1}+\eta'_{2,2}\tau_2\right)+\frac{1}{p}\theta_{9n}=\left(1-\frac{1}{p}\right)\left(\frac{p-1}{2p}+\frac{1}{p^2}\right)+\frac{1}{p}\theta_{9n}.$$

(n) The justification is identical to that of line (b).

(o) The justification is identical to that of line (c).

(p) This is the definition of σ''_5.

The table above gives us a relation between θ_9 and σ''_5, while the definition of σ''_5 gives another:

$$\sigma''_5=\sum_{i=0}^{9}\eta'_{6,i}\theta_i.$$

Solving the two simultaneously give the values of $\theta_9 = (4.8.19)$ and $\sigma_5'' = (4.8.9)$. □

Completing the proofs of Proposition 4.5.18 and Theorem 4.1.5

To complete the proof of Proposition 4.5.18, we must compute σ_5. In doing so, we will also compute the exact value of ρ, thereby completing the proof of part of Theorem 4.1.5 as well.

Proof of Proposition 4.5.18. Recall that $\sigma_5' = (4.8.8)$ and $\sigma_5'' = (4.8.9)$ were computed in the proofs of Lemmas 4.5.19 and 4.5.21, respectively. Thus all that remains is to compute σ_5.

Recall that σ_5 is related to ρ by

$$\sigma_5 = \frac{1}{p^{14}}\rho + \left(1 - \frac{1}{p^7}\right)\sum_{i=0}^{9} \eta_{6,i}\tau_i + \left(\frac{p^7-1}{p^{14}}\right)\sum_{i=0}^{9}\eta_{6,i}\theta_i,$$

where the values of $\eta_{6_i}, \tau_i, \theta_i$ are given in Lemmas 4.5.6, 4.5.19, and 4.5.21, respectively. On the other hand, we have

$$\rho = \sum_{i=1}^{5} \xi_i \sigma_i,$$

with ξ_i given in Corollary 4.5.3 and σ_i for $1 \leq i \leq 4$ given in Propositions 4.5.7, 4.5.8, 4.5.9, 4.5.15, respectively. We can thus solve the two equations above for σ_5 and ρ as rational functions in p,

$$\rho = (4.8.1),$$
$$\sigma_5 = (4.8.5),$$

thereby completing the proof of Proposition 4.5.18. For an implementation in Sage [Sag21], see the GitHub repository associated to this paper [BK21b, `SEC_rho36_23Aug21.ipynb`].

Thus we have verified that for $i = 1, 2$, we have $\rho(p) = R_i(p)$ for an explicit rational function $R_i(t)$ and all sufficiently large primes $p \equiv i \pmod 3$ as stated in Theorem 4.1.5. It remains to observe the asymptotic behavior, i.e. that when $p \equiv 1 \pmod 3$, this explicit

function satisfies

$$1 - \rho(p) \sim \frac{2}{3}p^{-4},$$

and if $p \equiv 2 \pmod 3$ then

$$1 - \rho(p) \sim \frac{53}{144}p^{-7}.$$

□

4.5.6 Small primes

All that remains to prove Theorem 4.1.5 is to compute $\rho(p)$ for the remaining eight primes p, not handled directly by Propositions 4.5.7, 4.5.8, 4.5.9, 4.5.15, and 4.5.18, namely $p = 2, 3, 7, 13, 19, 31, 37, 43$. We handle the cases of $p = 2$ and $p = 3$ separately from the six remaining primes $p \equiv 1 \pmod 3$ and conclude this section with the the exact calculation of $\rho_{3,6} \approx 96.94\%$.

The case of $p = 2$

Suppose $p = 2$. By the proof of Proposition 4.3.4, for all binary sextic forms $f(x, z)$ such that $\overline{f} \neq 0, x^2(x+z)^2z^2$, we can lift a point on the reduction $\overline{C_f}$ to a $\mathbb{Q}_2$-point of C_f. Thus we first restrict our attention to lifting $\mathbb{F}_2$-points of

$$y^3 = x^2(x+z)^2z^2.$$

By the same argument as that for θ_4 in the proof of Lemma 4.5.21, the probability of $[0:0:1]$, $[1:0:1]$, or $[1:0:0]$ lifting to a $\mathbb{Q}_2$-point are equal and independent. Thus it suffices to determine how often $[0:0:1]$ lifts. In fact, we will need the following lemma for all primes $p \neq 3$.

Lemma 4.5.22. *Let $p \neq 3$ be a prime. Fix c_2 such that $v(c_2) = 0$ and $c_3, c_4, c_5, c_6 \in \mathbb{Z}_p$. As c_0, c_1 range over $p\mathbb{Z}_p$, let ν denote the probability that the $\mathbb{F}_p$-solution $[0:0:1]$ to*

$\overline{F}(x,y,z) = 0$ *lifts to a* $\mathbb{Q}_p$*-solution to* $F(x,y,z) = 0$*. We have*

$$\nu = \frac{1}{p}\left(\eta'_{2,1} + \eta'_{2,2}\theta_2\right) = \begin{cases} \frac{3p^4-p^3+p^2-3p+6}{6p^5} & p \equiv 1 \pmod 3, \\ \frac{p^4+p^3-p^2-p+2}{2p^5} & p \equiv 2 \pmod 3. \end{cases}$$

Proof. Let $[x : y : z] \equiv [0 : 0 : 1] \pmod p$. We observe that $v(c_2x^2z^4 + c_1xz^5) \geq 2$, so if $v(c_0) = 1$, the equation is seen to be insoluble modulo p^2. With probability $\frac{1}{p}$ we have $c_0 \in p^2\mathbb{Z}_p$.

Replacing x by px, our equation becomes

$$y^3 = \sum_{i=0}^{6} p^i c_i x^i.$$

Rewriting c_i as $p^i c_i$, we have the valuations (in descending order) are given by

$$\geq 6 \ \geq 5 \ \geq 4 \ \geq 3 \ = 2 \ \geq 2 \ \geq 2.$$

Thus it is necessary for $p^3 \mid (c_2x^2 + c_1x + c_0)$, so with probability $\eta'_{2,0} = \frac{p-1}{2p}$, the equation is insoluble. With probability $\eta'_{2,1} = \frac{p-1}{2p}$, we have a lift, and with probability $\eta'_{2,2} = \frac{1}{p}$, we are in the situation of θ_2 of Lemma 4.5.21, and the proof is seen to be valid for all p. Putting this together yields the giving probability that $[0 : 0 : 1]$ lifts to a $\mathbb{Q}_p$-solution. □

Corollary 4.5.23. *Let* $f(x,z)$ *be a binary sextic form with* $\overline{f}(x,z) = x^2(x+z)^2z^2 \pmod 2$*. The probability that* C_f *has a* $\mathbb{Q}_2$*-point is*

$$1 - (1-\nu)^3 = \frac{2675}{4096}.$$

The probability that C_f *has an affine* $\mathbb{Q}_2$*-point of the form* $[x : y : 1]$ *is*

$$1 - (1-\nu)^2 = \frac{135}{256}.$$

Proof. The two statements follow from applying Lemma 4.5.22 to the two affine and three

total $\mathbb{F}_2$-points of $\overline{C_f}$ independently (see the argument for θ_4 in the proof of Lemma 4.5.21).

□

At this point, we have

$$\rho_{3,6}(2) = 1 - \frac{1}{2^6} + \frac{1}{2^7}\left(\frac{2675}{4096} + \sigma_5\right), \tag{4.5.16}$$

where σ_5 is the probability of solubility when $\overline{f}(x, z) = 0$.

To compute σ_5, we can follow the proofs of Proposition 4.5.18. For $0 \leq i \leq 6$, the values of τ_i and θ_i from Lemmas 4.5.19 and 4.5.21 hold for $p = 2$. Corollary 4.5.23 can be used to compute θ_7, μ, τ_7, and μ', in that order. We catalog these values below and highlight the modified steps.

$$\begin{aligned}
\theta_7 &= \frac{13575}{16384} && \left(\text{use } \theta_{7g} = \frac{135}{256}\right), \\
\theta_8 &= \frac{62727}{65536} && (\text{use updated } \theta_7), \\
\mu &= \frac{90887}{131072} && (\text{use updated } \theta_7 \text{ in (4.5.13)}), \\
\tau_7 &= \frac{3760903}{8388608} && (\text{use } \tau_{7g} = \mu), \\
\tau_8 &= \frac{12149511}{16777216} && (\text{use updated } \tau_8), \\
\mu' &= \frac{40461063}{67108864} && (\text{use updated } \tau_7 \text{ in (4.5.14)}).
\end{aligned}$$

We then solve the following equations, using the values above and Corollary 4.5.23

appropriately in the calculation of τ_9,

$$\begin{aligned}
\tau_9 &= \frac{1}{32768}\sigma_5' + \frac{7283817}{16252928} && \left(\text{use } \tau_{9k} = \frac{1}{2}\cdot\frac{136}{256} + \frac{1}{2}\tau_{9\ell}\right),\\
\sigma_5' &= \sum_{i=0}^{9} \eta_{6,i}'\tau_i && (\text{use updated } \tau_7, \tau_8),\\
\theta_9 &= \frac{1}{32768}\sigma_5'' + \frac{3559852801497}{4260607557632} && \left(\text{use updated } \mu' \text{ in } \theta_{9k}\right),\\
\sigma_5'' &= \sum_{i=0}^{9} \eta_{6,i}'\theta_i && (\text{use updated } \theta_7, \theta_8),\\
\sigma_5 &= \frac{1}{2^{14}}\rho + \left(1 - \frac{1}{2^7}\right)\sum_{i=0}^{9}\eta_{6,i}\tau_i + \left(\frac{2^7-1}{2^{14}}\right)\sum_{i=0}^{9}\eta_{6,i}\theta_i,\\
\rho &= 1 - \frac{1}{2^6} + \frac{1}{2^7}\left(\frac{2675}{4096} + \sigma_5\right) && (\text{see (4.5.16)}).
\end{aligned}$$

This yields

$$\rho_{3,6}(2) = \frac{45948977725819217081}{46164832540903014400} \approx 0.99532, \tag{4.5.17}$$

a considerable improvement over $1 - \frac{1}{2^6}$.

The case of small primes $p \equiv 1 \pmod 3$

Suppose p is one of $p = 7, 13, 19, 31, 37, 43$. Here we are not able to conclude that when $\overline{F}(x, y, z)$ is absolutely irreducible, that C_f has a $\mathbb{Q}_p$-point, i.e. that $\sigma_1 = 1$. At various other junctures, including the calculations of τ_i and θ_i in Lemmas 4.5.19 and 4.5.21, we use assumptions about the size of p to conclude that certain equations over $\mathbb{F}_p$ always possess a liftable point. To circumvent this and fix the necessary calculations, we need a few intermediate results.

Consider equations of the form

$$y^3 = c_3x^3 + c_2x^2 + c_1x + c_0 \tag{4.5.18}$$

and denote by $\rho_{3,3}^{\text{aff}}(p)$ the probability that (4.5.18) has an affine $\mathbb{Q}_p$-point as c_0, c_1, c_2, c_3 vary in $\mathbb{Z}_p$ with $v(c_3) = 0$.

Lemma 4.5.24. *Let $p \equiv 1 \pmod 3$. When $p > 7$ we have*

$$\rho_{3,3}^{\mathrm{aff}}(p) = \frac{1}{3} + \frac{2}{3}\beta = \frac{3p^4 + 3p^3 + p^2 + 3p + 1}{3(p^4 + p^3 + p^2 + p + 1)}.$$

In the case of $p = 7$,

$$\rho_{3,3}^{\mathrm{aff}}(7) = \frac{1}{2058}\left(2002 + 28\alpha\right) = \frac{401245}{411747}.$$

Proof. Note that the justification when $p > 7$ is essentially that of $\tau_{9\ell}$ or θ_{9g}. Whenever $c_3 \in \left(\mathbb{F}_p^\times\right)^3$ we have a solution, as the Hasse bound (4.3.2) applies to the normalization of the reduction of (4.5.18) whenever $p > 7$, and if the right hand side factors as $c_3(x-a)^3$, we can lift $[a+1 : y : 1]$ using Hensel's lemma. If $c_3 \notin \left(\mathbb{F}_p^\times\right)^3$, then we are in the situation of β, giving the first statement.

When $p = 7$, a computer search shows that of the 2058 equations (4.5.18) over $\mathbb{F}_7$ with $v(c_3) = 0$, 2002 can be lifted via Hensel's lemma, 28 are insoluble, and 28 are of the form $y^3 = c_3(x-a)^3$, where $c_3 \notin \left(\mathbb{F}_p^\times\right)^3$. See the procedure `count_cubic_forms(p)`, contained in the file `CountForms.m`, found in the GitHub repository associated to this paper [BK21b], for an implementation in Magma [BCP97]. The probability of lifting in this case is given by α, proving the second statement. □

The following lemma complements Lemma 4.5.22, in that it provides the probability that a triple root modulo p lifts to a $\mathbb{Q}_p$-point.

Lemma 4.5.25. *Let $p \equiv 1 \pmod 3$ and fix $c_4, c_5, c_6 \in \mathbb{Z}_p$. As c_0, c_1, c_2, c_3 vary in $\mathbb{Z}_p$ with $v(c_3) = 0$, the $\mathbb{F}_p$-solution $[0:0:1]$ to $\overline{F}(x,y,z) = 0$ lifts to a $\mathbb{Q}_p$-solution to $F(x,y,z) = 0$ with probability*

$$\pi = \frac{1}{p} - \frac{1}{p^2} + \frac{1}{p^3}\rho_{3,3}^{\mathrm{aff}} = \begin{cases} \frac{17694619}{141229221} & p = 7, \\ \frac{3p^6+3p^4+3p^3+p^2+1}{3(p^4+p^3+p^2+p+1)p^3} & p > 7. \end{cases}$$

Proof. The proof follows techniques similar to ones we have already seen.

$$\begin{array}{rll|ccccccc} & & & c_6 & c_5 & c_4 & c_3 & c_2 & c_1 & c_0 \\ \pi = & \pi_a = \frac{1}{p}\pi_b & & \geq 0 & \geq 0 & \geq 0 & = 0 & \geq 1 & \geq 1 & \geq 1 \\ & \pi_b = \left(1 - \frac{1}{p}\right) + \frac{1}{p}\pi_c & & \geq 6 & \geq 5 & \geq 4 & = 3 & \geq 3 & \geq 2 & \geq 2 \\ & \pi_c = \frac{1}{p}\pi_d & & \geq 6 & \geq 5 & \geq 4 & = 3 & \geq 3 & \geq 3 & \geq 2 \\ & \pi_d = \rho_{3,3}^{\mathrm{aff}} & & \geq 3 & \geq 2 & \geq 1 & = 0 & \geq 0 & \geq 0 & \geq 0 \end{array}$$

(a) We observe that $v(c_3x^3+c_2x^2+c_1x) \geq 2$, so it is necessary for $v(c_0) \geq 2$, which occurs with probability $\frac{1}{p}$. At this point, we replace x by px and c_i by $p^i c_i$ and move to the next line.

(b) The justification is identical to that of θ_{9e}.

(c) The justification is identical to that of θ_{9f}.

(d) The probability of finding a solution of the form $[x : y : 1]$ is precisely $\rho_{3,3}^{\mathrm{aff}}(p)$ by definition.

Putting these steps together, along with the value of $\rho_{3,3}^{\mathrm{aff}}$ from Lemma 4.5.24 yields the given formula. □

Consider now equations of the form

$$y^3 = c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \tag{4.5.19}$$

with $v(c_3) = 0$. Let the proportion of equations (4.5.19) over $\mathbb{Z}_p$ possessing an affine $\mathbb{Q}_p$-point be denoted $\rho_{3,4}^{\mathrm{aff}}(p)$. This quantity came up in computing θ_7 and τ_9, (see in particular θ_{7g}, τ_{9k}), and hence also the quantities derived from them, including $\mu, \mu', \tau_7, \tau_8, \theta_8$, and θ_9. When $p > 31$, an application of the Hasse–Weil bound (4.3.2) is sufficient to guarantee the existence of a $\mathbb{Q}_p$-point; for $p \leq 31$, we have the following.

Lemma 4.5.26. *Let $p \equiv 1 \pmod 3$. For $p \geq 31$ we have $\rho_{3,4}^{\mathrm{aff}} = 1$. For $p < 31$, we have*

$$\begin{aligned}
\rho_{3,4}^{\mathrm{aff}}(7) &= \frac{93877018682}{96889010407} \approx 0.96891, \\
\rho_{3,4}^{\mathrm{aff}}(13) &= \frac{813159544}{815730721} \approx 0.99684, \\
\rho_{3,4}^{\mathrm{aff}}(19) &= \frac{6856}{6859} \approx 0.99956.
\end{aligned}$$

Proof. For $p > 31$ this is a consequence of the Hasse–Weil bound (4.3.2). For the four primes $p \leq 31$, the proof proceeds by enumeration of all binary quartic forms $f(x, z)$ over $\mathbb{F}_p$ with $c_4 \not\equiv 0 \pmod p$. If for any $[x : 1]$ we have $f(x, 1) \in \left(\mathbb{F}_p^\times\right)^3$ or $f(x, 1) = 0$ is a root of multiplicity 1, then Hensel's lemma allows us to lift to a $\mathbb{Q}_p$-point. Of course, if $y^3 = f(x, z)$ is insoluble modulo p, then there exist no $\mathbb{Q}_p$-points.

The only other possibility is that $f(x, z)$ has one or two double roots. In either case, the probability that such a root lifts to a $\mathbb{Q}_p$-point is ν, by Lemma 4.5.22. By enumerating all such $f(x, z)$ and determining their value sets and factorizations, we computed $\rho_{3,4}^{\mathrm{aff}}(p)$ as listed above, finding in particular that $\rho_{3,4}^{\mathrm{aff}}(31) = 1$.

This enumeration procedure was implemented in Magma [BCP97]. The relevant procedure, `count_quartic_forms(p)`, is contained in the file `CountForms.m` and can be found in the GitHub repository associated to this paper [BK21b]. □

With a similar approach as that of Lemmas 4.5.24 and 4.5.26, we can determine σ_1 and σ_1^* exactly for $p = 7, 13, 19, 31, 37, 43$.

Proposition 4.5.27. *For the primes $p \equiv 1 \pmod 3$ with $p \leq 43$, the values of σ_1 and σ_1^* are given below.*

$$\begin{aligned}
\sigma_1(7) &= \frac{577619497568784534247}{586438262710350126300} \approx 0.98496 & \sigma_1^*(7) &= \frac{653206973052553734217}{670215157383257287200} \approx 0.97462 \\
\sigma_1(13) &= \frac{5931415654903952}{5941011706232655} \approx 0.99838 & \sigma_1^*(13) &= \frac{455813699762383}{457000900479435} \approx 0.99740 \\
\sigma_1(19) &= \frac{1294027438921}{1294326278072} \approx 0.99976 & \sigma_1^*(19) &= \frac{43009044017}{43024696224} \approx 0.99963 \\
\sigma_1(31) &= \frac{3697903}{3697928} \approx 0.999993 & \sigma_1^*(31) &= \frac{477147}{477152} \approx 0.999989 \\
\sigma_1(37) &= \frac{937764}{937765} \approx 0.999998 & \sigma_1^*(37) &= \frac{608279}{608280} \approx 0.999998 \\
\sigma_1(43) &= \frac{41047793}{41047800} \approx 0.9999998 & \sigma_1^*(43) &= \frac{3818399}{3818400} \approx 0.9999997
\end{aligned}$$

Proof. We proceed by enumerating binary sextic forms $f(x,z)$ and checking for liftable points in Magma [BCP97]; see §4.6 for a description, including optimizations necessary to shorten the runtime of these calculations, and [BK21b] for the code.

Let $\overline{f}(x,z)$ be a binary sextic form over $\mathbb{F}_p$ which is not equal to $h(x,z)^3$ for any binary quadratic form $h(x,z)$ (resp. also satisfying condition $(*)$). If $\overline{f}(x,z) \in \left(\mathbb{F}_p^\times\right)^3$ or $\overline{f}(x,z) = 0$ is a root of multiplicity 1, then by Hensel's lemma it lifts to a $\mathbb{Q}_p$-point of C_f.

If no such $[x:z]$ exist, then the equation is either insoluble, in which case $C_f(\mathbb{Q}_p) = \emptyset$, or the only $\mathbb{F}_p$-points come from multiple roots of $\overline{f}(x,z)$. These could be up to three double roots, or a triple root (note that two triple roots or a sextic root are ruled out by being in factorization case 1). By Lemma 4.5.22, each double root lifts (independently, by the same arguments as those for θ_4 in the proof of Lemma 4.5.21) to a $\mathbb{Q}_p$-point with probability ν, while a triple root lifts with probability π by Lemma 4.5.25.

Summing up the number of forms and weighting by the appropriate probability yields the given values of σ_1 (resp. σ_1^*). See (4.6.1) for the case of $p = 13$ as an example. □

At this point, we can repeat the calculations of §4.5.4, 4.5.5 — namely those of σ_4 and σ_5 — using the modifications above as appropriate. These modifications are described below; for the full implementation, see [BK21b, `SEC_rho36_23Aug21.ipynb`].

- $\theta_{7g} = \rho_{3,4}^{\mathrm{aff}}$ in the proof of Lemma 4.5.21. This is used to compute θ_7, which is then used to compute μ, τ_7, and μ' in succession, and these values are used throughout.

- In the proof of Proposition 4.5.15, the correct σ_1^* value from Proposition 4.5.27 must be used in (4.5.4).

- In the calculation of τ_9 in Lemma 4.5.19, we use

$$\tau_{9k} = \left(1 - \frac{1}{p}\right)\rho_{3,4}^{\mathrm{aff}}(p) + \frac{1}{p}\tau_{9\ell} \quad \text{and}$$
$$\tau_{9\ell} = \left(1 - \frac{1}{p}\right)\rho_{3,3}^{\mathrm{aff}}(p) + \frac{1}{p}\tau_{9m},$$

  where $\rho_{3,3}^{\mathrm{aff}}(p)$ and $\rho_{3,4}^{\mathrm{aff}}(p)$ are given in Lemmas 4.5.24 and 4.5.26, respectively.

- In the calculation of θ_9 in Lemma 4.5.21, we use

$$\theta_{9g} = \left(1 - \frac{1}{p}\right) \rho_{3,3}^{\text{aff}}(p) + \frac{1}{p}\theta_{9h}.$$

- In the final calculation of ρ, we use the correct σ_1 value from Proposition 4.5.27 in (4.5.3).

The exact values of $\rho_{3,6}(p)$ are recorded in (4.8.20) – (4.8.25).

The case of $p = 3$

Suppose now that $p = 3$. This case breaks from the others in that when $f(x, z) \not\equiv 0 \pmod 3$, one cannot determine whether there exists a $\mathbb{Q}_3$-solution to $y^3 = f(x, z)$ from information modulo p alone. Instead, one needs to know information modulo $3^3 = 27$.

In $\mathbb{Z}/27\mathbb{Z}$, the nonzero cubic residue classes are precisely

$$\left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3 = \{1, 8, 10, 17, 19, 26\}.$$

For $a \in \mathbb{Z}_3$ with $v(a) = 0$, there exists $y \in \mathbb{Z}_3$ satisfying $y^3 = a$ if and only if $a \in (\mathbb{Z}/27\mathbb{Z}^\times)^3$. This is seen by applying Hensel's lemma, in the form of (4.3.1), with respect to y. Note also that for any $a \in \mathbb{Z}_3$, we have that its residue $a \in (\mathbb{Z}/27\mathbb{Z}^\times)^3$ if and only if $a+9 \in (\mathbb{Z}/27\mathbb{Z}^\times)^3$; this will be used later.

Our approach mirrors that of the other primes p in this section; we first establish some technical results, then use them to adapt our general strategy to work for $p = 3$, yielding a value for $\rho_{3,6}(3)$. We begin with the following lemma, which effectively takes the place of Φ in the proofs of various lifting results.

Lemma 4.5.28. *Consider the probability of $F(x, y, 1) = 0$ having a $\mathbb{Q}_3$-solution under the following conditions.*

(a) Fix $c_3, c_4, c_5, c_6 \in 3\mathbb{Z}_3$ and vary $c_0 \in \mathbb{Z}_3 - 3\mathbb{Z}_3$ and $c_1, c_2 \in 3\mathbb{Z}_3$. The probability that $F(x, y, 1) = 0$ has a $\mathbb{Q}_3$-solution is $\frac{19}{27}$.

(b) *Fix* $c_3, c_4, c_5, c_6 \in 9\mathbb{Z}_3$ *and vary* $c_0 \in \mathbb{Z}_3 - 3\mathbb{Z}_3$, $c_1 \in 3\mathbb{Z}_3$, *and* $c_2 \in 3\mathbb{Z}_3 - 9\mathbb{Z}_3$. *The probability that* $F(x, y, 1) = 0$ *has a* $\mathbb{Q}_3$*-solution is* $\frac{2}{3}$.

(c) *Fix* $c_2, c_3, c_4, c_5, c_6 \in 9\mathbb{Z}_3$ *and vary* $c_0 \in \mathbb{Z}_3 - 3\mathbb{Z}_3$ *and* $c_1 \in 3\mathbb{Z}_3$. *The probability that* $F(x, y, 1) = 0$ *has a* $\mathbb{Q}_3$*-solution is* $\frac{7}{9}$.

Proof. The restrictions on the c_i guarantee that for any $(x, y) \in \mathbb{Z}_3^2$, we have $v\left(F(x, y, 1)\right) = 0$. Thus it suffices to work modulo $3^3 = 27$ and determine if $f(x, 1)$ takes a value in $\left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$. By our earlier observation that nonzero cubic residues modulo 27 are invariant under addition by multiples of 9, we have that $f(x, 1) \in \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$ if and only if $f(x+3, 1) \in \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$, and hence it suffices to check at

$$\begin{aligned} f(0, 1) &= c_0, \\ f(1, 1) &= \sum_{i=0}^{6} c_i, \text{and} \\ f(-1, 1) &= \sum_{i=0}^{6} (-1)^i c_i. \end{aligned}$$

We have that $c_0 \in \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$ with probability $\frac{1}{3}$. If not, then we may check at the other values.

Consider first (a). If c_0 is not in $\left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$ then let $c \equiv c_0 + c_3 + c_4 + c_5 + c_6 \pmod{27}$. Exactly one of c, $c + 3$, and $c - 3$ are in $\left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$, and as c_1, c_2 varying in $3\mathbb{Z}_3$, we have that $c_1 + c_2 \equiv 0, 3, -3 \pmod 9$ each with equal probability of $1/3$. If $\sum c_i \notin \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$, then we verify by direct enumeration that the probability of $-c_1 + c_2$ satisfying $\sum (-1)^i c_i \in \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$ is also $1/3$. Hence we have the probability in (a) is given by

$$\frac{1}{3} + \frac{2}{3}\left(\frac{1}{3} + \frac{2}{3}\left(\frac{1}{3}\right)\right) = \frac{19}{27}.$$

For (b) and (c), we are in a similar situation, except we can ignore $c_3, \ldots, c_6$ entirely as their values will not affect whether $f(x, 1)$ takes a value in $\left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$. To compute (b), we note that if c_0 is not in $\left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$, then $c_0 + c_2$ is with probability $\frac{1}{2}$, since $9 \nmid c_2$. If this is the case, there is a $\frac{1}{3}$ chance that $9 \mid c_1$ and we have $f(1, 1) \in \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$. If $c_0 + c_2 \notin \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$, then there is a $\frac{2}{3}$ chance that one of $f(\pm 1, 1) \in \left(\mathbb{Z}/27\mathbb{Z}^\times\right)^3$. This

comes out to the probability

$$\frac{1}{3} + \frac{2}{3}\left(\frac{1}{2}\right) = \frac{2}{3}.$$

For (c) we follow a similar approach, observing that if c_0 is not in $(\mathbb{Z}/27\mathbb{Z}^\times)^3$, we have a $\frac{2}{3}$ chance that one of $c_0 \pm c_1$ is, as only when $9 \mid c_1$ is the sum not a cube modulo 27. Thus we obtain

$$\frac{1}{3} + \frac{2}{3}\left(\frac{2}{3}\right) = \frac{7}{9}.$$

□

We now compute the probability of lifting a point $[x : 0 : z]$ on $y^3 = f(x, z)$ when $f(x, z)$ has a double root modulo 3; after a change of coordinates, we may consider the point $[0 : 0 : 1]$. We call this probability ν as in Lemma 4.5.22.

Lemma 4.5.29. *Fix $c_2, c_3, c_4, c_5, c_6 \in \mathbb{Z}_3$ and suppose $v(c_2) = 0$. As c_0, c_1 vary in $3\mathbb{Z}_3$, the $\mathbb{F}_3$-solution $[0 : 0 : 1]$ to $\overline{F}(x, y, z) = 0$ lifts to a $\mathbb{Q}_3$-solution to $F(x, y, z) = 0$ with probability*

$$\nu = \frac{43}{243}.$$

Proof. Following the proof of Lemma 4.5.22, we have

$$\nu = \frac{1}{p}\left(\eta'_{2,1} + \eta'_{2,2}\theta_2\right).$$

To compute θ_2, we follow the proof of Lemma 4.5.21, except that in the first step we take

$$\theta_{2a} = \frac{2}{3} \cdot \left(\frac{2}{3}\right) + \frac{1}{3}\theta_{2b},$$

justifying as follows. With probability $\frac{2}{3}$ we have $v(c_0) = 0$, putting us in the case of Lemma 4.5.28(c), in which case a lift exists with probability $\frac{2}{3}$, giving the left-hand term. With probability $\frac{1}{3}$ we have $3 \mid c_0$, and we continue with the computation of θ_2 as in the proof of Lemma 4.5.21.

Note that in the last step, we may take $\theta_{2d} = 1$ as usual, since the partial derivative of the quadratic $c_2x^2 + c_1x + c_0$ can only vanish modulo 3 for at most one value of x. Hence

one of the other x values may always be used to lift to a $\mathbb{Q}_3$-solution. This results in

$$\theta_2 = \frac{16}{27} \qquad \text{and} \qquad \nu = \frac{43}{243}.$$

□

Next, we consider σ_1. The values of $\rho_{3,3}^{\text{aff}}$ and $\rho_{3,4}^{\text{aff}}$ will follow from similar reasoning. Of the 2160 (see Lemma 4.5.2) binary sextic forms $\overline{f}(x,z)$ modulo 3 with $\overline{F}$ absolutely irreducible, all but 54 have at least one $[x:z]$ such that the partial derivative of $\overline{F}$ with respect to x (or z) is nonvanishing modulo 3, and hence liftable via Hensel's lemma (see Proposition 4.3.9). The remaining 54 may be enumerated and are seen to have the factorization types as follows:

- 24 have one double root (i.e. $\overline{f}(x,z)$ has factorization type $1^2 4$ or $1^2 22$) modulo 3,
- 12 have two double roots (i.e. $\overline{f}$ has type $1^2 1^2 2$) modulo 3,
- 8 have three double roots (i.e. $\overline{f}$ has type $1^2 1^2 1^2$) modulo 3, and
- 10 have no roots modulo 3.

This leads to our determination of σ_1, as well as $\rho_{3,3}^{\text{aff}}$ and $\rho_{3,4}^{\text{aff}}$.

Proposition 4.5.30. *When $p = 3$, we have*

$$\begin{aligned}
\sigma_1 &= \frac{5780143846}{5811307335} \approx 0.99463, \\
\rho_{3,3}^{\text{aff}} &= \frac{2103}{2183} \approx 0.96335, \\
\rho_{3,4}^{\text{aff}} &= \frac{4585681}{4782969} \approx 0.95875.
\end{aligned}$$

Proof. To compute σ_1, we need only determine the probability of lifting for each of the four values $[x:z]$, and see that they are independent of one another. When $f(x,z) \neq 0 \pmod 3$, the probability of lifting is $\frac{1}{3}$, exactly the proportion of residues in $(\mathbb{Z}/27\mathbb{Z})^\times$ in the image of the cube map. The probability of a double root modulo p lifting is ν, as after a change of coordinates we may assume $[x:z] = [0:1]$, putting us in the case of Lemma 4.5.29.

For the independence, we treat each of the four cases separately, illustrating the argument in the case that $\overline{f}(x,z)$ has exactly one double root modulo 3, occurring at $[0:1]$. By Lemma 4.5.29 the probability of lifting is ν, and since this proof relies on Lemma 4.5.28(c), the lifting behavior depends only on the values of c_0 and c_1. The lifting behavior at $[x:z] = [1:1], [-1:1], [1:0]$, for which $f(x,z) \not\equiv 0 \pmod 3$, does not depend on the choice of lift of $[x:z]$ to $\mathbb{Z}/27\mathbb{Z}$ by our earlier discussions. Hence this depends only on, say, c_3, c_4, and c_6.

Since lifting a double root depends only on $f(x,z)$ and $f'(x,z)$ modulo 27, lifting a nonzero value depends only on the value itself in this case, and we have 7 coefficients varying, the argument above easily extends to the other three cases. This justifies

$$\sigma_1 = \frac{1}{2160}\left(2106 + 10\left(1-\left(\frac{2}{3}\right)^4\right) + 24\nu\left(1-\left(\frac{2}{3}\right)^3\right)\right.$$
$$\left. + 12\left(1-(1-\nu)^2\right)\left(1-\left(\frac{2}{3}\right)^2\right) + 8\left(1-(1-\nu)^3\right)\left(\frac{1}{3}\right)\right).$$

For $\rho_{3,4}^{\mathrm{aff}}$, the story is similar, except we are only interested in lifting affine solutions $[x:1]$. Of the 162 quartics $c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$ modulo 3, all but 18 have nonzero partial derivative, with the cases of no (affine) roots, one (affine) double root, and two (affine) double roots each appearing 6 times. The same lifting probabilities and independence arguments above apply, yielding the stated value.

Finally, to compute $\rho_{3,3}^{\mathrm{aff}}$, we note that so long as c_1, c_2 are not both in $3\mathbb{Z}_3$, the partial derivative does not vanish and we have a root by Hensel's lemma. If $3 \mid c_1, c_2$, then $\overline{f}(x,z) = c_3x^3z^3 + c_0z^6$, and after a change of variables over $\mathbb{F}_3$, we may assume $\overline{f}(x,z) = x^3z^3$.

Let $f(x,z) \in \mathbb{Z}_3[x,z]$ be a binary sextic form reducing to $\overline{f} = x^3z^3$. Using the same techniques as in the proof of Lemma 4.5.28, we have that the probability that $[\pm 1:1]$ has a lift to a $\mathbb{Q}_3$-point is $\frac{1}{3}$ for each. Note that this can be made independent of the choices of c_4, c_5 and c_6, which is necessary to use in our calculations of θ_{9g} and $\tau_{9\ell}$. If neither of these lift, the probability that $[0:1]$ is computed by first replacing x by $3x$, giving the valuations on c_3, c_2, c_1, c_0

$$\cdots \ = 3 \ \geq 3 \ \geq 2 \ \geq 1.$$

We compute that we have a lift with probability $\frac{2}{9} + \frac{1}{27}\rho_{3,3}^{\text{aff}}$, yielding that

$$\rho_{3,3}^{\text{aff}} = \frac{8}{9} + \frac{1}{9}\left(\frac{5}{9} + \frac{4}{9}\left(\frac{2}{9} + \frac{1}{27}\rho_{3,3}^{\text{aff}}\right)\right),$$

and solving for $\rho_{3,3}^{\text{aff}}$ gives the stated value. □

Taken together, we once again repeat the calculations of §4.5.5 to obtain σ_5 and ρ, using the same modifications we did previously with the primes $p \equiv 1 \pmod 3$ up to $p = 43$. We also must replace Φ by the appropriate probability in Lemma 4.5.28 wherever necessary in the proofs of Lemmas 4.5.19 and 4.5.21. Finally solving

$$\rho_{3,6}(3) = \frac{2160}{2187}\sigma_1 + \frac{1}{27}\sigma_5$$

yields

$$\rho_{3,6}(3) = \frac{900175334869743731875930997281}{908381960435133191895132960000} \approx 0.99096. \tag{4.5.20}$$

Once again, the implementation may be found in [BK21b, `SEC_rho36_23Aug21.ipynb`].

Calculating $\rho_{3,6}$ exactly

We are now ready to complete the proof of Theorem 4.1.5.

Proof of Theorem 4.1.5. We have already seen that $\rho(p) = R_i(p)$ for sufficiently large $p \equiv i \pmod 3$; see §4.5.5. For the remaining primes, $p = 2, 3, 7, 13, 19, 31, 37, 43$, we have computed $\rho(p)$ in the preceding sections; see (4.5.17), (4.8.20) – (4.8.25), and (4.5.20). This yields the exact expression

$$\rho_{3,6} = \prod_{p=2,3,7,13,19,31,37,43} \rho(p) \prod_{\substack{p\equiv 1 \pmod 3 \\ p>43}} R_1(p) \prod_{\substack{p\equiv 2 \pmod 3 \\ p>2}} R_2(p).$$

To obtain a numerical value, we compute the product of $\rho(p)$ for all $p \leq 10000$, finding

$\prod_{p\leq 10000}\rho(p)\approx 0.96943$. Using the estimates $R_1(t)\geq 1-t^{-4}$ and $R_2(t)\geq 1-t^{-7}$, we find

$$1\geq \prod_{\substack{p\equiv 1 \pmod 3\\ p>10000}} R_1(p) \prod_{\substack{p\equiv 2 \pmod 3\\ p>10000}} R_2(p)\geq 1-1.6856\cdot 10^{-14},$$

which more than suffices to conclude our numerical value is correct to several decimal places. Once again, these calculations are recorded in the GitHub repository associated to this paper [BK21b, `SEC_rho36_23Aug21.ipynb`]. □

4.6 Bounds for $\rho_{m,d}(p)$ via computer search

The lower bounds for $\rho_{3,6}$ and $\rho_{5,5}$ produced by Corollary 4.3.10, discussed in Examples 4.3.15 and 4.3.16, were limited by the performance of Proposition 4.3.6 for primes $p\equiv 1 \pmod m$ such that $p<4g^2$. As noted in Remarks 4.3.7 and 4.3.8, the proof of Proposition 4.3.6 likely leaves out many liftable points, including those given by roots of $f(x,z)$ of multiplicity 1. Here we discuss how to use a computer search to improve our lower bounds of $\rho_{m,d}(p)$, an implementation in the case of $\rho_{3,6}(13)$, and how this approach is used in the exact determination of $\sigma_1(p)$ for small primes p in §4.5.6. The relevant code may be found in the GitHub repository associated to this paper [BK21b], available at the link below:

`https://github.com/c-keyes/Density-of-locally-soluble-SECs`.

Suppose $p\nmid m$. Using a computer algebra system it is straightforward to enumerate all binary degree d forms $\overline{f}(x,z)$ over $\mathbb{F}_p$ and for each such f, determine whether

- there exists a root $\overline{f}(x_0,z_0)=0$ of multiplicity 1, or
- there exists $[x_0:z_0]$ such that $\overline{f}(x_0,z_0)\in\left(\mathbb{F}_p^\times\right)^m$.

In either case, for any $f(x,z)\in\mathbb{Z}_p[x,z]$ such that $f\equiv\overline{f} \pmod p$, Hensel's lemma (Theorem 4.3.1) ensures $C_f(\mathbb{Q}_p)\neq\emptyset$.

Naïvely, this amounts to enumerating p^{d+1} polynomials, which quickly becomes prohibitively time consuming. To mitigate this, we first recognize that C_f has a smooth point if and only if $C_{u^m f}$ does for $u\in\mathbb{F}_p^\times$. This corresponds to the change of variables $y\mapsto\frac{y}{u}$.

Thus we may assume that the leading coefficient, c_d, of $f(x,z)$ is either 0 or equal to one of the representatives of the three cosets in $\mathbb{F}_p^\times/\left(\mathbb{F}_p^\times\right)^m$. This cuts down the running time by about a factor of p, as we need only enumerate the coefficients $c_0,\dots,c_{d-1}$.

To further improve the running time by a factor of p, we ran these searches for fixed values of the constant term c_0 in parallel. To avoid having to run p such programs, which again becomes cumbersome for large p, we observe that for a generator $a\in\mathbb{F}_p^\times$, the change of variables $z\mapsto az$ transforms the constant term by a factor of a^d, without affecting the leading term. Thus we may assume c_0 to be either 0 or equal to one of the representatives of the $\gcd(d,p-1)$ cosets in $\mathbb{F}_p^\times/\left(\mathbb{F}_p^\times\right)^d$. In particular, $\gcd(d,p-1)$ is bounded by d, so the number of parallel computations needed is bounded as p grows.

We implemented the strategy above in Magma [BCP97] for $(m,d)=(3,6)$ to obtain better bounds for $\rho_{3,6}(p)$ for the seven primes p such that $p\equiv 1 \pmod 3$ and $p\le 61$. The relevant file is [BK21b, `CountForms.m`]; namely, the procedure `count_sextic_forms`(p,c_0) counts binary sextic forms $\overline{f}(x,z)$ which, after the aforementioned changes of variables, have specified coefficient c_0 and such that $y^3=\overline{f}(x,z)$ has a smooth point. It is convenient to also keep track of whether or not the forms satisfy condition $(*)$, whether $y^3-\overline{f}(x,z)$ is absolutely irreducible, or both, to give lower bounds for ρ^*, σ_1, and σ_1^*.

To illustrate this procedure, the output in the $p=13$ case is tabulated below in Table 4.6.1. Notice the symmetry present in the table; the c_0 and $-c_0$ rows are identical. This is the result of the facts that $\langle 2\rangle=\mathbb{F}_{13}^\times$, and $2^6\equiv -1 \pmod{13}$, and our observations above about the change of variables $z\mapsto 2z$. Considering only the presence of Hensel-liftable points and insoluble equations, these computations produce the following bounds.

$$\begin{aligned}
0.99851\approx\frac{62655132}{62748517}\le\rho(13)\ &\le\frac{4819929}{4826809}\approx 0.99857\\
0.99735\approx\frac{740621}{742586}\le\rho^*(13)&\le\frac{370433}{371293}\approx 0.99768\\
0.99837\approx\frac{8605}{8619}\le\sigma_1(13)&\le\frac{43034}{43095}\approx 0.99858\\
0.99738\approx\frac{105803}{106080}\le\sigma_1^*(13)&\le\frac{26459}{26520}\approx 0.99769
\end{aligned}$$

To verify the data in Table 4.3.1, we repeat these computations considering only the

Table 4.6.1: Counts of binary sextic forms $f(x,z) \in \mathbb{F}_{13}[x,z]$ with smooth points for specified constant coefficient, using `count_sextic_forms`$(13, c_0)$

c_0	Hensel	insoluble	total
0	4825604	0	4826809
1	4814593	10608	4826809
2	4820270	5680	4826809
3	4820634	5364	4826809
4	4820619	5364	4826809
5	4813393	12024	4826809
6	4820255	5680	4826809
7	4820255	5680	4826809
8	4813393	12024	4826809
9	4820619	5364	4826809
10	4820634	5364	4826809
11	4820270	5680	4826809
12	4814593	10608	4826809
Totals	62645132	89440	62748517

Hensel–liftable and insoluble equations for the seven primes $p \equiv 1 \pmod 3$ with $p \leq 61$. The resulting lower bounds are recorded in Table 4.6.2 below along with the approximate runtime of an instance of `count_sextic_forms`(p, c_0) on a server with four Intel Xeon E5-4627 CPUs, a total of 40 cores, and 1 TB of memory. As one expected, the complexity is about $O(p^5)$. Note in particular that for $p = 61$, the computation reflects the improved Hasse–Weil bound (4.3.3), which implied $\sigma_1 = \sigma_1^* = 1$ for $p = 61$ in Proposition 4.5.7.

Table 4.6.2: Lower bounds for ρ, ρ^*, σ_1, σ_1^* for $p \equiv 1 \pmod 3$ with $p \leq 61$

p	$\rho \geq$	$\rho^* \geq$	$\sigma_1 \geq$	$\sigma_1^* \geq$	runtime (s)
7	$\frac{810658}{823543}$	$\frac{32731}{33614}$	$\frac{7237}{7350}$	$\frac{32731}{33600}$	18
13	$\frac{62645132}{62748517}$	$\frac{740621}{742586}$	$\frac{8605}{8619}$	$\frac{105803}{106080}$	419
19	$\frac{893660256}{893871739}$	$\frac{2475177}{2476099}$	$\frac{522607}{522728}$	$\frac{825059}{825360}$	2961
31	$\frac{27512408250}{27512614111}$	$\frac{28628820}{28629151}$	$\frac{3697903}{3697928}$	$\frac{477147}{477152}$	37161
37	$\frac{94931742132}{94931877133}$	$\frac{69343806}{69343957}$	$\frac{937764}{937765}$	$\frac{608279}{608280}$	90131
43	$\frac{271818511748}{271818611107}$	$\frac{294016723}{294016886}$	$\frac{41047793}{41047800}$	$\frac{3818399}{3818400}$	194243
61	$\frac{3142742684700}{3142742836021}$	$\frac{13845840}{13845841}$	1	1	1091730

For $(m,d) = (5,5)$, a similar procedure using the above mentioned parallelization strat-

egy was used to produce the data for $p \equiv 1 \pmod 5$ with $p \leq 131$, tabulated in Table 4.3.2 in Example 4.3.16. For other (m, d), this enumeration strategy could be useful in estimating $\rho_{m,d}(p)$ and offers an improvement on Proposition 4.3.6, at the cost of the time required.

This enumeration strategy was also instrumental in determining the exact values of σ_1 and σ_1^* for small primes p, i.e. the proof of Proposition 4.5.27. After enumerating all binary sextic forms $\overline{f}(x, z)$ with Hensel-liftable points, we keep track of the factorization type modulo p — namely the presence of multiple roots — and determine the lifting probabilities using ν and π (see Lemmas 4.5.22, 4.5.25).

For example, when determining $\sigma_1(13)$, we find that 62644400 of the 62746320 forms $\overline{f}(x, z)$ produce $F(x, y, z)$ with a Hensel-liftable point and 88816 are insoluble. Of the remaining $\overline{f}(x, z)$, we find 10920 that have one double root, 2184 having two double roots, and no other factorization types occur. Thus

$$\sigma_1(13) = \frac{1}{62746320}\left(62644400 + 10920\nu + 2184(1-(1-\nu)^2)\right) = \frac{5931415654903952}{5941011706232655}, \tag{4.6.1}$$

the value given in Proposition 4.5.27. This calculation is repeated for the primes $p = 7, 19, 31, 37, 43$ and a similar philosophy is used for $p = 3$ in Proposition 4.5.30.

4.7 Counting binary forms by factorization type

Lemma 4.7.1. *For $2 \leq d \leq 6$ let $N_{d,i}$ (resp. $N'_{d,i}$) denote the number of binary forms $f(x, z)$ over $\mathbb{F}_p$ up to scaling (resp. monic) having the factorization types specified by i in the second column of the table below. For $N_{d,i}$ and $N'_{d,i}$ can be computed in terms of p and are tabulated below.*

d	*Fact. type*	$N_{d,i}$	$N'_{d,i}$
2	*0. No roots*	$\frac{1}{2}(p-1)p$	$\frac{1}{2}(p-1)p$
	1. $(1*)$	$\frac{1}{2}(p+1)p$	$\frac{1}{2}(p-1)p$
	2. (1^2)	$p+1$	p
3	*0. No roots*	$\frac{1}{3}(p+1)(p-1)p$	$\frac{1}{3}(p+1)(p-1)p$
	1. $(1*)$	$\frac{1}{3}(2p+1)(p+1)p$	$\frac{2}{3}(p+1)(p-1)p$
	2. (1^3)	$p+1$	p
	0. No roots	$\frac{1}{8}(3p^2+p+2)(p-1)p$	$\frac{1}{8}(3p^2+p+2)(p-1)p$

d	*Fact. type*	$N_{d,i}$	$N'_{d,i}$
	1. $(1*)$	$\frac{1}{8}\big(5p^2+p+2\big)(p+1)p$	$\frac{1}{8}\big(5p^2+3p+2\big)(p-1)p$
	2. $(1^2 2)$	$\frac{1}{2}(p+1)(p-1)p$	$\frac{1}{2}(p-1)p^2$
	3. $(1^2 1^2)$	$\frac{1}{2}(p+1)p$	$\frac{1}{2}(p-1)p$
	4. (1^4)	$p+1$	p
5	*0. No roots*	$\frac{1}{30}\big(11p^2-5p+6\big)(p+1)(p-1)p$	$\frac{1}{30}\big(11p^2-5p+6\big)(p+1)(p-1)p$
	1. $(1*)$	$\frac{1}{30}\big(19p^3+6p^2+4p+1\big)(p+1)p$	$\frac{1}{30}\big(19p^3+14p^2+4p-6\big)(p-1)p$
	2. $(1^2 3)$	$\frac{1}{3}(p+1)^2(p-1)p$	$\frac{1}{3}(p+1)(p-1)p^2$
	3. $(1^3 2)$	$\frac{1}{2}(p+1)(p-1)p$	$\frac{1}{2}(p-1)p^2$
	4. $(1^2 1^3)$	$(p+1)p$	$(p-1)p$
	5. (1^5)	$p+1$	p
6	*0. No roots*	$\frac{1}{144}\big(53p^4+26p^3+19p^2-2p+24\big)(p-1)p$	$\frac{1}{144}\big(53p^4+26p^3+19p^2-2p+24\big)(p-1)p$
	1. $(1*)$	$\frac{1}{144}\big(91p^4+26p^3+23p^2+16p-12\big)(p+1)p$	$\frac{1}{144}\big(91p^3-27p^2+50p-48\big)(p+1)(p-1)p$
	2. $(1^2 4), (1^2 22)$	$\frac{1}{8}\big(3p^2+p+2\big)(p+1)(p-1)p$	$\frac{1}{8}\big(3p^2+p+2\big)(p-1)p^2$
	3. $(1^2 1^2 2)$	$\frac{1}{4}(p+1)(p-1)p^2$	$\frac{1}{4}(p-1)^2p^2$
	4. $(1^2 1^2 1^2)$	$\frac{1}{6}(p+1)(p-1)p$	$\frac{1}{6}(p-1)(p-2)p$
	5. $(1^3 3)$	$\frac{1}{3}(p+1)^2(p-1)p$	$\frac{1}{3}(p+1)(p-1)p^2$
	6. $(1^3 1^3)$	$\frac{1}{2}(p+1)p$	$\frac{1}{2}(p-1)p$
	7. $(1^4 2)$	$\frac{1}{2}(p+1)(p-1)p$	$\frac{1}{2}(p-1)p^2$
	8. $(1^2 1^4)$	$(p+1)p$	$(p-1)p$
	9. (1^6)	$p+1$	p

Proof. This is an elementary computation, as noted in [BCF21, Lemma 2.3], in which each subsequent row is obtained from the previous one. We give a proof for $d = 6$ here, assuming the results in the previous rows of the table. To obtain the result for $d < 6$ — or indeed any d value if one is patient — one can use the same idea.

Let $f(x, z)$ be a degree 6 binary form over $\mathbb{F}_p$, up to scaling. We first consider all cases in which f has a multiple root but no simple root, which are precisely Types 2 – 9 above. Several of these can be calculated via combinatorics alone, beginning with Case 9, where f has a sextuple root, or factorization type (1^6). There are exactly $p+1$ such roots, corresponding to the $p+1$ distinct linear factors up to scaling, so we have $p+1$ forms up to scaling. Case 8 is similar: to give a form of type $(1^2 1^4)$ up to scaling, it suffices to identify a distinct linear factor for each root. Since the multiplicities are different, order matters, giving $(p+1)p$ possibilities. Types 4 and 6 ($(1^2 1^2 1^2)$ and $(1^3 1^3)$ respectively) are similar, but order does not matter, so there are $\binom{p+1}{3}$ and $\binom{p+1}{2}$ possibilities, respectively.

To deal with Type 7, $(1^4 2)$, we use the $d = 2$ row in the table to determine how many binary quadratic forms there are up to scaling, and multiply this by $p + 1$, the number of possible 1^4 factors. Similar arguments work for $(1^3 3)$ and $(1^2 4)$, using the result for degrees 3 and 4.

The case of $(1*)$ is the most involved, so we break the calculation down into cases based on the number of distinct simple roots f has, i.e. the number of 1's appearing in its factorization type. If f has 6 distinct simple roots, there are $\binom{p+1}{6}$ possibilities for f. It is not possible to have exactly 5 simple roots, so we move to the case of 4 distinct simple roots times a quadratic which has no double roots. There are $\binom{p+1}{4} N_{2,0}$ possibilities when the quadratic is irreducible and $\binom{p}{4} N_{2,2}$ when the quadratic has a double root. Note there is one fewer linear factor to choose the 4 simple roots from, since they must avoid the double root of the quadratic factor.

Continuing along this line, we find

$$\begin{aligned} N_{6,1} = \binom{p+1}{6} + \binom{p+1}{4} N_{2,0} + \binom{p}{4} N_{2,2} + \binom{p+1}{3} N_{3,0} + \binom{p}{3} N_{3,2} \\ + \binom{p+1}{2} N_{4,0} + \binom{p}{2} (N_{4,2} + N_{4,4}) + \binom{p-1}{2} N_{4,3} \\ + (p+1) N_{5,0} + p(N_{5,2} + N_{5,3} + N_{5,5}) + (p-1) N_{5,4}, \end{aligned}$$

which may be computed via computer algebra software; an implementation is included in the GitHub repository associated to this paper [BK21b, `SEC_rho36_23Aug21.ipynb`]. To conclude, we recognize that Types 1 – 9 are precisely those f possessing a root. Therefore we have

$$N_{6,0} = \left(\sum_{i=0}^{6} p^i \right) - \left(\sum_{j=1}^{d} N_{6,j} \right).$$

The same strategies work for computing each $N'_{6,i}$ for the monic case. The only differences are that there are p choices of linear factors, rather than $p + 1$, due to the monicity assumption, and that the appropriate monic quantities $N'_{d,i}$ are used in place of $N_{d,i}$ throughout. □

Proof of Lemma 4.5.6. Let $\eta_{d,i}$ (resp. $\eta'_{d,i}$) denote the proportion of binary degree d forms

$f(x,z)$ over $\mathbb{F}_p$ up to scaling by $\mathbb{F}_p^\times$ (resp. $f(x,z)$ is monic) having a factorization type corresponding to i in Lemma 4.7.1. By our earlier observations,

$$\eta_{d,i} = \frac{N_{d,i}}{\sum_{j=0}^{d} p^j}, \qquad \eta'_{d,i} = \frac{N'_{d,i}}{p^d}.$$

These values are precisely those in Lemma 4.5.6. □

Remark 4.7.2. There is no serious obstacle to extending Lemma 4.7.1 and thus Lemma 4.5.6 to higher degrees. In fact, one would likely have to do so in order to compute exact formulas for $\rho_{m,d}$ when $d > 6$.

Remark 4.7.3. Let $\eta_{d,1}$ (resp. $\eta'_{d,1}$) denote the proportion of degree d forms $f(x,z) \in \mathbb{F}_p[x,z]$ which possess at least one simple root. Writing $\eta_{d,1} = \eta_{d,1}(p)$ and taking limits as $p, d \to \infty$, we find

$$\lim_{d\to\infty}\lim_{p\to\infty} \eta_{d,1}(p) = \lim_{d\to\infty}\lim_{p\to\infty} \eta'_{d,1}(p) = 1 - \frac{1}{e} \approx 0.63212.$$

To see why, consider the case of monic forms; that of forms up to scaling follows from the same argument. We first observe that as $p \to \infty$, the proportion of forms with a multiple root goes to 0, so we may safely ignore these when considering the large p limit.

We then count forms with at a root by inclusion-exclusion. There are $p^d = p \cdot p^{d-1}$ choices of $f = (x-\alpha)g$ for g monic of degree $d-1$, but this double counts those of the form $f = (x-\alpha)(x-\beta)h$ for $\alpha \neq \beta$ and h monic of degree $d-2$, of which there are seen to be $\binom{p}{2}p^{d-2}$. Continuing in this manner, we find

$$\begin{aligned}\lim_{p\to\infty} \eta'_{d,1}(p) &= \lim_{p\to\infty} \frac{1}{p^d} \sum_{j=1}^{d} (-1)^{j+1} \binom{p}{j} p^{d-j} \\ &= \sum_{j=1}^{d} (-1)^{j+1} \frac{1}{j!}.\end{aligned}$$

Taking the limit as $d \to \infty$, we obtain $\sum_{j\geq 1} (-1)^{j+1} \frac{1}{j!} = 1 - \frac{1}{e}$, as seen from the Taylor expansion of the exponential function.

This is related to the proportion of permutations in S_d possessing at least one fixed

point, which is well known to approach $1 - \frac{1}{e}$ as $d \to \infty$. For much more, and results on the density of polynomials with a fixed number of roots, see [BCFG22].

4.8 Explicit formulas for rational functions

$$\rho = \begin{cases} \big(1296p^{57} + 3888p^{56} + 9072p^{55} + 16848p^{54} + 27648p^{53} + 39744p^{52} + 53136p^{51} + 66483p^{50} \\ + 80019p^{49} + 93141p^{48} + 107469p^{47} + 120357p^{46} + 135567p^{45} + 148347p^{44} + 162918p^{43} + 176004p^{42} \\ + 190278p^{41} + 203459p^{40} + 218272p^{39} + 232083p^{38} + 243639p^{37} + 255267p^{36} + 261719p^{35} \\ + 264925p^{34} + 265302p^{33} + 261540p^{32} + 254790p^{31} + 250736p^{30} + 241384p^{29} + 226503p^{28} \\ + 214137p^{27} + 195273p^{26} + 170793p^{25} + 151839p^{24} + 136215p^{23} + 118998p^{22} + 105228p^{21} + 94860p^{20} \\ + 80471p^{19} + 67048p^{18} + 52623p^{17} + 40617p^{16} + 28773p^{15} + 19247p^{14} + 12109p^{13} + 7614p^{12} \\ + 3420p^{11} + 756p^{10} - 2248p^{9} - 4943p^{8} - 6300p^{7} - 6894p^{6} - 5994p^{5} - 2448p^{4} - 648p^{3} + 324p^{2} \\ + 1296p + 1296\big) \Big/ \Big(1296\big(p^{12} - p^{11} + p^{9} - p^{8} + p^{6} - p^{4} + p^{3} - p + 1\big)\big(p^{8} - p^{6} + p^{4} - p^{2} + 1\big) \\ \times \big(p^{6} + p^{5} + p^{4} + p^{3} + p^{2} + p + 1\big)\big(p^{4} + p^{3} + p^{2} + p + 1\big)^{3}\big(p^{4} - p^{3} + p^{2} - p + 1\big) \\ \times \big(p^{2} + p + 1\big)\big(p^{2} + 1\big)p^{11}\Big), & p \equiv 1 \pmod 3 \\ \\ \big(144p^{57} + 432p^{56} + 1008p^{55} + 1872p^{54} + 3168p^{53} + 4608p^{52} + 6336p^{51} + 8011p^{50} + 9803p^{49} \\ + 11357p^{48} + 13061p^{47} + 14525p^{46} + 16295p^{45} + 17875p^{44} + 19654p^{43} + 21212p^{42} + 23030p^{41} \\ + 24563p^{40} + 26320p^{39} + 27771p^{38} + 29711p^{37} + 30859p^{36} + 31135p^{35} + 31525p^{34} \\ + 31510p^{33} + 29436p^{32} + 28502p^{31} + 28616p^{30} + 26856p^{29} + 25087p^{28} + 25057p^{27} \\ + 23041p^{26} + 19921p^{25} + 18119p^{24} + 16287p^{23} + 13798p^{22} + 12140p^{21} + 10844p^{20} \\ + 9191p^{19} + 7480p^{18} + 5839p^{17} + 4265p^{16} + 2909p^{15} + 1943p^{14} + 1109p^{13} + 590p^{12} \\ + 604p^{11} + 372p^{10} - 144p^{9} - 87p^{8} - 84p^{7} - 678p^{6} - 618p^{5} - 144p^{4} - 168p^{3} - 156p^{2} + 144p \\ + 144\big) \Big/ \Big(144\big(p^{12} - p^{11} + p^{9} - p^{8} + p^{6} - p^{4} + p^{3} - p + 1\big)\big(p^{8} - p^{6} + p^{4} - p^{2} + 1\big) \\ \times \big(p^{6} + p^{5} + p^{4} + p^{3} + p^{2} + p + 1\big)\big(p^{4} + p^{3} + p^{2} + p + 1\big)^{3}\big(p^{4} - p^{3} + p^{2} - p + 1\big) \\ \times \big(p^{2} + p + 1\big)\big(p^{2} + 1\big)p^{11}\Big), & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.1}$$

$$\begin{aligned} \rho^* = \; & \big(72p^{34} + 216p^{33} + 432p^{32} + 720p^{31} + 1008p^{30} + 1224p^{29} + 1260p^{28} + 1296p^{27} \\ & + 1152p^{26} + 1080p^{25} + 1068p^{24} + 1032p^{23} + 1104p^{22} + 1092p^{21} + 1116p^{20} \\ & + 1089p^{19} + 1104p^{18} + 1088p^{17} + 1126p^{16} + 1149p^{15} + 1017p^{14} + 906p^{13} + 830p^{12} \\ & + 634p^{11} + 360p^{10} + 441p^{9} + 378p^{8} + 194p^{7} + 280p^{6} + 327p^{5} + 93p^{4} + 36p^{3} \\ & + 60p^{2} - 36p - 72\big) \Big/ \Big(72\big(p^{8} - p^{6} + p^{4} - p^{2} + 1\big)\big(p^{4} + p^{3} + p^{2} + p + 1\big)^{3} \\ & \times \big(p^{4} - p^{3} + p^{2} - p + 1\big)\big(p^{2} + 1\big)(p + 1)p^{7}\Big) \end{aligned} \tag{4.8.2}$$

$$\sigma_4 = \begin{aligned}&\big(72p^{29}+180p^{28}+396p^{27}+684p^{26}+1044p^{25}+1392p^{24}+1608p^{23}\\&+1824p^{22}+1848p^{21}+1872p^{20}+1845p^{19}+1860p^{18}+1844p^{17}+1882p^{16}\\&+1905p^{15}+1845p^{14}+1878p^{13}+2018p^{12}+2110p^{11}+2124p^{10}+2349p^{9}\\&+2214p^{8}+1850p^{7}+1504p^{6}+1119p^{5}+525p^{4}+216p^{3}+96p^{2}-36p\\&-72\big)\Big/\Big(72\big(p^8-p^6+p^4-p^2+1\big)\big(p^4+p^3+p^2+p+1\big)^3\big(p^4-p^3+p^2-p+1\big)\\&\times\big(p^2+p+1\big)\big(p^2+1\big)p^2\Big)\end{aligned} \tag{4.8.3}$$

$$\sigma_4^* = \begin{aligned}&\big(72p^{29}+108p^{28}+288p^{27}+432p^{26}+648p^{25}+852p^{24}+960p^{23}+1104p^{22}\\&+1092p^{21}+1116p^{20}+1089p^{19}+1104p^{18}+1088p^{17}+1126p^{16}\\&+1149p^{15}+1089p^{14}+1122p^{13}+1262p^{12}+1354p^{11}+1368p^{10}+1593p^{9}\\&+1530p^{8}+1202p^{7}+1000p^{6}+759p^{5}+309p^{4}+108p^{3}+60p^{2}-36p\\&-72\big)\Big/\Big(72\big(p^8-p^6+p^4-p^2+1\big)\big(p^4+p^3+p^2+p+1\big)^3\big(p^4-p^3+p^2-p+1\big)\\&\times\big(p^2+1\big)(p+1)p^3\Big)\end{aligned} \tag{4.8.4}$$

$$\sigma_5 = \begin{cases}\begin{aligned}&\big(819p^{50}+2691p^{49}+6309p^{48}+12573p^{47}+21573p^{46}+32895p^{45}+45387p^{44}+59238p^{43}+73080p^{42}\\&+86742p^{41}+100547p^{40}+114472p^{39}+128439p^{38}+141579p^{37}+157131p^{36}+169247p^{35}+184741p^{34}\\&+203094p^{33}+219096p^{32}+237726p^{31}+261800p^{30}+276904p^{29}+283923p^{28}+291645p^{27}\\&+286281p^{26}+267993p^{25}+254943p^{24}+240039p^{23}+222678p^{22}+208152p^{21}+198396p^{20}\\&+183383p^{19}+170848p^{18}+156267p^{17}+142677p^{16}+128205p^{15}+115607p^{14}+101365p^{13}+86670p^{12}\\&+73512p^{11}+57564p^{10}+39824p^{9}+25201p^{8}+13608p^{7}+2430p^{6}-2106p^{5}-864p^{4}-1080p^{3}-540p^{2}\\&+1296p+1296\big)\Big/\Big(1296\big(p^{12}-p^{11}+p^9-p^8+p^6-p^4+p^3-p+1\big)\big(p^8-p^6+p^4-p^2+1\big)\\&\times\big(p^6+p^5+p^4+p^3+p^2+p+1\big)\big(p^4+p^3+p^2+p+1\big)^3\big(p^4-p^3+p^2-p+1\big)\\&\times\big(p^2+p+1\big)\big(p^2+1\big)p^4\Big),\end{aligned} & p\equiv 1 \pmod 3\\[2ex]\begin{aligned}&\big(91p^{50}+299p^{49}+701p^{48}+1397p^{47}+2429p^{46}+3767p^{45}+5347p^{44}+6982p^{43}+8684p^{42}\\&+10358p^{41}+12035p^{40}+13648p^{39}+15243p^{38}+17183p^{37}+18907p^{36}+19903p^{35}+21877p^{34}\\&+23878p^{33}+24684p^{32}+26774p^{31}+30344p^{30}+31608p^{29}+32719p^{28}+34705p^{27}+34273p^{26}\\&+31873p^{25}+30647p^{24}+28815p^{23}+26470p^{22}+24668p^{21}+23516p^{20}+21719p^{19}+20152p^{18}\\&+18367p^{17}+16793p^{16}+15005p^{15}+13607p^{14}+11765p^{13}+10094p^{12}+8524p^{11}\\&+6708p^{10}+4464p^{9}+3081p^{8}+1788p^{7}+330p^{6}-186p^{5}-168p^{3}-156p^{2}+144p\\&+144\big)\Big/\Big(144\big(p^{12}-p^{11}+p^9-p^8+p^6-p^4+p^3-p+1\big)\big(p^8-p^6+p^4-p^2+1\big)\\&\times\big(p^6+p^5+p^4+p^3+p^2+p+1\big)\big(p^4+p^3+p^2+p+1\big)^3\big(p^4-p^3+p^2-p+1\big)\\&\times\big(p^2+p+1\big)\big(p^2+1\big)p^4\Big),\end{aligned} & p\equiv 2 \pmod 3\end{cases} \tag{4.8.5}$$

$$\mu' = \begin{cases} \big(45p^{20} - 18p^{19} + 27p^{18} + 18p^{17} - 36p^{16} - 12p^{15} + 12p^{14} \\ \quad + 36p^{12} - 27p^{11} - 6p^{10} + 5p^9 - 30p^8 + 69p^7 - 29p^6 \\ \quad - 39p^5 + 81p^4 - 120p^3 + 60p^2 + 108p - 72\big) \Big/ 72p^{20}, & p \equiv 1 \pmod 3 \\ \big(5p^{20} - 2p^{19} + 3p^{18} + 2p^{17} - 4p^{16} + 4p^{15} - 4p^{14} + 4p^{12} - 3p^{11} + 2p^{10} \\ \quad - 3p^9 + 2p^8 + 5p^7 - 13p^6 + 9p^5 + 9p^4 - 24p^3 + 12p^2 + 12p - 8\big) \Big/ 8p^{20}, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.6}$$

$$\begin{aligned} \lambda = {} & \big(72p^{28} + 144p^{27} + 288p^{26} + 504p^{25} + 744p^{24} + 888p^{23} + 1068p^{22} \\ & + 1092p^{21} + 1116p^{20} + 1089p^{19} + 1104p^{18} + 1088p^{17} + 1126p^{16} \\ & + 1149p^{15} + 1089p^{14} + 1122p^{13} + 1262p^{12} + 1354p^{11} + 1368p^{10} + 1665p^9 \\ & + 1566p^8 + 1346p^7 + 1144p^6 + 903p^5 + 417p^4 + 180p^3 + 96p^2 - 36p \\ & - 72\big) \Big/ \Big(72\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ & \times \big(p^2 + 1\big)(p + 1)p^2\Big) \end{aligned} \tag{4.8.7}$$

$$\sigma_5' = \begin{cases} \Big(91p^{30} + 246p^{29} + 478p^{28} + 850p^{27} + 1262p^{26} + 1680p^{25} + 1902p^{24} + 2202p^{23} + 2242p^{22} + 2271p^{21} \\ \quad + 2243p^{20} + 2270p^{19} + 2214p^{18} + 2185p^{17} + 2299p^{16} + 2142p^{15} + 2228p^{14} + 2570p^{13} + 2512p^{12} \\ \quad + 2701p^{11} + 3300p^{10} + 2984p^9 + 2348p^8 + 2323p^7 + 1363p^6 + 288p^5 + 186p^4 + 60p^3 - 264p^2 \\ \quad - 72p + 144\Big) \Big/ \Big(144\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \quad \times \big(p^2 + 1\big)(p + 1)p^3\Big), & p \equiv 1 \pmod 3 \\ \Big(91p^{30} + 246p^{29} + 478p^{28} + 850p^{27} + 1294p^{26} + 1792p^{25} + 2206p^{24} + 2410p^{23} + 2578p^{22} + 2671p^{21} \\ \quad + 2635p^{20} + 2574p^{19} + 2590p^{18} + 2769p^{17} + 2667p^{16} + 2286p^{15} + 2580p^{14} + 2826p^{13} + 2160p^{12} \\ \quad + 2781p^{11} + 3852p^{10} + 3096p^9 + 2628p^8 + 3195p^7 + 1827p^6 + 432p^5 + 522p^4 + 252p^3 - 360p^2 \\ \quad - 72p + 144\Big) \Big/ \Big(144\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \quad \times \big(p^2 + 1\big)(p + 1)p^3\Big), & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.8}$$

$$\sigma_5'' = \begin{cases} \big(819p^{43} + 2376p^{42} + 4599p^{41} + 7424p^{40} + 11091p^{39} + 14515p^{38} + 16101p^{37} + 19341p^{36} \\ + 19532p^{35} + 19542p^{34} + 20605p^{33} + 21042p^{32} + 21969p^{31} + 25640p^{30} + 27075p^{29} + 25531p^{28} \\ + 26901p^{27} + 24399p^{26} + 18864p^{25} + 19800p^{24} + 18900p^{23} + 16200p^{22} + 14580p^{21} + 14148p^{20} \\ + 8478p^{19} + 6102p^{18} + 3492p^{17} + 1476p^{16} + 378p^{15} + 378p^{14} - 324p^{13} + 468p^{12} + 180p^{11} \\ - 864p^{10} + 594p^9 + 2052p^8 + 684p^7 + 3096p^6 + 4590p^5 + 1674p^4 + 648p^3 + 1080p^2 - 648p \\ - 1296\big) \Big/ \big(1296\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \times \big(p^2 + 1\big)(p+1)p^{16}\big), & p \equiv 1 \pmod 3 \\ \\ \big(91p^{43} + 300p^{42} + 607p^{41} + 1024p^{40} + 1531p^{39} + 1903p^{38} + 2329p^{37} + 2581p^{36} \\ + 2404p^{35} + 2686p^{34} + 2725p^{33} + 2166p^{32} + 2497p^{31} + 3216p^{30} + 2739p^{29} + 2943p^{28} \\ + 3897p^{27} + 3279p^{26} + 2544p^{25} + 2904p^{24} + 2676p^{23} + 1992p^{22} + 1908p^{21} + 1764p^{20} \\ + 1134p^{19} + 630p^{18} + 324p^{17} + 180p^{16} + 90p^{15} - 54p^{14} - 36p^{13} + 180p^{12} - 108p^{11} \\ - 288p^{10} + 162p^9 + 180p^8 - 180p^7 + 360p^6 + 558p^5 + 90p^4 + 72p^3 + 216p^2 - 72p \\ - 144\big) \Big/ \big(144\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \times \big(p^2 + 1\big)(p+1)p^{16}\big), & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.9}$$

4.8.1 τ_i values (see Lemma 4.5.19)

$$\tau_6 = \begin{cases} \big(6p^4 + 3p^3 + 5p^2 + 4p + 4\big)\big(3p^3 + p^2 + 2p + 2\big) \Big/ 9\big(p^4 + p^3 + p^2 + p + 1\big)^2, & p \equiv 1 \pmod 3 \\ \\ \big(6p^4 + 3p^3 + 3p^2 + 4p + 4\big)\big(3p^2 + 2\big)(p+1) \Big/ 9\big(p^4 + p^3 + p^2 + p + 1\big)^2, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.10}$$

$$\tau_7 = \begin{cases} \big(72p^{16} - 48p^{15} + 12p^{14} + 36p^{12} - 27p^{11} - 6p^{10} + 5p^9 - 30p^8 \\ \quad + 69p^7 - 29p^6 - 39p^5 + 81p^4 - 120p^3 + 60p^2 + 108p - 72\big) \Big/ 72p^{17}, & p \equiv 1 \pmod 3 \\ \\ \big(8p^{16} - 4p^{14} + 4p^{12} - 3p^{11} + 2p^{10} - 3p^9 + 2p^8 + 5p^7 \\ \quad - 13p^6 + 9p^5 + 9p^4 - 24p^3 + 12p^2 + 12p - 8\big) \Big/ 8p^{17}, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.11}$$

$$\tau_8 = \begin{cases} \big(144p^{17} - 120p^{16} + 60p^{15} - 12p^{14} + 36p^{13} - 63p^{12} \\ \quad + 21p^{11} + 11p^{10} - 35p^9 + 99p^8 - 98p^7 - 10p^6 + 120p^5 \\ \quad - 201p^4 + 180p^3 + 48p^2 - 180p + 72\big) \Big/ 72p^{18}, & p \equiv 1 \pmod 3 \\ \big(16p^{17} - 8p^{16} - 4p^{15} + 4p^{14} + 4p^{13} - 7p^{12} + 5p^{11} - 5p^{10} \\ \quad + 5p^9 + 3p^8 - 18p^7 + 22p^6 - 33p^4 + 36p^3 - 20p + 8\big) \Big/ 8p^{18}, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.12}$$

$$\tau_9 = \begin{cases} \big(144p^{44} + 336p^{43} + 600p^{42} + 936p^{41} + 1416p^{40} + 1704p^{39} + 1968p^{38} + 2160p^{37} + 2328p^{36} \\ + 2136p^{35} + 2280p^{34} + 2472p^{33} + 2592p^{32} + 2784p^{31} + 3115p^{30} + 3030p^{29} + 2806p^{28} \\ + 2650p^{27} + 2366p^{26} + 2256p^{25} + 1998p^{24} + 1914p^{23} + 1642p^{22} + 1335p^{21} + 827p^{20} \\ + 566p^{19} + 246p^{18} + 25p^{17} - 29p^{16} + 6p^{15} - 52p^{14} + 98p^{13} - 80p^{12} - 83p^{11} \\ + 276p^{10} + 200p^9 + 20p^8 + 523p^7 + 259p^6 - 288p^5 - 54p^4 + 12p^3 - 264p^2 - 72p \\ + 144\big) \Big/ \Big(144\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \times \big(p^2 + 1\big)(p+1)p^{18}\Big), & p \equiv 1 \pmod 3 \\ \big(144p^{44} + 432p^{43} + 792p^{42} + 1224p^{41} + 1800p^{40} + 2184p^{39} + 2352p^{38} + 2640p^{37} + 2712p^{36} \\ + 2424p^{35} + 2472p^{34} + 2664p^{33} + 2592p^{32} + 2880p^{31} + 3403p^{30} + 3414p^{29} + 3286p^{28} \\ + 3226p^{27} + 2878p^{26} + 2656p^{25} + 2494p^{24} + 2122p^{23} + 1786p^{22} + 1447p^{21} + 835p^{20} \\ + 390p^{19} + 238p^{18} + 129p^{17} - 45p^{16} - 138p^{15} + 108p^{14} + 162p^{13} - 432p^{12} - 99p^{11} \\ + 540p^{10} - 72p^9 - 180p^8 + 819p^7 + 243p^6 - 432p^5 + 90p^4 + 108p^3 - 360p^2 - 72p \\ + 144\big) \Big/ \Big(144\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \times \big(p^2 + 1\big)(p+1)p^{18}\Big), & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.13}$$

4.8.2 θ_i values (see Lemma 4.5.21)

$$\theta_3 = \begin{cases} \big(10p^3 - p^2 + 3p - 6\big)\big(2p^2 - 3p + 3\big)(p+2) \Big/ 36p^6, & p \equiv 1 \pmod 3 \\ \big(2p^3 + p^2 + p - 2\big)\big(2p^2 - 3p + 2\big)(p+1) \Big/ 4p^6, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.14}$$

$$\theta_4 = \begin{cases} \big(76p^6 - 14p^5 + 43p^4 - 90p^3 + 21p^2 - 36p + 36\big) \\ \quad \times \big(2p^2 - 3p + 3\big)(p+2)\Big/216p^9, & p \equiv 1 \pmod 3 \\ \big(4p^6 + 2p^5 + 3p^4 - 2p^3 - 3p^2 - 4p + 4\big)\big(2p^2 - 3p + 2\big)(p+1)\Big/8p^9, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.15}$$

$$\theta_6 = \begin{cases} \big(5p^4 + 3p^3 + 6p^2 + 4p + 4\big)\big(p^4 + 3p^3 + 2p + 2\big)\Big/9\big(p^4 + p^3 + p^2 + p + 1\big)^2, & p \equiv 1 \pmod 3 \\ \big(3p^4 + 3p^3 + 6p^2 + 4p + 4\big)\big(3p^3 + 2\big)(p+1)\Big/9\big(p^4 + p^3 + p^2 + p + 1\big)^2, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.16}$$

$$\theta_7 = \begin{cases} \big(2p^8 + 4p^7 - 6p^6 + 3p^5 + 2p^4 - 4p^3 + 2p^2 + 9p - 6\big)\Big/6p^8, & p \equiv 1 \pmod 3 \\ \big(2p^8 - 2p^6 + p^5 + 2p^4 - 4p^3 + 2p^2 + 3p - 2\big)\Big/2p^8, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.17}$$

$$\theta_8 = \begin{cases} \big(20p^{11} + 20p^{10} - 40p^9 + 54p^8 - 37p^7 + 27p^6 \\ \quad + 10p^4 - 3p^3 + 21p^2 - 72p + 36\big)\Big/36p^{11}, & p \equiv 1 \pmod 3 \\ \big(4p^{11} - 2p^8 - p^7 + 7p^6 - 4p^5 - 6p^4 + 13p^3 - 3p^2 - 8p + 4\big)\Big/4p^{11}, & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.18}$$

$$\theta_9 = \begin{cases} \big(432p^{37} + 2160p^{36} + 3888p^{35} + 6264p^{34} + 9720p^{33} + 12528p^{32} + 13392p^{31} \\ + 16848p^{30} + 19440p^{29} + 21168p^{28} + 22842p^{27} + 25920p^{26} + 24948p^{25} + 23004p^{24} \\ + 22356p^{23} + 20907p^{22} + 19548p^{21} + 19179p^{20} + 20276p^{19} + 19569p^{18} + 20185p^{17} \\ + 17433p^{16} + 16929p^{15} + 13646p^{14} + 10200p^{13} + 7753p^{12} + 8118p^{11} + 5301p^{10} \\ + 5336p^9 + 6501p^8 + 4741p^7 + 1665p^6 + 2547p^5 + 450p^4 - 882p^3 - 540p^2 + 108p \\ - 648\big)\Big/\Big(1296\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \times \big(p^2+1\big)(p+1)p^{10}\Big), & p \equiv 1 \pmod 3 \\ \big(144p^{37} + 432p^{36} + 720p^{35} + 1080p^{34} + 1656p^{33} + 1872p^{32} + 1872p^{31} + 2160p^{30} + 2448p^{29} \\ + 2448p^{28} + 2826p^{27} + 3264p^{26} + 3252p^{25} + 3036p^{24} + 2964p^{23} + 2803p^{22} + 2592p^{21} \\ + 2515p^{20} + 2644p^{19} + 2665p^{18} + 2389p^{17} + 2221p^{16} + 2041p^{15} + 1414p^{14} + 976p^{13} + 817p^{12} \\ + 474p^{11} + 229p^{10} + 480p^9 + 453p^8 + 297p^7 + 453p^6 + 387p^5 + 66p^4 + 30p^3 + 36p^2 - 84p \\ - 72\big)\Big/\Big(144\big(p^8 - p^6 + p^4 - p^2 + 1\big)\big(p^4 + p^3 + p^2 + p + 1\big)^3\big(p^4 - p^3 + p^2 - p + 1\big) \\ \times \big(p^2+1\big)(p+1)p^{10}\Big), & p \equiv 2 \pmod 3 \end{cases} \tag{4.8.19}$$

4.8.3 Small primes p (see §4.5.6)

$$\rho(7) = \frac{631044947551786228516032926231872770547437301836456778939 72}{640831747872066968824299456558012815388441498964001598153 75} \approx 0.98472 \tag{4.8.20}$$

$$\rho(13) = \frac{787772835724457741402590193129674740968207625566652698451527352682285 3}{789064357062010674777673729279278062351072702642077953989377239970147 5} \approx 0.99836 \tag{4.8.21}$$

$$\rho(19) = \frac{312267371548920615044928586824336115039223579936581526687943839327934679567 1}{312341001331136515503596447983796679756085133361427149013648133708063645418 0} \approx 0.99976 \tag{4.8.22}$$

$$\rho(31) = \frac{919679645767831886913908993678646214653521003983285045429787748202063507385715975829 9}{919686506158784354483098904147380879891312858742599564585782857261091843603583390725 0} \approx 0.999992 \tag{4.8.23}$$

$$\rho(37) = \frac{171128647900820194784458101787952920169924464886519055453844647154184805036447476640345735119}{171128889636157060536894474187017088464271236509977199491208939449738127658679723715588944500} \approx 0.999998 \tag{4.8.24}$$

$$\rho(43) = \frac{840001213432830903886533564318041007073313647792906644905471057688678448627121344478327205087502 81}{840001516715135551916477125675961017108008462091168305680137293774049911509019731050930399392375 00} \approx 0.9999996 \tag{4.8.25}$$

Chapter 5

Mertens' theorem for Chebotarev sets

5.1 Introduction

The Chebotarev density theorem (c.f. Theorem 2.3.6) is a deep generalization of the prime number theorem; it contains Dirichlet's theorem for primes in arithmetic progressions as a special case. In [Wil74], Williams proved Mertens' theorem for primes in arithmetic progressions. Here, adapting Williams' method, we generalize Mertens' theorem to Chebotarev sets of prime ideals in a number field. Given a Galois extension of number fields E/F with Galois group $G := \mathrm{Gal}(E/F)$, and given a conjugacy class $C \subseteq G$, we prove

$$\prod_{\substack{N(P)\leq x\\ \mathrm{Frob}_P=C}} \left(1-\frac{1}{N(P)}\right) \sim \left(\frac{e^{-\gamma(E/F,C)}}{\log x}\right)^{\#C/\#G}, \quad \text{as } x\to\infty, \tag{5.1.1}$$

where P runs over all primes of F which are unramified in E and with absolute norm bounded by x. In addition, we provide a power saving error term and a description of the constant $e^{-\gamma(E/F,C)}$.

Taking $E = F = \mathbb{Q}$, (5.1.1) specializes to Mertens' theorem [Mer74]; i.e.,

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}, \quad \text{as } x\to\infty, \tag{5.1.2}$$

where γ is the Euler constant. See, for example, [MV06, Theorem 2.7] for a modern discussion and proof of (5.1.2).

Further, taking a cyclotomic extension $E = \mathbb{Q}(\zeta_b) \supset F = \mathbb{Q}$, the Galois group is isomorphic to $(\mathbb{Z}/b\mathbb{Z})^\times$. Picking the conjugacy class corresponding to some element $a \in (\mathbb{Z}/b\mathbb{Z})^\times$, and letting $\varphi(b) := \#(\mathbb{Z}/b\mathbb{Z})^\times$ be the usual totient function, (5.1.1) specializes to Williams' theorem [Wil74, Theorem 1]

$$\prod_{\substack{p \le x \\ p \equiv a \bmod b}} \left(1 - \frac{1}{p}\right) \sim \left(\frac{e^{-\gamma(a,b)}}{\log x}\right)^{1/\varphi(b)}, \quad \text{as } x \to \infty. \tag{5.1.3}$$

Our result relies heavily on work of Rosen [Ros99, Theorem 2], who proved the Mertens-type analog of Landau's prime ideal theorem. Taking $E = F \supset \mathbb{Q}$, (5.1.1) specializes to Rosen's result; i.e.,

$$\prod_{N(P) \le x} \left(1 - \frac{1}{N(P)}\right) \sim \frac{e^{-\gamma_E}}{\log x}, \quad \text{as } x \to \infty. \tag{5.1.4}$$

We summarize these cases, in analogy with the corresponding prime number theorems, in Table 5.1.1 below.

5.1.1 Notation

We use s to denote a complex variable and write $s := \sigma + it$ for its real and imaginary parts.

For an algebraic number field $F/\mathbb{Q}$, let $\mathcal{O}_F$ be its ring of integers. Given a non-zero integral ideal $I \trianglelefteq \mathcal{O}_F$, we use $N_F(I) := \#(\mathcal{O}_F/I)$ and $\varphi_F(I) := \#(\mathcal{O}_F/I)^\times$ to denote its absolute norm and totient, respectively. We will take Σ_F to be the set of maximal ideals of $\mathcal{O}_F$.

The Dedekind zeta function of F is denoted by $\zeta_F(s)$, and $\varkappa_F$ will stand for its residue at the pole $s = 1$.

Given a subset $S \subseteq \Sigma_F$ and a real number $x \ge 2$, we define $S(x) := \{P \in S : N_F(P) \le x\}$. If S has a natural density, it will be denoted by $\delta(S)$ as in Definition 2.3.2.

Table 5.1.1: Prime number theorems vs. Mertens-type theorems

Trivial extension $E = F = \mathbb{Q}$	Prime number theorem $\sum_{p \leq x} 1 \sim \frac{x}{\log x}$	Mertens' theorem $\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}$
Cyclotomic extension $E = \mathbb{Q}(\zeta_b), F = \mathbb{Q}$	Dirichlet's theorem $\sum_{\substack{p \leq x \\ p \equiv a \bmod b}} 1 \sim \frac{1}{\varphi(b)} \frac{x}{\log x}$	Williams' theorem $\prod_{\substack{p \leq x \\ p \equiv a \bmod b}} \left(1 - \frac{1}{p}\right) \sim \left(\frac{e^{-\gamma(a,b)}}{\log x}\right)^{1/\varphi(b)}$
Number field $E = F \supseteq \mathbb{Q}$	Laundau's theorem $\sum_{N(P) \leq x} 1 \sim \frac{x}{\log x}$	Rosen's theorem $\prod_{N(P) \leq x} \left(1 - \frac{1}{N(P)}\right) \sim \frac{e^{-\gamma_E}}{\log x}$
Galois extension $E \supseteq F \supseteq \mathbb{Q}$	Chebotarev's theorem $\sum_{\substack{N(P) \leq x \\ \mathrm{Frob}_P = C}} 1 \sim \frac{\#C}{\#G} \frac{x}{\log x}$	Equation 5.1.1 $\prod_{\substack{N(P) \leq x \\ \mathrm{Frob}_P = C}} \left(1 - \frac{1}{N(P)}\right) \sim \left(\frac{e^{-\gamma(E/F,C)}}{\log x}\right)^{\#C/\#G}$

Throughout the chapter, E/F will be a Galois extension of number fields with Galois group $G := \mathrm{Gal}(E/F)$, and $C \subseteq G$ will be a fixed conjugacy class. The letters Q and P stand for elements of Σ_E and Σ_F, respectively. Moreover, Q will always be a prime of E above P. Their respective residue fields are denoted by $\mathbb{F}_Q$ and $\mathbb{F}_P$.

$$\begin{array}{ccc} E & \supset & Q \\ {\scriptstyle G=\mathrm{Gal}(E/F)}\big| & & \big| \\ F & \supset & P \end{array} \qquad\qquad \begin{array}{c} \mathbb{F}_Q \\ \big| {\scriptstyle \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P)} \\ \mathbb{F}_P \end{array}$$

As in §2.3, we denote by $I_Q \trianglelefteq D_Q \subseteq G$ the inertia and decomposition groups of a prime Q above P. Choosing another prime above P, the corresponding inertia and decomposition groups are G-conjugates of I_Q and D_Q. Recall from Definition 2.3.5 that a Frobenius element $\mathrm{Frob}_Q \in D_Q$ has image in $\mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ the cyclic generator. Frobenius elements are only defined modulo the inertia subgroup. Recall that $P \in \Sigma_F$ is unramified in E if and only if P does not divide the discriminant ideal $\Delta := \Delta_{E/F}$. We will denote the set of unramified primes by $S_{E/F} \subseteq \Sigma_F$. For an unramified prime, P, we denote by Frob_P the (well defined) conjugacy class of Frobenius elements at all primes Q above P. Given a conjugacy class

$C \subseteq G$, let $\mathcal{C}$ be the set of unramified primes in Σ_F with Frobenius conjugacy class equal to C.

Let $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ be a representation of G with underlying vector space V. We will use χ to denote the trace of ρ. Given any prime $P \in \Sigma_F$, and $Q \in \Sigma_E$ above P, let

$$L_P(s, \chi, F) := \sigma > 1, \tag{5.1.5}$$

be the **Artin Euler factor** at P. The **Artin L-function** of χ is defined for $\sigma > 1$ by the Euler product $L(s, \chi, F) := \prod_{P \in \Sigma_F} L_P(s, \chi, F)$. We will use the facts that $L(s, \chi, F)$ has a meromorphic extension to the complex numbers, and if χ is a nontrivial character then $L(1, \chi, F) \neq 0$. When a Galois extension E/F is fixed, we abbreviate $L(s, \chi, F)$ to $L(s, \chi)$. For a comprehensive introduction to the topic of Artin L-functions, see [MM12].

5.1.2 Main result

Now that we have the necessary notation in place, we are ready to state our main result.

Theorem 5.1.1. *Let E/F be a Galois extension of number fields, with Galois group $G := \mathrm{Gal}(E/F)$, and let $C \subset G$ be a conjugacy class. Then,*

$$\prod_{P \in \mathcal{C}(x)} \left(1 - \frac{1}{N(P)}\right) = \left(\frac{e^{-\gamma(E/F,C)}}{\log x}\right)^{\#C/\#G} + O\left(\frac{1}{(\log x)^{\delta(\mathcal{C})+1}}\right) \tag{5.1.6}$$

when $x \to \infty$, and the implied constant depends on the extension E/F and C. Furthermore, the constant $e^{-\gamma(E/F,C)}$ is given by

$$e^{-\gamma(E/F,C)} = e^{-\gamma_F} \prod_{P \in \Sigma_F} \left(1 - \frac{1}{N(P)}\right)^{\alpha(E/F,C;P)} \tag{5.1.7}$$

where $\gamma_F := \gamma + \log \varkappa_F$, and

$$\alpha(E/F, C; P) = \begin{cases} -1, & P \mid \Delta, \\ \frac{\#G}{\#C} - 1, & \mathrm{Frob}_P = C, \\ -1, & \mathrm{Frob}_P \neq C. \end{cases} \tag{5.1.8}$$

A result similar to Theorem 5.1.1, of which we became aware after finishing our work, appears in an unpublished survey article of Bardestani and Freiberg [BF, §8]. The approach sketched there follows an adaptation of a proof of Mertens' Theorem due to Hardy, while our method closely follows the strategy of Williams and obtains both an improved statement for the error term and a description of the constants involved.

Remark 5.1.2 (Error terms)**.** The error term $O\left(\frac{1}{(\log x)^{\delta(\mathcal{C})+1}}\right)$ in (5.1.6) agrees with that given by Williams [Wil74]. In the case of a cyclotomic extension $\mathbb{Q}(\zeta_b)/\mathbb{Q}$, the error term may be improved by studying zero-free regions of Dirichlet L-functions; see [LZ07]. Assuming the generalized Riemann hypothesis (GRH), one can improve this error term all the way to $O\left(\frac{(\log x)^{1-\varphi(b)}}{\sqrt{x}}\right)$ [LZ07, Theorem 4]. Assuming GRH, one also obtains similarly sharp error estimates for (5.1.4), Mertens' theorem over number fields; see [Leb07, Theorem 7]. In order to carry these improvements to the error term in (5.1.6) to the general case, we need faster convergence of $L(1,\chi)$ for irreducible non-trivial χ than what we use in Theorem 5.2.1 (see [Ros99, Theorem 5]). This was studied in a recent paper of Garcia and Lee [GL22, Theorem B].

5.1.3 Layout

In §5.2, we summarize the work of Williams and Rosen and prove some supporting lemmas. In §5.3 we prove Theorem 5.1.1. In §5.4 we provide some examples.

Acknowledgments

We would like to thank Robert Lemke Oliver and David Zureick-Brown for helpful conversations and Paul Pollack for bringing the work of Languasco and Zaccagnini to our attention. We also thank Kenneth Williams for suggesting we investigate the case of primes represented by quadratic forms.

5.2 Background

5.2.1 Williams' argument

Consider momentarily the case of a cyclotomic extension. Let b be a positive integer, and choose $0 < a < b$ coprime to b. In [Wil74], Williams proved

$$\prod_{\substack{p \leq x \\ p \equiv a \bmod b}} \left(1 - \frac{1}{p}\right) = \left(\frac{e^{-\gamma(a,b)}}{\log x}\right)^{1/\varphi(b)} + O_b\left(\frac{1}{(\log x)^{1/\varphi(b)+1}}\right). \tag{5.2.1}$$

Furthermore, he was able to give a formula for the constant $\gamma(a,b)$ in terms of

- the Euler constant $\gamma := \lim_{s \to 1^+} \left(\zeta(s) - \frac{1}{s-1}\right)$;
- the ramified primes of the extension $\mathbb{Q}(\zeta_b)/\mathbb{Q}$, namely $\prod_{p|b}(1-p^{-1})^{-1} = b/\varphi(b)$;
- the values at $s = 1$ of the Dirichlet L-functions $L(s,\chi)$, for all non-trivial irreducible characters χ of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_b)/\mathbb{Q}) \cong (\mathbb{Z}/b\mathbb{Z})^\times$;
- the values at $s = 1$ of some auxiliary functions $K(s,\chi)$, attached to all non-trivial irreducible characters χ of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_b)/\mathbb{Q}) \cong (\mathbb{Z}/b\mathbb{Z})^\times$.

Explicitly,

$$e^{-\gamma(a,b)} := e^{-\gamma}\frac{b}{\varphi(b)} \prod_{\chi \neq \chi_0} \left(\frac{K(1,\chi)}{L(1,\chi)}\right)^{\overline{\chi}(a)}. \tag{5.2.2}$$

The crux of the proof is to use the orthogonality relations between irreducible characters of finite groups to write

$$\prod_{\substack{p \leq x \\ p \equiv a \bmod b}} \left(1 - \frac{1}{p}\right)^{\varphi(b)} = \prod_{\chi} \left[\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{\chi(p)}\right]^{\overline{\chi}(a)}, \tag{5.2.3}$$

where χ ranges over all the irreducible characters of $(\mathbb{Z}/b\mathbb{Z})^\times$. Afterward, he defines an arithmetic function $k_\chi(n)$ for each χ that allows one to factor out the Euler factors of the Dirichlet L-function as follows

$$\left(1 - \frac{1}{p}\right)^{\chi(p)} = \left(1 - \frac{\chi(p)}{p}\right)\left(1 - \frac{k_\chi(p)}{p}\right)^{-1}. \tag{5.2.4}$$

Defining

$$K(s,\chi) := \prod_p K_P(s,\chi) := \prod_p \left(1 - \frac{k_\chi(p)}{p^s}\right)^{-1}, \quad \text{for } \sigma > 0, \tag{5.2.5}$$

the argument then reduces to calculating the asymptotics as $x \to \infty$ of the partial products

$$\prod_{p \le x} L_P(1,\chi)^{-1} \quad \text{and} \quad \prod_{p \le x} K_P(1,\chi).$$

When $\chi = \chi_0$, the calculation follows from Mertens' theorem. For non-trivial characters, the result follows by standard methods. See [Wil74] for additional details.

Back to the general case of an arbitrary Galois extension of number fields E/F, with Galois group G, and $C \subseteq G$ a fixed conjugacy class, essentially the same argument works when all the irreducible representations of G are one dimensional (e.g. the case of abelian extensions). However, for higher dimensional representations, we are led to consider a linear approximation of Artin's L-function, which we call $M(s,\rho)$ for alphabetical reasons.

5.2.2 Rosen's Work

Our goal is now to extend the tools used by Williams to the case of arbitrary Galois extensions. The following theorems of Rosen in [Ros99] gives estimates of analogues of the partial products of $L_P(1,\chi)$ and $\zeta_F(s)$ as above.

Rosen's generalization of Mertens' theorem is analogous to the so called prime ideal theorem, Landau's generalization of the prime number theorem to prime ideals in number fields.

Theorem 5.2.1 (Theorem 2 in [Ros99])**.** *Let $F/\mathbb{Q}$ be an algebraic number field. Then,*

$$\prod_{P \in \Sigma_F(x)} \left(1 - \frac{1}{N(P)}\right) = \frac{e^{-\gamma_F}}{\log x} + O\left(\frac{1}{\log^2 x}\right), \tag{5.2.6}$$

as $x \to \infty$. Furthermore, $\gamma_F = \gamma + \log \varkappa_F$, and the implied constant in the error term depends only on the number field F.

Rosen's proof of Theorem 5.2.1 extends to a general class of Dirichlet series based on F (Theorem 4 in [Ros99]). In particular, he proves a Mertens-type theorem for Artin L-

functions based of F, see [Ros99, Theorem 5]. We reformulate the original statement in the equivalent case of an irreducible representation.

Theorem 5.2.2. *Let E/F be a Galois extension of number fields with Galois group G. Let χ be a non-trivial irreducible character of G. Then,*

$$\prod_{P\in\Sigma_F(x)} L_P(1,\chi)^{-1} = \frac{1}{L(1,\chi)} + O_{\chi,F}\left(\frac{1}{\log x}\right). \tag{5.2.7}$$

Proof. We are specializing [Ros99, Theorem 5] to the case of an irreducible and non trivial character. In Rosen's notation, $\rho = \chi$, $k = 0$, and $\alpha = L(1,\chi)$. □

5.2.3 The M-function

Let $P \in \Sigma_F$, and let ρ be an Artin representation of G. Let

$$f_{\chi,P}(T) := \det\left(I - \rho(\mathrm{Frob}_Q)|_{V^{I_Q}} T\right) \in \mathbb{C}[T] \tag{5.2.8}$$

be the characteristic polynomial of ρ corresponding to P via any Frobenius element. Denote the **trace of Frobenius at** P by

$$\chi(P) := \mathrm{Tr}\,\rho(\mathrm{Frob}_Q)|_{V^{I_Q}} \tag{5.2.9}$$

for any prime $Q \in \Sigma_E$ above $P \in \Sigma_F$. Isolating the linear term, we have

$$f_{\chi,P}(T) = 1 - \chi(P)T + g_{\chi,P}(T)T^2, \tag{5.2.10}$$

where $g_{\chi,P}(T) \in \mathbb{C}[T]$. Factoring out the linear term, we may write

$$f_{\chi,P}(T) = (1-\chi(P)T)\left(1 + \frac{g_{\chi,P}(T)T^2}{1-\chi(P)T}\right) \in \mathbb{C}(T). \tag{5.2.11}$$

Taking the change of variables $T = N(P)^{-s}$, we obtain

$$L_P(s,\chi) = \left(1 - \frac{\chi(P)}{N(P)^s}\right)^{-1}\left(1 + \frac{g_{\chi,P}(N(P)^{-s})}{N(P)^s(N(P)^s - \chi(P))}\right)^{-1},\ \sigma > 1. \tag{5.2.12}$$

Since $-\log_{N(P)}(|T|) = \sigma$, we have $0 < |T| \leq \frac{1}{N(P)} \leq \frac{1}{2}$ when $\sigma \geq 1$. Define

$$\xi_\chi := \sup_{P \in \Sigma_F} \left(\sup_{T \in [0,1/2]} |g_{\chi,P}(T)| \right) \tag{5.2.13}$$

to give an upper bound $g_{\chi,P}(T) \leq \xi_\chi$. This is well defined since $g_{\chi,P}(T)$ depends only on the class of Frob_Q and the set of the $g_{\chi,P}$ is finite.

Definition 5.2.3 (M-function)**.** Given $P \in \Sigma_F$ and ρ and Artin representation of G with character χ, define the M-**Euler factor at** P by

$$M_P(s,\chi) := \left(1 - \frac{\chi(P)}{N(P)^s}\right)^{-1}, \quad \text{for } \sigma > 1. \tag{5.2.14}$$

We define the M-**function** as the Euler product $M(s,\chi) := \prod_{P \in \Sigma_F} M_P(s,\chi)$.

Note that $M(s,\chi)$ defines an holomorphic function in the half plane $\sigma > 1$. When ρ is one dimensional, the polynomial $R_{\chi,P}(T)$ is zero, and in particular $L(s,\chi) = M(s,\chi)$. For higher dimensional representations, this is certainly not the case. We think of $M(s,\chi)$ as a linear approximation of $L(s,\chi)$, at least on the level of local factors.

As a preliminary step in the proof of Theorem 5.1.1, we prove a Mertens-type theorem for $M(s,\chi)$. Though it would be interesting to further explore the analytic properties of $M(s,\chi)$, we restrict ourselves to applications of $M(s,\chi)$ to the proof of the main theorem.

When the representation ρ is one dimensional, $\chi(P)$ is always a root of unity. For higher dimensional representations, $\chi(P)$ is a sum of roots of unity and $|\chi(P)| \leq \chi(1)$. In particular, it may be the case that $\chi(P) = N(P)$. To deal with these technicalities, we restrict to a cofinite subset $\mathcal{S}$ of Σ_F over which this inconvenience disappears. Define

$$\mathcal{S} := \{P \in S_{E/F} : |\chi(P)| < N(P), \text{ for every irreducible character } \chi \text{ of } G\}. \tag{5.2.15}$$

Lemma 5.2.4. *Let E/F be a Galois extension of number fields with Galois group G. Let χ be a non-trivial irreducible character of G and let $\mathcal{S}$ be as in (5.2.15). Then,*

$$\prod_{P \in \mathcal{S}(x)} M_P(1,\chi)^{-1} = \frac{R_{\mathcal{S},\chi} M_{\mathcal{S},\chi}}{L(1,\chi)} + O\left(\frac{1}{\log x}\right), \tag{5.2.16}$$

when $x \to \infty$ and the implied constant in the error term depends on the extension E/F. Furthermore, the constants $R_{\mathcal{S},\chi}$ and $M_{\mathcal{S},\chi}$ are given by

$$R_{\mathcal{S},\chi} = \prod_{P \in \mathcal{S}} R_P(1,\chi)^{-1} \text{ and } M_{\mathcal{S},\chi} = \prod_{P \in \Sigma_F - \mathcal{S}} L_P(1,\chi). \tag{5.2.17}$$

Proof. Factoring the linear term of the characteristic polynomial of Frobenius

$$f_{\chi,P}(T) = (1-\chi(P)T)\left(1 + \frac{g_{\chi,P}(T)T^2}{1-\chi(P)T}\right), \tag{5.2.18}$$

and define,

$$R_P(1,\chi) := \left(1 + \frac{g_{\chi,P}(N(P)^{-1})N(P)^{-2}}{1-\chi(P)N(P)^{-1}}\right) = \left(1 + \frac{g_{\chi,P}(N(P)^{-1})}{N(P)(N(P)-\chi(P))}\right). \tag{5.2.19}$$

Combining (5.2.19) with (5.2.12) and (5.2.14) gives us that

$$L_P(1,\chi) = M_P(1,\chi)R_P(1,\chi)^{-1}. \tag{5.2.20}$$

Taking a product over $P \in \mathcal{S}(x)$ of the above expression, we get

$$\prod_{P \in \mathcal{S}(x)} M_P(1,\chi)^{-1} = \prod_{P \in \mathcal{S}(x)} L_P(1,\chi)^{-1} \prod_{P \in \mathcal{S}(x)} R_P(1,\chi)^{-1}. \tag{5.2.21}$$

We can use Theorem 5.2.2 to understand the product of $L_P(1,\chi)$. Doing so, one sees

$$\begin{aligned}\prod_{P \in \mathcal{S}(x)} L_P(1,\chi)^{-1} &= \prod_{P \in \Sigma_F(x)} L_P(1,\chi)^{-1} \prod_{P \in \Sigma_F(x) - \mathcal{S}(x)} L_P(1,\chi) \\ &= \left(\prod_{P \in \Sigma_F(x) - \mathcal{S}(x)} L_P(1,\chi)\right)\left(\frac{1}{L(1,\chi)} + O_{\chi,F}\left(\frac{1}{\log x}\right)\right)\end{aligned} \tag{5.2.22}$$

What remains is to understand the product over $R_P(1,\chi)^{-1}$, i.e.,

$$\prod_{P \in \mathcal{S}(x)} R_P(1,\chi)^{-1} = \prod_{P \in \mathcal{S}(x)} \left(1 + \frac{g_{\chi,P}(N(P)^{-1})}{N(P)(N(P)-\chi(P))}\right)^{-1}, \tag{5.2.23}$$

and to show the product of $R_P(1,\chi)^{-1}$ over all $P \in \mathcal{S}$ converges, say to

$$R_{\mathcal{S},\chi} := \prod_{P\in\mathcal{S}} R_P(1,\chi)^{-1}.$$

We have, for large enough x,

$$\prod_{P\in\mathcal{S}(x)} R_P(1,\chi)^{-1} = R_{\mathcal{S},\chi} \prod_{N(P)>x} R_P(1,\chi). \tag{5.2.24}$$

To understand the rightmost term above, take logs and expand via Taylor series as follows,

$$\begin{aligned}
\left|\log\left(\prod_{\substack{P\in\mathcal{S}\\N(P)>x}} R_P(1,\chi)\right)\right| &= \left|\sum_{\substack{P\in\mathcal{S}\\N(P)>x}} \log\left(1+\frac{g_{\chi,P}(N(P)^{-1})}{N(P)(N(P)-\chi(P))}\right)\right| \\
&\le \sum_{N(P)>x}\sum_{j=1}^{\infty}\frac{1}{j}\left|\frac{\xi_\chi}{N(P)(N(P)-\chi(P))}\right|^j \\
&\le \sum_{j=1}^{\infty}\frac{1}{j}\left(\sum_{N(P)>x}\frac{\xi_\chi}{N(P)(N(P)-\chi(P))}\right)^j \\
&\le \sum_{j=1}^{\infty}\frac{1}{j}\left(\sum_{N(P)>x} O\left(\frac{1}{N(P)^2}\right)\right)^j = \sum_{j=1}^{\infty}\frac{1}{j}\left(O\left(\frac{1}{x}\right)\right)^j = O\left(\frac{1}{x}\right).
\end{aligned} \tag{5.2.25}$$

Where the first equality in (5.2.25) follows from the prime ideal theorem and partial summation. From (5.2.25) and the Taylor series of the exponential, observe $\exp\left(O\left(\frac{1}{x}\right)\right) = 1 + O\left(\frac{1}{x}\right)$. This is sufficient to establish

$$\prod_{N(P)>x} R_P(1,\chi) = 1 + O\left(\frac{1}{x}\right), \tag{5.2.26}$$

and further

$$\prod_{P\in\mathcal{S}(x)} R_P(1,\chi)^{-1} = R_{\mathcal{S},\chi} + O\left(\frac{1}{x}\right). \tag{5.2.27}$$

Finally, starting from (5.2.21) and substituting in both (5.2.22) and (5.2.27) appropriately suffices to prove the lemma. □

5.2.4 The K-function

In this section, we investigate the analog of Williams' K-function, defined in the case of cyclotomic extensions by (5.2.4) and (5.2.5).

Definition 5.2.5 (K-function)**.** Given $P \in \Sigma_F$ and ρ an Artin representation of G with character χ, define

$$k_\chi(P) := N(P)\left[1 - \left(1 - \frac{\chi(P)}{N(P)}\right)\left(1 - \frac{1}{N(P)}\right)^{-\chi(P)}\right]. \tag{5.2.28}$$

The K-**Euler factor at** P is defined by

$$K_P(s,\chi) := \left(1 - \frac{k_\chi(P)}{N(P)^s}\right)^{-1}, \tag{5.2.29}$$

and we define the K-**function** as the Euler product $K(s,\chi) := \prod_{P\in\Sigma_F} K_P(s,\chi)$.

Note that $|\chi(P)| < N(P)$, so $K_P(1,\chi)$ is well defined and non-zero for every prime $P \in \Sigma_F$.

To prove Theorem 5.1.1 it is enough to restrict the Euler product in the definition of K to the primes in $\mathcal{S}$.

First we show the truncated product $\prod_{P\in\mathcal{S}(x)} K_P(1,\chi)$ converges to $\prod_{P\in\mathcal{S}} K_P(1,\chi)$ quickly, in a precise sense. This is the statement of Lemma 5.2.9. To prove this, we will need some intermediate lemmas. The following lemma is implicit in [Wil74] and will be critical to the analysis of $k_\chi(p)$.

Lemma 5.2.6. *Let a, b be complex numbers such that $|a/b| < 1$ and $b \geq 2$. Then,*

$$b\left[1 - \left(1 - \frac{a}{b}\right)\left(1 - \frac{1}{b}\right)^{-a}\right] = \frac{a(a-1)}{b}\left[\frac{1}{2} + \sum_{n=1}^{\infty} \frac{(a+1)\cdots(a+n)}{b^n(n+1)!}\frac{n+1}{n+2}\right]. \tag{5.2.30}$$

While we omit the details of the proof of Lemma 5.2.6, we comment that it follows from writing the left hand side as a doubly infinite series. We can then rearrange this series into a power series in $\frac{1}{b}$, then use induction to show that the coefficients take the desired form. The key application of Lemma 5.2.6 is the following estimate.

Lemma 5.2.7. *Let χ be a d-dimensional irreducible character of G. Then for all $P \in \mathcal{S}$,*

$$|k_\chi(P)| \leq \frac{d(d+1)}{2}\frac{1}{N(P)} + \frac{C_d}{N(P)^2} \tag{5.2.31}$$

for some constant $C_d > 0$ depending only on d.

Proof. Fix $P \in \mathcal{S}$. The conditions of Lemma 5.2.6 are satisfied for $a = \chi(P)$ and $b = N(P)$. Noting that $|\chi(P)| \leq d$, we have

$$\begin{aligned}
|k_\chi(P)| &= \left| \frac{\chi(P)(\chi(P)-1)}{N(P)} \left[\frac{1}{2} + \sum_{n=1}^{\infty} \frac{(\chi(P)+1)\cdots(\chi(P)+n)}{N(P)^n (n+1)!} \frac{n+1}{n+2} \right] \right| \\
&\leq \frac{d(d+1)}{2}\frac{1}{N(P)} + \frac{d(d+1)}{N(P)^2} \sum_{n=0}^{\infty} \frac{(n-1+d)!}{d!\; n!} \frac{1}{N(P)^n} \\
&\leq \frac{d(d+1)}{2}\frac{1}{N(P)} + \left(\frac{d(d+1)}{d!} \sum_{n=0}^{\infty} \frac{(n-1+d)!}{n!} \frac{1}{2^n} \right) \frac{1}{N(P)^2}.
\end{aligned}$$

The constant C_d is given by the expression inside the big parenthesis in the last inequality,

$$C_d = \frac{d(d+1)}{d!} \sum_{n=0}^{\infty} \frac{(n-1+d)!}{n!} \frac{1}{2^n}. \tag{5.2.32}$$

To determine the convergence of the series, it is enough to notice that $(n-1+d)!/n!$ is a polynomial of degree $d-1$ in n. □

Combining the estimate of Lemma 5.2.7 with the prime ideal theorem, we have the following estimate on the tail of the infinite sum of $|k_\chi(P)|/N(P)$ over primes $P \in \mathcal{S}$.

Lemma 5.2.8. *Let $x > 0$. Then*

$$\sum_{\substack{P \in \mathcal{S} \\ N(P) > x}} \frac{|k_\chi(P)|}{N(P)} = O\left(\frac{1}{x}\right)$$

where the implied constant depends on the extension E/F.

Proof. Notice that when x is sufficiently large, all primes P with norm $N(P) > x$ are contained in $\mathcal{S}$. This allows us to drop the requirement in the summation that $P \in \mathcal{S}$.

By (5.2.31) we have

$$\sum_{N(P)>x} \frac{|k_\chi(P)|}{N(P)} \leq \frac{d^2+d}{2} \sum_{N(P)>x} \frac{1}{N(P)^2} + C_d \sum_{N(P)>x} \frac{1}{N(P)^3}$$

for the constant C_d depending on the dimension of the representation associated to χ given above in (5.2.32). Of course, $1/N(P)^3 < 1/N(P)^2$, so it suffices to show that $\sum_{N(P)>x} \frac{1}{N(P)^2} = O(1/x)$. This follows from the same argument as in (5.2.25). □

Lemma 5.2.9. *Let E/F be a Galois extension of number fields with Galois group G. Let χ be a non-trivial irreducible character of G, and let $\mathcal{S}$ be as defined in (5.2.15). Then*

$$\prod_{P\in\mathcal{S}(x)} K_P(1,\chi) = K_{\mathcal{S},\chi} + O\left(\frac{1}{x}\right), \tag{5.2.33}$$

when $x \to \infty$ and the implied constant depends on the extension E/F. Furthermore, the constant $K_{\mathcal{S},\chi}$ is given by

$$K_{\mathcal{S},\chi} := \prod_{P\in\mathcal{S}} K_P(1,\chi). \tag{5.2.34}$$

Proof. The set $\mathcal{S}$ as defined in (5.2.15) provides that $|\chi(P)| < N(P)$, so for all $P \in \mathcal{S}$, we can see by (5.2.28) that $k_\chi(P) \neq N(P)$, and hence by (5.2.29) the local factor $K_P(1,\chi)$ is both well defined and nonzero. Our goal is thus to show that the infinite product $K_{\mathcal{S},\chi}$ converges and that the truncation $\prod_{P\in\mathcal{S}(x)} K_P(1,\chi)$ converges to it with the error term $O_F\left(\frac{1}{x}\right)$.

Taking logarithms, the limit of

$$\log\left(\prod_{P\in\mathcal{S}(x)} K_P(1,\chi)\right) = -\sum_{P\in\mathcal{S}(x)} \log\left(1-\frac{k_\chi(P)}{N(P)}\right)$$

converges as $x \to \infty$. To see this, and obtain the desired asymptotic, it suffices to estimate the tail

$$\left|\sum_{\substack{P\in\mathcal{S}\\ N(P)>x}} \log\left(1-\frac{k_\chi(P)}{N(P)}\right)\right|.$$

For x sufficiently large, all primes of sufficiently large norm are in $\mathcal{S}$, so it suffices to estimate

this tail for all $N(P) > x$. Taking absolute values and using the Taylor series expansion, which is valid since $P \in \mathcal{S}$, we have

$$\begin{aligned}\left|\sum_{N(P)>x} \log\left(1-\frac{k_\chi(P)}{N(P)}\right)\right| &\leq \sum_{N(P)>x}\left|\sum_{j=1}^{\infty}\frac{1}{j}\left(\frac{k_\chi(P)}{N(P)}\right)^j\right| \\ &\leq \sum_{N(P)>x}\sum_{j=1}^{\infty}\frac{1}{j}\left(\frac{|k_\chi(P)|}{N(P)}\right)^j \\ &\leq \sum_{j=1}^{\infty}\frac{1}{j}\sum_{N(P)>x}\left(\frac{|k_\chi(P)|}{N(P)}\right)^j \\ &\leq \sum_{j=1}^{\infty}\frac{1}{j}\left(\sum_{N(P)>x}\frac{|k_\chi(P)|}{N(P)}\right)^j = \sum_{j=1}^{\infty}\frac{1}{j}O_F\left(\frac{1}{x}\right)^j.\end{aligned}$$

The last equality follows from Lemma 5.2.8. As in (5.2.25), this suffices to establish $\prod_{N(P)>x} K_P(1,\chi) = 1 + O\left(\frac{1}{x}\right)$, completing the proof of (5.2.33). □

5.3 Proof of Theorem 5.1.1

In this section we will first prove the content of Theorem 5.1.1 and then show an alternative determination of the constant following a method shown in [LZ07, §6].

5.3.1 Proof of the main theorem

The starting point of our proof is the same as that of Williams, namely, the orthogonality relations for irreducible characters of finite groups. Given a fixed conjugacy class C of G, and an unramified prime $P \in S_{E/F}$, we have

$$\sum_{\chi}\chi(P)\overline{\chi}(C) = \begin{cases}\frac{\#G}{\#C}, & \text{if } C = \mathrm{Frob}_P, \\ 0, & \text{if } C \neq \mathrm{Frob}_P\,.\end{cases} \tag{5.3.1}$$

This leads to the natural generalization of Equation (5.2.3).

$$\prod_{P\in S_C(x)}\left(1-\frac{1}{N(P)}\right)^{\#G/\#C} = \prod_{\chi}\left[\prod_{P\in S_{E/F}(x)}\left(1-\frac{1}{N(P)}\right)^{\chi(P)}\right]^{\overline{\chi}(C)}. \tag{5.3.2}$$

When $\chi = \chi_0$ is the trivial character, Rosen's theorem (Theorem 5.2.1) yields

$$\prod_{P \in S_{E/F}(x)} \left(1 - \frac{1}{N(P)}\right) = \frac{N(\Delta)}{\varphi(\Delta)} \frac{e^{-\gamma_F}}{\log x} + O_F\left(\frac{1}{\log^2 x}\right). \tag{5.3.3}$$

When $\chi \neq \chi_0$, we first split the product as follows

$$\prod_{P \in S_{E/F}(x)} \left(1 - \frac{1}{N(P)}\right)^{\chi(P)} = \prod_{P \in S_{E/F}(x) - \mathcal{S}(x)} \left(1 - \frac{1}{N(P)}\right)^{\chi(P)} \prod_{P \in \mathcal{S}(x)} \left(1 - \frac{1}{N(P)}\right)^{\chi(P)}. \tag{5.3.4}$$

Call $B_{\mathcal{S},\chi}$ the constant given by the product over the primes $P \in S_{E/F} - \mathcal{S}$ in the right hand side of (5.3.4). For every $P \in \mathcal{S}$ we are able to factor out $M_P(1,\chi)$ from the expression, obtaining

$$\prod_{P \in \mathcal{S}(x)} \left(1 - \frac{1}{N(P)}\right)^{\chi(P)} = \prod_{P \in \mathcal{S}(x)} M_P(1,\chi)^{-1} \prod_{P \in \mathcal{S}(x)} K_P(1,\chi) \tag{5.3.5}$$

$$= \left[\frac{R_{\mathcal{S},\chi} M_{\mathcal{S},\chi}}{L(1,\chi)} + O\left(\frac{1}{\log x}\right)\right] \left[K_{\mathcal{S},\chi} + O\left(\frac{1}{x}\right)\right] \tag{5.3.6}$$

$$= \frac{R_{\mathcal{S},\chi} M_{\mathcal{S},\chi} K_{\mathcal{S},\chi}}{L(1,\chi)} + O\left(\frac{1}{\log x}\right). \tag{5.3.7}$$

The equality in (5.3.6) follows from applying Lemma 5.2.4 and Lemma 5.2.9. Again, the constants only depend on the extension E/F. Assembling the pieces together, we get the desired result.

Finally, the constant $-\gamma(E/F, C)$ is defined by the equality

$$e^{-\gamma(E/F,C)} = \frac{N(\Delta)}{\varphi(\Delta)} \prod_{\chi \neq \chi_0} \left(\frac{B_{\mathcal{S},\chi} R_{\mathcal{S},\chi} M_{\mathcal{S},\chi} K_{\mathcal{S},\chi}}{L(1,\chi)}\right)^{\overline{\chi}(C)} e^{-\gamma_F}. \tag{5.3.8}$$

Note that the constants $B_{\mathcal{S},\chi}$ and $M_{\mathcal{S},\chi}$ are easily computed finite products. To obtain a numerical value for $e^{-\gamma(E/F,C)}$ for a given, E/F and $C \subset G$, one would need to compute these along with the infinite products $R_{\mathcal{S},\chi}$, $K_{\mathcal{S},\chi}$, and the L-function $L(1,\chi)$ for each nontrivial character χ of G.

5.3.2 An alternative determination of the constant

Languasco and Zaccagnini observed in [LZ07] that the orthogonality relations of finite group characters can also be used to provide a cleaner formula for the constant $e^{-\gamma(a,b)}$ appearing in Williams' theorem. Their method extends to this setting as well, and we record it here for completeness.

First, note

$$\lim_{x\to\infty} \prod_{P\in S_{E/F}(x)} \left(1-\frac{1}{N(P)}\right)^{\chi(P)} = \frac{K(1,\chi)}{L(1,\chi)}.$$

Thus, from (5.3.8),

$$\begin{aligned} e^{-\gamma(E/F,C)} &= e^{-\gamma_F}\frac{N(\Delta)}{\varphi(\Delta)} \lim_{x\to\infty} \prod_{\chi\neq\chi_0} \prod_{P\in S_{E/F}(x)} \left(1-\frac{1}{N(P)}\right)^{\chi(P)\overline{\chi(C)}} \\ &= e^{-\gamma_F}\frac{N(\Delta)}{\varphi(\Delta)} \lim_{x\to\infty} \prod_{P\in S_{E/F}(x)} \left(1-\frac{1}{N(P)}\right)^{\sum_{\chi\neq\chi_0}\chi(P)\overline{\chi(C)}} \\ &= e^{-\gamma_F} \lim_{x\to\infty} \prod_{P\in \Sigma_{E/F}(x)} \left(1-\frac{1}{N(P)}\right)^{\alpha(E/F,C;P)} \\ &= e^{-\gamma_F} \prod_{P\in \Sigma_F} \left(1-\frac{1}{N(P)}\right)^{\alpha(E/F,C;P)} \end{aligned} \tag{5.3.9}$$

where, using character orthogonality (5.3.1),

$$\alpha(E/F,C;P) = \begin{cases} -1, & P \mid \Delta, \\ \frac{\#G}{\#C}-1, & \mathrm{Frob}_P = C, \\ -1, & \mathrm{Frob}_P \neq C. \end{cases}$$

and (5.3.9) follows from the product formula of the Euler totient function

$$\frac{\varphi(\Delta)}{N(\Delta)} = \prod_{P\mid\Delta}\left(1-\frac{1}{N(P)}\right).$$

This calculation is sufficient to prove (5.1.7) of Theorem 5.1.1.

5.4 Examples

5.4.1 Quadratic extensions

Set $F = \mathbb{Q}$ and let $E = \mathbb{Q}(\sqrt{D})$, with D square-free, be a quadratic extension of $\mathbb{Q}$.

Corollary 5.4.1. *Let $E/\mathbb{Q}$ be a quadratic extension of discriminant Δ. Then*

$$\prod_{\substack{\left(\frac{D}{p}\right)=\pm 1 \\ p \le x}} \left(1 - \frac{1}{p}\right) = \left(\frac{\Delta}{\varphi(\Delta)} \frac{e^{-\gamma}}{\log x} \prod_{p \nmid \Delta} \left(1 - \frac{1}{p}\right)^{\pm\left(\frac{D}{p}\right)}\right)^{1/2} + O\left(\frac{1}{(\log x)^{3/2}}\right),$$

where $\gamma = \gamma_{\mathbb{Q}}$ is the usual Euler constant.

In this case, $G = \mathrm{Gal}(E/\mathbb{Q}) \cong \{\pm 1\}$, so there is one nontrivial conjugacy class $\{-1\} \subseteq G$, consisting of the inert primes in $\mathcal{O}_E$, while the trivial class corresponds to the split primes. Our two characters are the trivial character, χ_0, and the nontrivial character

$$\chi_1(p) = \begin{cases} 1, & \text{if } p \text{ is split,} \\ -1, & \text{if } p \text{ is inert.} \end{cases}$$

This is precisely the quadratic residue symbol, $\chi_1(p) = \left(\frac{D}{p}\right)$, which in our notation also coincides with Frob_p.

Following the algorithm implicit in the proof of the main theorem (§5.3.1), we have $|\chi_i(p)| = 1 < p$ for both $i = 0, 1$ and all primes p, so $\mathcal{S} = S_{E/\mathbb{Q}}$ is precisely the set of unramified primes.

First consider the case where $C = \{1\}$. By (5.3.2) and (5.3.3) we have

$$\prod_{\substack{\left(\frac{D}{p}\right)=1 \\ p \le x}} \left(1 - \frac{1}{p}\right)^2 = \frac{\Delta}{\varphi(\Delta)} \frac{e^{-\gamma}}{\log x} \prod_{p \nmid \Delta} \left(1 - \frac{1}{p}\right)^{\left(\frac{D}{p}\right)} + O\left(\frac{1}{\log^3 x}\right),$$

where γ is the usual Euler constant. Taking square roots, we have

$$\prod_{\substack{\left(\frac{D}{p}\right)=1 \\ p \le x}} \left(1-\frac{1}{p}\right) = \left(\frac{\Delta}{\varphi(\Delta)}\frac{e^{-\gamma}}{\log x}\prod_{p\nmid\Delta}\left(1-\frac{1}{p}\right)^{\left(\frac{D}{p}\right)}\right)^{1/2} + O\left(\frac{1}{\log^{3/2} x}\right).$$

If we took $C = \{-1\}$, then we find

$$\prod_{\substack{\left(\frac{D}{p}\right)=-1 \\ p \le x}} \left(1-\frac{1}{p}\right) = \left(\frac{\Delta}{\varphi(\Delta)}\frac{e^{-\gamma}}{\log x}\prod_{p\nmid\Delta}\left(1-\frac{1}{p}\right)^{-\left(\frac{D}{p}\right)}\right)^{1/2} + O\left(\frac{1}{\log^{3/2} x}\right).$$

Using Theorem 5.1.1 (5.1.7) we obtain the exact same formula for the constant.

5.4.2 Primes represented by quadratic forms

Let

$$Q(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y],$$

be a binary integral quadratic form. Assume that Q is primitive, irreducible, and positive definite. That is, a and c are positive integers with $\gcd(a,b,c) = 1$, $D = b^2 - 4ac$ is not a square, and $D < 0$. An integer n is said to be represented by Q if there exist integers x and y such that $Q(x,y) = n$.

Denote by $\mathcal{Q}$ the set of rational primes represented by Q.

Corollary 5.4.2. *Let Q be a primitive, irreducible, positive definite, and integral binary quadratic form with discriminant D, and let E be the ring class field of the order of D. Then,*

$$\prod_{p\in\mathcal{Q}(x)} \left(1-\frac{1}{p}\right) = \left(\frac{e^{-\gamma(E/\mathbb{Q},\mathcal{C})}}{\log x}\right)^{\frac{\#C}{2h(D)}} \prod_{\substack{p\,|\,\Delta_E \\ p\in\mathcal{Q}}} \left(1-\frac{1}{p}\right) + O\left(\frac{1}{(\log x)^{1+\frac{\#C}{2h(D)}}}\right), \tag{5.4.1}$$

where $C \subset \mathrm{Gal}(E/\mathbb{Q})$ is the conjugacy class corresponding to Q via class field theory, and $h(D)$ is the class number of $\mathbb{Q}(\sqrt{D})$.

Proof. By class field theory and the theory of quadratic forms, see for example [Cox13,

Chapter 9], the class $[Q]$ corresponds to an element $\sigma_0 \in \mathrm{Gal}(E/\mathbb{Q}(\sqrt{D})) \subseteq \mathrm{Gal}(E/\mathbb{Q})$. Therefore, the class C is the $\mathrm{Gal}(E/\mathbb{Q})$-conjugacy class of σ_0. The result follows by noting that $\mathcal{Q} - \mathcal{C}$ is the finite set of primes ramified in L that are represented by Q. In particular

$$\delta(\mathcal{C}) = \delta(\mathcal{Q}) = \begin{cases} \frac{1}{2h(D)}, & \text{if } Q \text{ is equivalent to its opposite.} \\ \frac{1}{h(D)}, & \text{otherwise.} \end{cases}$$

The relation between $\mathcal{C}$ and $\mathcal{Q}$ is made explicit in the proof of [Cox13, Theorem 9.12] using the ring class field as described in [Cox13, §9.A]. □

5.4.3 General abelian extensions

In the special case the Galois group G is abelian, all irreducible representations are one-dimensional. In particular, the trace of Frobenius is a root of unity, and as such it has absolute value strictly smaller that the norm of every prime. In our notation, this means $\mathcal{S} = S_{E/F}$. Moreover, the Artin L-function coincides with the M-function, and we have the following corollary.

Corollary 5.4.3. *Let E/F be an abelian Galois extension of number fields, with Galois group G, and let $g \in G$ be any element. Then,*

$$\prod_{\substack{P \in S_{E/F}(x) \\ \mathrm{Frob}_P = g}} \left(1 - \frac{1}{N(P)}\right) = \left(\frac{e^{-\gamma(E/F,g)}}{\log x}\right)^{1/[E:F]} + O\left(\frac{1}{(\log x)^{1+1/[E:F]}}\right) \tag{5.4.2}$$

when $x \to \infty$ and the implied constant depends on the extension E/F. Furthermore, the constant $\gamma(E/F, g)$ is given by

$$\begin{aligned} e^{-\gamma(E/F,g)} &= e^{-\gamma_F} \frac{N(\Delta)}{\varphi(\Delta)} \prod_{\chi \neq \chi_0} \left(\prod_{P \nmid \Delta} \frac{K_P(1,\chi)}{L_P(1,\chi)}\right)^{\overline{\chi}(g)} \\ &= e^{-\gamma_F} \frac{N(\Delta)}{\varphi(\Delta)} \prod_{\substack{P \\ \mathrm{Frob}_P = g}} \left(1 - \frac{1}{N(P)}\right)^{[E:F]-1} \prod_{\substack{P \\ \mathrm{Frob}_P \neq g}} \left(1 - \frac{1}{N(P)}\right)^{-1}. \end{aligned}$$

5.4.4 Sextic S_3-extensions

Finally, we consider the case when $E/\mathbb{Q}$ sextic S_3-extension. We denote the three conjugacy classes of G by the identity class C_1, the class of transpositions C_2, and the class of 3-cycles C_3. The three irreducible characters χ_0, χ_1, χ_2 are given by the character table in Figure 5.4.1.

	C_1	C_2	C_3
χ_0	1	1	1
χ_1	1	-1	1
χ_2	2	0	-1

Figure 5.4.1: The character table for S_3

It is clear from the table that for all *odd* primes p, we have $|\chi(p)|< p$, so all odd unramified primes are contained in $\mathcal{S}$. For the even prime, $2 \notin \mathcal{S}$ if (i) it is ramified or (ii) if it is unramified and $\chi(2) = 2$ for some χ. From Figure 5.4.1, (ii) can only occur for χ_2 in the case where Frob_2 is the identity class, i.e., precisely when 2 is totally split in E. This condition does occur, for example it happens with $p = 2$ in the case where E is the splitting field of $x^6 - 2x^5 - 14x^3 + 123x^2 - 208x + 164$ over $\mathbb{Q}$ [LMF21, Number field 6.0.80062991.1].

This allows us to compute $B_{\mathcal{S},\chi}$:

$$B_{\mathcal{S},\chi} = \prod_{p \in S_{E/\mathbb{Q}} - \mathcal{S}} \left(1 - \frac{1}{N(P)}\right)^{\chi(P)} = \begin{cases} \frac{1}{2^{\chi(2)}}, & \text{if 2 is unramified and } \mathrm{Frob}_2 = C_1, \\ 1, & \text{otherwise.} \end{cases} \tag{5.4.3}$$

Similarly we can compute $M_{\mathcal{S},\chi}$:

$$\begin{aligned} M_{\mathcal{S},\chi} &= \prod_{p \in \Sigma_{\mathbb{Q}} - \mathcal{S}} L_p(1,\chi) \\ &= \begin{cases} L_2(1,\chi) \prod_{p|\Delta} L_p(1,\chi), & \text{if 2 is unramified and } \mathrm{Frob}_2 = C_1, \\ \prod_{p|\Delta} L_p(1,\chi), & \text{otherwise.} \end{cases} \end{aligned} \tag{5.4.4}$$

From the definition of $k_\chi(p)$ in (5.2.28), we have

$$k_\chi(p) = \begin{cases} 0, & \text{if } \chi(p) = 0 \text{ or } \chi(p) = 1, \\ 1/p, & \text{if } \chi(p) = -1, \\ p/(p-1)^2, & \text{if } \chi(p) = 2. \end{cases}$$

This allows us to produce $K(1,\chi)$ for $\chi = \chi_1, \chi_2$ according to (5.2.29):

$$K(1,\chi_1) = \prod_{\mathrm{Frob}_p = C_2} \left(1 - \frac{1}{p^2}\right)^{-1}$$
$$K(1,\chi_2) = \prod_{\mathrm{Frob}_p = C_1} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{\mathrm{Frob}_p = C_3} \left(1 - \frac{1}{p^2}\right)^{-1}$$

It remains to describe L and $R_{\mathcal{S},\chi}$. Since $\chi = \chi_1$ is one dimensional, we have $L_p(s,\chi) = M_p(s,\chi)$ and $R_{\mathcal{S},\chi_1} = 1$. On the other hand, χ_2 is two dimensional, and as such $R_{\mathcal{S},\chi_2}$ is nontrivial. Thus, if 2 is not totally split $E/\mathbb{Q}$, we may use (5.4.3) and (5.4.4) to give a more explicit description of $e^{-\gamma(E/\mathbb{Q},C)}$ given in (5.3.8):

$$e^{-\gamma(E/\mathbb{Q},C_1)} = e^{-\gamma}\frac{N(\Delta)}{\varphi(\Delta)} \left(\prod_{p \nmid \Delta} L_p(1,\chi_1) \prod_{\mathrm{Frob}_p = C_2} \left(1 - \frac{1}{p^2}\right)^{-1} \right) \times$$
$$\left(R_{\mathcal{S},\chi_2} \prod_{p \nmid \Delta} L_p(1,\chi_2)^{-1} \prod_{\mathrm{Frob}_p = C_1} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{\mathrm{Frob}_p = C_3} \left(1 - \frac{1}{p^2}\right)^{-1} \right)^2,$$
$$e^{-\gamma(E/\mathbb{Q},C_2)} = e^{-\gamma}\frac{N(\Delta)}{\varphi(\Delta)} \prod_{p \nmid \Delta} L(1,\chi_1) \prod_{\mathrm{Frob}_p = C_2} \left(1 - \frac{1}{p^2}\right),$$
$$e^{-\gamma(E/\mathbb{Q},C_3)} = e^{-\gamma}\frac{N(\Delta)}{\varphi(\Delta)} \left(\prod_{p \nmid \Delta} L_p(1,\chi_1)^{-1} \prod_{\mathrm{Frob}_p = C_2} \left(1 - \frac{1}{p^2}\right)^{-1} \right) \times$$
$$\left(\frac{\prod_{p \nmid \Delta} L_p(1,\chi_2)}{R_{\mathcal{S},\chi_2}} \prod_{\mathrm{Frob}_p = C_1} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\mathrm{Frob}_p = C_3} \left(1 - \frac{1}{p^2}\right) \right).$$

If 2 is unramified and totally split in E, these can be modified by taking $B_{\mathcal{S},\chi}$ and $M_{\mathcal{S},\chi}$ as in (5.4.3) and (5.4.4). One could use Theorem 5.1.1 (5.1.7) for an alternate determination of the constants $e^{-\gamma(E/\mathbb{Q},C_i)}$ above.

5.4.5 Future work

We suspect our methods can be extended to the case of global function fields in a straightforward manner. More generally, it would be interesting to consider the case of varieties over finite fields, by using Lebaque's [Leb07] generalization of Mertens' theorem in place of Rosen's theorem (Theorem 5.2.1).

Theorem 5.4.4 ([Leb07, Theorem 5])**.** *Let X be a smooth, projective, and geometrically irreducible variety of dimension d defined over a finite field $\mathbb{F}_q$. Call $\varkappa_X$ the residue of the Weil zeta function $\zeta_X(s)$ at $s = d$. Then*

$$\prod_{\deg P \leq N} \left(1 - \frac{1}{N(P)^d}\right) = \frac{e^{-\gamma_X}}{N} + O\left(\frac{1}{N^2}\right), \tag{5.4.5}$$

where the product runs over the closed points $P \in X$ and $\gamma_X = \gamma + \log(\varkappa_X \log q)$.

Bibliography

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[AGH+22] Theresa C. Anderson, Ayla Gafni, Kevin Hughes, Robert J. Lemke Oliver, David Lowry-Duda, Frank Thorne, Jiuya Wang, and Ruixiang Zhang. Improved bounds on number fields of small degree. Preprint available at https://arxiv.org/abs/2204.01651, 2022.

[AH91] Dan Abramovich and Joe Harris. Abelian varieties and curves in $W_d(C)$. *Compositio Math.*, 78(2):227–238, 1991.

[Alb21] Brandon Alberts. Statistics of the first Galois cohomology group: a refinement of Malle's conjecture. *Algebra Number Theory*, 15(10):2513–2569, 2021.

[APnKK22] Santiago Arango-Piñeros, Daniel Keliher, and Christopher Keyes. Mertens' theorem for Chebotarev sets. *Int. J. Number Theory*, 18(8):1823–1842, 2022.

[Aru20] Vishal Arul. *Explicit Division and Torsion Points on Superelliptic Curves and Jacobians*. PhD thesis, Massachusetts Institute of Technology, 2020.

[Aru21] Vishal Arul. Division by $1-\zeta$ on superelliptic curves and Jacobians. *Int. Math. Res. Not. IMRN*, 2021(4):3143–3185, 2021.

[ASVW21] S. Ali Altuğ, Arul Shankar, Ila Varma, and Kevin H. Wilson. The number of

D_4-fields ordered by conductor. *J. Eur. Math. Soc. (JEMS)*, 23(8):2733–2785, 2021.

[BBL16] M. J. Bright, T. D. Browning, and D. Loughran. Failures of weak approximation in families. *Compos. Math.*, 152(7):1435–1475, 2016.

[BCF16] Manjul Bhargava, John Cremona, and Tom Fisher. The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point. *Int. J. Number Theory*, 12(4):1077–1092, 2016.

[BCF21] Manjul Bhargava, John Cremona, and Tom Fisher. The proportion of genus one curves over $\mathbb{Q}$ defined by a binary quartic that everywhere locally have a point. *Int. J. Number Theory*, 17(4):903–923, 2021.

[BCFG22] Manjul Bhargava, John Cremona, Tom Fisher, and Stevan Gajović. The density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$. *Proceedings of the London Mathematical Society*, 124(5):713–736, 2022.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BEL+19] Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray. On the level of modular curves that give rise to isolated j-invariants. *Adv. Math.*, 357:106824, 33, 2019.

[BF] Mohammad Bardestani and Tristan Freiberg. Mertens's theorem for splitting primes and more. Preprint available at https://arxiv.org/abs/1309.7482.

[BGRW20] Abbey Bourdon, David Gill, Jeremy Rouse, and Lori Watson. Odd degree isolated points on $X_1(N)$ with rational j-invariant. Preprint available at https://arXiv.org/abs/2006.14966, 2020.

[BGW17] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any

odd degree extension. *J. Amer. Math. Soc.*, 30(2):451–493, 2017. With an appendix by Tim Dokchitser and Vladimir Dokchitser.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[Bha10] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[BK21a] Lea Beneish and Christopher Keyes. Fields generated by points on superelliptic curves. Preprint available at https://arxiv.org/abs/2103.16672, 2021.

[BK21b] Lea Beneish and Christopher Keyes. Github repository *Density-of-locally-soluble-SECs*. Available at https://github.com/c-keyes/Density-of-locally-soluble-SECs, 2021.

[BK23] Lea Beneish and Christopher Keyes. On the proportion of locally soluble superelliptic curves. *Finite Fields and Their Applications*, 85:102128, 2023.

[BN15] Peter Bruin and Filip Najman. Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields. *LMS J. Comput. Math.*, 18(1):578–602, 2015.

[Box21] Josha Box. Quadratic points on modular curves with infinite Mordell-Weil group. *Math. Comp.*, 90(327):321–343, 2021.

[Bro17] T. D. Browning. Many cubic surfaces contain rational points. *Mathematika*, 63(3):818–839, 2017.

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[BSW22] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. An improvement on schmidt's bound on the number of number fields of bounded discriminant

and small degree. Preprint available at https://arxiv.org/abs/2204.01331, 2022.

[Cha41] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Con] Keith Conrad. Factoring after dedekind. Expository paper, available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[Cox13] David Cox. *Primes of the Form $x^2 + ny^2$*. Pure and Applied Mathematics. John Wiley & Sons, second edition, 2013.

[Cre13] Brendan Creutz. Explicit descent in the Picard group of a cyclic cover of the projective line. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 295–315. Math. Sci. Publ., Berkeley, CA, 2013.

[DEvH+21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021.

[DF93] Olivier Debarre and Rachid Fahlaoui. Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves. *Compositio Math.*, 88(3):235–249, 1993.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[EH21] Jordan S. Ellenberg and Daniel Rayor Hast. Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty. *Int. Math. Res. Not. IMRN*, 2022(19):14770–14796, 2021.

[Eke91] Torsten Ekedahl. An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.*, 40(1):53–59, 1991.

[EV06] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Fal94] Gerd Faltings. The general case of S. Lang's conjecture. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 175–182. Academic Press, San Diego, CA, 1994.

[FHP21] Tom Fisher, Wei Ho, and Jennifer Park. Everywhere local solubility for hypersurfaces in products of projective spaces. *Res. Number Theory*, 7(1):Paper No. 6, 27, 2021.

[Fuj16] Matsusaburô Fujiwara. Uber die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung. *Tôhoku Math. J.*, 10:167–171, 1916.

[GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2008. Reprint of the 1994 edition.

[GL22] Stephan Ramon Garcia and Ethan Simpson Lee. Unconditional explicit Mertens' theorems for number fields and Dedekind zeta residue bounds. *Ramanujan J.*, 57(3):1169–1191, 2022.

[GLL13] Ofer Gabber, Qing Liu, and Dino Lorenzini. The index of an algebraic variety. *Invent. Math.*, 192(3):567–626, 2013.

[GM19] Joseph Gunther and Jackson S. Morrow. Irrational points on hyperelliptic curves. Preprint available at https://arxiv.org/abs/1709.02041, 2019.

[Gui18] Pierre Guillot. *A gentle course in local class field theory*. Cambridge University Press, Cambridge, 2018. Local number fields, Brauer groups, Galois cohomology.

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

[HS91] Joe Harris and Joe Silverman. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.*, 112(2):347–356, 1991.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Key22] Christopher Keyes. Growth of points on hyperelliptic curves over number fields. *Journal de théorie des nombres de Bordeaux*, 34(1):271–294, 2022.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[Kim09] Minhyong Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Leb07] Philippe Lebacque. Generalised Mertens and Brauer-Siegel theorems. *Acta Arithmetica*, 130(4):333–350, 2007.

[LMF21] The LMFDB Collaboration. Number field 6.0.80062991.1. https://www.lmfdb.org/NumberField/6.0.80062991.1, 2021.

[LT21] Robert J. Lemke Oliver and Frank Thorne. Rank growth of elliptic curves in non-abelian extensions. *Int. Math. Res. Not. IMRN*, 2021(24):18411–18441, 2021.

[LT22] Robert J. Lemke Oliver and Frank Thorne. Upper bounds on number fields of given degree and bounded discriminant. *Duke Mathematical Journal*, 171(15):3077 – 3087, 2022.

[LZ07] Alessandro Languasco and Alessandro Zaccagnini. A note on Mertens' formula for arithmetic progressions. *Journal of Number Theory*, 127:37–46, 2007.

[Mat10] Richard J. Mathar. Table of Dirichlet L-series and prime zeta modulo functions for small moduli. Preprint available at https://arxiv.org/abs/1008.2547, 2010.

[Mer74] Franz Mertens. Ein beitrag zur analytischen zahlentheorie. *J. reine angew. Math.*, 78:46–62, 1874.

[Mil20] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[MM12] M. Ram Murty and V. Kumar Murty. *Non-vanishing of L-functions and Applications*. Springer, Basel, 2012.

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[MR18] Barry Mazur and Karl Rubin. Diophantine stability. *Amer. J. Math.*, 140(3):571–616, 2018. With an appendix by Michael Larsen.

[MS15] Diane Maclagan and Bernd Sturmfels. *Introduction to tropical geometry*, volume 161 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2015.

[MV06] Hugh Montgomery and Robert Vaughan. *Multiplicative Number Theory*. Number 97 in Cambridge studies in advanced mathematics. Cambridge University Press, 2006.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[OS19] Ekin Ozman and Samir Siksek. Quadratic points on modular curves. *Math. Comp.*, 88(319):2461–2484, 2019.

[Osa87] Hiroyuki Osada. The Galois groups of the polynomials X^n+aX^l+b. *J. Number Theory*, 25(2):230–238, 1987.

[OU15] Thomas Occhipinti and Douglas Ulmer. Low-dimensional factors of superelliptic Jacobians. *Eur. J. Math.*, 1(2):279–285, 2015.

[PS99a] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[PS99b] Bjorn Poonen and Michael Stoll. A local-global principle for densities. In *Topics in number theory (University Park, PA, 1997)*, volume 467 of *Math. Appl.*, pages 241–244. Kluwer Acad. Publ., Dordrecht, 1999.

[PS14] Bjorn Poonen and Michael Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.

[PV04] Bjorn Poonen and José Felipe Voloch. Random Diophantine equations. In *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, volume 226 of *Progr. Math.*, pages 175–184. Birkhäuser Boston, Boston, MA, 2004. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz.

[Ros99] Michael Rosen. A generalization of Mertens' theorem. *Journal of the Ramanujan Mathematical Society*, 14:1–20, 1999.

[Sag21] Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2021. `https://www.sagemath.org`.

[Sch95] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. *Astérisque*, (228):189–195, 1995. Columbia University Number Theory Seminar (New York, 1992).

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem.* Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated

from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Ser12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[Sha18] Shahed Sharif. Period and index for higher genus curves. *J. Number Theory*, 186:259–268, 2018.

[ST22] Arul Shankar and Frank Thorne. On the asymptotics of cubic fields ordered by general invariants. Preprint available at https://arxiv.org/abs/2207.06514, 2022.

[Sto19] Michael Stoll. Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank. *J. Eur. Math. Soc. (JEMS)*, 21(3):923–956, 2019.

[Sut] Andrew Sutherland. Totally ramified extensions and Krasner's lemma. Number theory course notes, available at https://math.mit.edu/classes/18.785/2017fa/LectureNotes11.pdf.

[SV22] Geoffrey Smith and Isabel Vogt. Low degree points on curves. *Int. Math. Res. Not. IMRN*, 2022(1):422–445, 2022.

[SW18] Arul Shankar and Xiaoheng Wang. Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.*, 154(1):188–222, 2018.

[Vak17] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. Draft, 2017. See this blog.

[Wat21] Lori D. Watson. Hasse principle violations in twist families of superelliptic curves. Preprint available at see https://arxiv.org/abs/2103.05731, 2021.

[Wil74] Kenneth S. Williams. Mertens' theorem for arithmetic progressions. *J. Number Theory*, 6:353–359, 1974.

[Zar10] Yuri G. Zarhin. Families of absolutely simple hyperelliptic Jacobians. *Proc. Lond. Math. Soc. (3)*, 100(1):24–54, 2010.

[Zar18] Yuri G. Zarhin. Endomorphism algebras of abelian varieties with special reference to superelliptic Jacobians. In *Geometry, algebra, number theory, and their information technology applications*, volume 251 of *Springer Proc. Math. Stat.*, pages 477–528. Springer, Cham, 2018.