Hasse Principle Violations in Twist Families of Hyperelliptic and Superelliptic Curves

by

Lori Desirae Watson

(Under the Direction of Pete L. Clark)

Abstract

In this work we consider Hasse Principle violations in families of twists of hyperelliptic and superelliptic curves defined over $\mathbb{Q}$.

Index words: Number theory, Hyperelliptic curves, Superelliptic curves, Hasse Principle, Local-to-global principles

Hasse Principle Violations in Twist Families of Hyperelliptic and Superelliptic Curves

by

Lori Desirae Watson

B.S., Florida Atlantic University, 2013

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2019

Hasse Principle Violations in Twist Families of Hyperelliptic and Superelliptic Curves

by

Lori Desirae Watson

Approved:

Major Professor:	Pete L. Clark
Committee:	Dino Lorenzini Paul Pollack Robert Rumely

Electronic Version Approved:

Dean's Name Here
Dean of the Graduate School
The University of Georgia
May 2019

Hasse Principle Violations in Twist Families of Hyperelliptic and Superelliptic Curves

Lori Desirae Watson

April 23, 2019

Acknowledgments

I would first like to thank my advisor Pete Clark for his guidance and support. I would also like to thank my committee members Dino Lorenzini, Paul Pollack and Robert Rumely for their instruction over the years. Ed Azoff, Kelly Black, and Robert Varley have been generous in sharing their time and knowledge.

My thanks to Laura Ackerley for her warmth and kindness and to all the staff in the math department for the great work they do. Thanks go to the friends I have made in the department, most especially Kübra, Jordan, Ernest, and Zerotti.

I can never express how grateful I am to my family - to say they have supported me through it all is a profound understatement. More than any others, my parents have stood by me and believed in me, even when I did not. For them (and for much more), my thanks go to the God who has blessed me beyond measure.

There are many people to whom I owe my deepest thanks, and though I am not be able to name them all here I hope they know they are appreciated.

Contents

Chapter 1

The Hasse Principle

1.1 Introduction and Definitions

We begin by reviewing the Hasse Principle. The Hasse Principle falls within the realm of "local-to-global principles". The motivating question for such principles is this: given an object X over a number field k, when does local information provide meaningful insight into global behavior?

1.1.1 Number Fields and Their Places

A global field k is either a number field (a finite extension of $\mathbb{Q}$), or a global function field (a finite extension of $\mathbb{F}_q(t)$ where $\mathbb{F}_q$ is a finite field of characteristic $p > 0$). Though the Hasse Principle and other local-to-global principles can be more broadly considered over arbitrary global fields, we restrict our attention to the number field case. Let k be a number field. Before reviewing the Hasse Principle, we briefly describe the set of non-trivial absolute values on k.

Let $\mathcal{O}_k$ denote a ring of integers of a number field k. For a nonzero prime ideal $\mathfrak{p}$, we define a valuation on k as follows: for $a \in \mathcal{O}_k$, if $a \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$, let $v_{\mathfrak{p}}(a) = n$. For $x \in k^*$, write

$x = \frac{a}{b}$, with $a, b \in \mathcal{O}_k$ relatively prime and let $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b)$. Define $v_{\mathfrak{p}}(0) = -\infty$.

We say that two absolute values of k are equivalent if they induce the same topology. To describe the set of absolute values of an arbitrary number field (up to equivalence), we begin with $k = \mathbb{Q}$. By a theorem of Ostrowski ([Ja96, Prop. II.1.4]), each absolute value of $\mathbb{Q}$ is equivalent to one of

(i) the usual absolute value $|x|_\infty = \max\{x, -x\}$

(ii) a p-adic absolute value $|x|_p = p^{-v_p(x)}$, where p is prime.

$\mathbb{Q}$ is not complete with respect to any nontrivial absolute value. If we complete $\mathbb{Q}$ with respect to the usual absolute value, we obtain the real numbers $\mathbb{R}$. If we complete $\mathbb{Q}$ with respect to a p-adic absolute value, we obtain the field $\mathbb{Q}_p$.

For a more general number field k, each absolute value is an absolute value whose restriction to $\mathbb{Q}$ is equivalent to one of the absolute values on $\mathbb{Q}$. Those which restrict to the usual absolute value are called archimedean; those which restrict to a p-adic absolute value are nonarchimedean. Let $k/\mathbb{Q}$ be of degree $n = r + 2s$ where r is the number of real embeddings of k and s is the number of conjugate pairs of complex embeddings. If $\sigma : k \hookrightarrow \mathbb{C}$ is an embedding, then $|x|_\sigma := |\sigma(x)|_\infty$ is an absolute value on k which restricts to the usual absolute value on $\mathbb{Q}$. There are $r + s$ non-equivalent archimedean absolute values of k corresponding the the r real embeddings and s pairs of conjugate embeddings ([Ja96, Thm. II.4.4]), each of which restricts to the usual absolute value on $\mathbb{Q}$; these are the archimedean absolute values of k. For the nonarchimedean absolute values on k, recall that for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$, the ring $\mathcal{O}_k/\mathfrak{p}$ is a finite field of order $N(\mathfrak{p}) := p^\alpha$ for some prime number p. The $\mathfrak{p}$-adic absolute value on k is normalized so that $|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$. As in the case of $\mathbb{Q}$ an arbitrary number field fails to be complete with respect to any of its nontrivial absolute values. We denote the completion of k with respect to an absolute value $|\cdot|_v$ by k_v (where v may denote either an archimedean or nonarchimedean place). A completion k_v is, in the archimdean case either $\mathbb{R}$ or $\mathbb{C}$ and in the nonarchimdean case, a finite extension of $\mathbb{Q}_p$ for some prime p.

1.1.2 The Hasse Principle

Having recalled some of the facts about number fields and their completions, we can review the Hasse Principle for a curve defined over a number field k. Throughout, we assume a curve is "nice" in the sense of [Po17, Def. 3.5.68], i.e., smooth, projective, and geometrically integral. Given a (nice) curve C defined over a k it is in general difficult to determine whether the curve has any k-rational points. One approach is to determine whether the curve has points over other fields containing k. If the curve fails to have an L-rational point for some field extension L/k, then we can conclude the curve fails to have a k-rational point. For a number field, a natural collection of fields to consider are the completions of k. For example, in attempting to determine whether a curve $C/\mathbb{Q}$ has any $\mathbb{Q}$-rational points, we can instead determine whether C has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p (equivalently, has a real point and has primitive $\mathbb{Z}/n\mathbb{Z}$ solutions for every integer n). If it fails to have a point over even one of those fields, then we can conclude that $C(\mathbb{Q}) = \emptyset$.

Example 1.1.1 *The projective curve C defined by $X^2 + Y^2 + Z^2 = 0$ has no $\mathbb{Q}$-rational points.*

If (X, Y, Z) are real numbers, at least one of which is nonzero, then $X^2 + Y^2 + Z^2 > 0$. Thus $C(\mathbb{R}) = \emptyset \implies C(\mathbb{Q}) = \emptyset$.

Example 1.1.2 *The projective curve C defined by $X^2 + Y^2 = 3Z^2$ has no $\mathbb{Q}$-rational points.*

If there were a rational solution, we could scale to produce a solution (U, V, W) with $U, V, W \in \mathbb{Z}$ relatively prime. If either of U or V is divisible by 3, then reducing $\pmod 3$, we conclude the other must be also; but then $U^2 + V^2$ is divisible by 9, hence W must be divisible by 3, contradicting the choice of relatively prime U, V, W. Thus we may conclude that neither U

nor V is divisible by 3. In this case, we have $(U/V)^2 \equiv -1 \pmod 3$, which is impossible as -1 is not a square modulo 3. Thus we conclude that $C(\mathbb{Q}) = \emptyset$.

One may hope that the absence of any of these "obvious" obstructions will imply the existence of a $\mathbb{Q}$-rational point. Indeed, for some varieties this is indeed the case, as shown in a classical theorem of Hasse and Minkowski ([Ser70, Thm. 8, IV.3.2]):

Theorem 1.1.3 (Hasse-Minkowski) *Let k be a number field. A quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$, $a_j \in k$ represents zero nontrivially in k if and only if it represents k nontrivially in k_v for all places v.*

The theorem inspires the following definition:

Definition 1.1.4 *Let k be a number field and X/k a nice variety. We say that X satisfies the* Hasse Principle *if $X(k_v) \neq \emptyset$ for every completion k_v implies $X(k) \neq \emptyset$.*

In the context of varieties, the Hasse-Minkowski theorem states that a smooth quadric hypersurface over a number field k satisfies the Hasse Principle. When a variety X has points over every completion of k, we will say that X *has points everywhere locally.* Thus the Hasse Principle is the statement that having points everywhere locally is equivalent to having a global (k-rational) point.

1.2 Examples and Counterexamples

We have seen that there are families of varieties for which the Hasse Principle holds. In the context of curves in particular, the Hasse-Minkowski theorem tells us that genus 0 curves (those of the form $aX^2 + bY^2 + cZ^2 = 0$) satisfy the Hasse Principle over any number field. Even in genus 1, however, counterexamples exist. The first known counterexample was found independently by Lind [Li40] and Reichardt [Re42]:

Example 1.2.1 (Lind-Reichardt) *The genus 1 curve defined by* $2y^2 = x^4 - 17$ *violates the Hasse Principle over* $\mathbb{Q}$*.*

A possibly more well-known example of a diagonal ternary cubic form violating the Hasse Principle is provided by Selmer [Se54]:

Example 1.2.2 (Selmer) *The genus 1 curve defined by* $3X^3 + 4Y^3 + 5Z^3 = 0$ *violates the Hasse Principle over* $\mathbb{Q}$*.*

A Hasse Principle violation (over $\mathbb{Q}$) of the form $C : aX^3 + bY^3 + cZ^3 = 0$ is especially interesting as it represents a nontrivial element of Ш$(E/\mathbb{Q})$, the Tate-Shafarevich of its Jacobian elliptic curve $E : X^3 + Y^3 + abcZ^3 = 0$ ([Ma93]).

Chapter 2

Hyperelliptic and Superelliptic Curves

In this chapter we provide background information on hyperelliptic and superelliptic curves over global fields (with restrictions on the characteristic of the global field as needed). Throughout, we again assume our curves are “nice” (smooth, projective, and geometrically integral).

2.1 Hyperelliptic Curves

A reference for this section is [Liu02, 7.4].

2.1.1 Definition and model

Let k be a field with $\mathrm{char}(k) \neq 2$. Let C be a curve of genus $g \geq 1$ defined over a field k. We say that C/k is a *hyperelliptic curve* if there exists a degree 2 morphism $\pi : C \to \mathbb{P}^1_k$ over k. The function field of such a curve is a quadratic extension of $k(\mathbb{P}^1) = k(x)$, so it is obtained by adjoining a square root of some element of $k(x)$. In other words, $k(C) = k(x, y)$ with $y^2 = f(x)$ for some $f(x) \in k(x)$. By multiplying by an element of $k(x)^*$, we can assume that $y^2 = f(x)$ for some $f(x) \in k[x]$. We may (and will) assume that $f(x)$ is squarefree. If k is infinite, we may, in addition, assume that the degree of f is even; otherwise, if the degree of f is $2g+1$, fix $\alpha \in k$ such that $f(\alpha) \neq 0$. The change of coordinates

$$(x, y) \mapsto \left(\frac{1}{x-\alpha}, \frac{y}{(x-\alpha)^{g+1}} \right)$$

yields an affine model for C with an even degree defining polynomial.

2.1.2 The Hyperelliptic Involution

For a hyperelliptic curve $C : y^2 = f(x)$ with $f(x)$ squarefree, there exists an order 2 automorphism of the curve ι called a hyperelliptic involution. On affine points, it is easy to see the action of the involution: For an affine point (x, y) of C,

$$\iota(x, y) = (x, -y).$$

The action of $\langle \iota \rangle$ on C induces an equivalence relation; under this relation, $(x, y) \sim \iota(x, y)$. Thus the two-to-one map $\pi : C \to \mathbb{P}^1_k$ given by $\pi(x, y) = x$ can be identified with the natural quotient map $C \to C/\langle \iota \rangle$. For genus $g \geq 2$, if a hyperelliptic involution exists, it is unique ([Liu02, Prop. 7.4.29]), and in such cases we will refer to "the" hyperelliptic involution.

2.1.3 Ramification

2.1.4 Genus

We have seen that over an infinite field k of characteristic different from 2, a hyperelliptic curve can be given an affine model of the form $C : y^2 = f(x)$, where $f(x)$ has even degree d and distinct roots over $\bar{k}$. The map $\pi : C \to \mathbb{P}^1$ has degree 2 and is ramified precisely at the points where $f(x) = 0$ - since we have assumed the degree of $f(x)$ is even, the map is unramified at infinity. Therefore, there are d ramified points, each of which must have ramification index 2. By the Riemann-Hurwitz formula ([Si97, Thm. II.5.9]), the genus g of the curve C satisfies the equation

$$2g-2=\deg(\pi)(2g(\mathbb{P}^1)-2)+\sum_{P\in C}(e_P-1)=-4+d$$

Thus for a hyperelliptic curve C with defining polynomial f of even degree d, the genus is given by $g=\frac{d-2}{2}$.

Remark 2.1.1 *Note that in the definition, we require $C/\langle\iota\rangle \cong \mathbb{P}^1_k$, and not merely that $C/\langle\iota\rangle$ is isomorphic to a genus 0 curve. In the former case we are guaranteed the existence of a model $y^2=f(x)$. In the latter, such a model may not exist, as shown in [PS97]. In Footnote 9 they exhibit a curve C defined by the equations $x^2+z^2=-1$ and $y^2=(x-1)(x-2)(x-3)(x-4)$ which is a double cover of the curve defined by $x^2+z^2=-1$. C becomes hyperelliptic over a quadratic extension of $\mathbb{Q}$. We may think of curves which map to pointless conics as "geometrically hyperelliptic". As we are concerned with curves with potential Hasse Principle violations, such curves are not of interest in this work as, if a curve defined over a number field k maps to a genus 0 curve which has no k-rational points, then that genus 0 curve, and hence the curve which maps to it, must fail to have a point over some completion k_v of k.*

2.2 Superelliptic Curves

Superelliptic curves are in some ways a natural generalization of hyperelliptic curves. One important feature that hyperelliptic and superelliptic curves share is the existence of nontrivial, abelian automorphism groups. These automorphisms lead to arithmetically interesting structure which will feature prominently in the main theorem. In this section, we introduce superelliptic curves and provide necessary background for future sections.

2.2.1 Model and automorphisms

We begin with a definition:

Definition 2.2.1 *Let $n \geq 2$ be an integer and let k be a field of characteristic $p \nmid n$. A superelliptic curve $C/_k$ is a nice curve admitting an affine model of the form $y^n = f(x)$, where $f(x) \in k[x]$ factors over $\bar{k}$ as*

$$f(x) = A \prod_{j=1}^{r} (x - \alpha_j)^{n_j},$$

where $A \in \bar{k}^*$, the α_j are distinct, $1 \leq n_j < n$ for each j, and $\gcd(n, n_1, \ldots, n_r) = 1$.

Remark 2.2.2 *As shown in [Ko91, Lemma 1], the condition $\gcd(n, n_1, \ldots, n_r) = 1$ guarantees that C is geometrically irreducible. We include Koo's proof below. Note that though Koo's hypotheses include that we work over a field of characteristic 0, the proof holds for a field of characteristic $p \nmid n$.*

Lemma 2.2.3 *Let D be a unique factorization domain of characteristic $p \nmid n$ with field of fractions K. Suppose $\mu_n \subset K$. For $B \in D$ put $B = \omega_1^{e_1} \cdots \omega_r^{e_r}$ with the ω_j nonassociate prime elements of D. If $n \in \mathbb{Z}^+$ is such that $\gcd(n, e_1, \ldots, e_r) = 1$, then the polynomial $F(y) = y^n - B$ is irreducible over K.*

Proof: Let ζ be a primitive nth root of unity in K, and let $\beta \in \bar{K}$ be a root of $F(y)$. Since $\mu_n \subset K$, by Kummer theory ([Bi67]) $K(\beta)/K$ is a finite Galois extension. Let $G = \mathrm{Gal}(K(\beta)/K)$ and let $m = |G| = [K(\beta) : K]$. We will show that $m = n$.

Suppose by way of contradiction that $m < n$. Let $\sigma \in G$. Then

$$\sigma(\beta)^n = \sigma(\beta^n) = \sigma(B) = B,$$

and so

$$\sigma(\beta) = \zeta^{v(\sigma)}\beta$$

for some $v(\sigma) \in \mathbb{Z}/n\mathbb{Z}$. From this we obtain an injective homomorphism

$$v : G \longrightarrow (\mathbb{Z}/n\mathbb{Z}, +),$$
$$\sigma \mapsto v(\sigma).$$

We may now view G as a subgroup of $\mathbb{Z}/n\mathbb{Z}$ and we will write $G = \langle \tau \rangle$. Since $K(\beta)/K$ is Galois, $m|n$. By definition of v, $\tau(\beta) = \zeta^{v(\tau)}\beta$, and so $\tau^m(\beta) = \zeta^{v(\tau^m)}\beta = \zeta^{mv(\tau)}\beta$. We also have $\tau^m(\beta) = \beta$, since $|\tau| = |G| = m$. Thus $mv(\tau) \equiv 0 \pmod{n}$. Recalling that $\tau(\beta) = \zeta^{v(\tau)}\beta$, we have

$$\tau(\beta^m) = (\tau(\beta))^m = (\zeta^{v(\tau)}\beta)^m = \zeta^{mv(\tau)}\beta^m = \beta^m,$$

and so $\beta^m \in K$.

Let $\beta^m = b \in K$. Then $b^{n/m} = (\beta^m)^{n/m} = \beta^n = B$. Let $\frac{n}{m} = s \in \mathbb{Z}$. Since by assumption $m < n$, $s > 1$. Thus $b^s = B = \omega_1^{e_1} \cdots \omega_r^{e_r}$. From this, we conclude that $s|e_j$ for each $1 \leq j \leq r$. But $s|n$ also, and so we have that $\gcd(n, e_1, \dots, e_r) > 1$, a contradiction. □

Let $f(x) = A\prod_{j=1}^{r}(x - \alpha_j)^{n_j} \in \bar{k}[x]$ with the α_j distinct and $n_j < n$ for all $1 \leq j \leq r$ and $\gcd(n, n_1, \dots, n_r) = 1$. Applying Lemma 2.2.3 with $D = \bar{k}[x]$, $K = \bar{k}(x)$, and $y^n = f(x)$, we see that the curve C determined by the affine model $y^n - f(x) = 0$ is geometrically irreducible.

2.2.2 Ramification

When a superelliptic curve C/k is given by affine model $y^n = f(x)$ with n prime, ramification with respect to the superelliptic automorphism group $\langle \tau \rangle$ is easy to determine. As the map $C \to \mathbb{P}^1$, $(x, y) \mapsto x$ is geometrically Galois and of degree n, we have that $e_P \mid n$ for the ramification index e_P of any point P of C (in addition, if P, P' map to the same point, then since the map is geometrically Galois, $e_P = e_{P'}$). When n is prime, this shows that either a point is unramified or it is totally ramified. When n is composite, the issue of ramification is slightly more complicated. Regardless of whether n is prime or composite, the ramification locus will consist of affine points of the form $(\alpha, 0)$, $\alpha \in \bar{k}$ a root of $f(x)$, and (possibly) points above ∞, depending on the degree of the defining polynomial.

2.2.3 Genus

Let k be a number field and let C/k be a superelliptic curve defined by $C : y^p = f(x)$, where p is a prime. If necessary, we may apply an automorphism of $\mathbb{P}^1$ to guarantee that C is unramified above ∞, in which case we have $p|\deg(f)$ (the ramification index of a point above ∞ is given by $\frac{p}{\gcd(p,\deg(f))}$ ([Ko91])). Thus, if $f(x)$ factors over $\bar{k}$ as $f(x) = A\prod_{j=1}^{r}(x-\alpha_j)^{n_j}$, $1 \leq n_j < p$ for all j, then by the Riemann-Hurwitz formula, the genus g of C satisfies

$$2g - 2 = -2p + \sum_{j=1}^{r}(p-1),$$

and so

$$g = \frac{(r-2)(p-1)}{2}.$$

In the case that $f(x)$ has no repeated roots, writing $\deg(f) = pk + p$, $k \geq 0$, Riemann-Hurwitz gives

$$2g - 2 = -2p + (pk + p)(p-1).$$

After rearrangement, we find

$$\deg(f) = pk + p = \frac{2g}{p-1} + 2$$

Work of Koo [Ko91, §3] gives the following genus formula for more general superelliptic curves defined over $\mathbb{C}$.

Theorem 2.2.4 (Koo) *Let C be a superelliptic curve over $\mathbb{C}$ with affine model $y^n = f(x)$ where*

$$f(x) = A\prod_{j=1}^{r}(x-\alpha_j)^{n_j},$$

with $n_j < n$ for all $1 \leq j \leq r$ and $\gcd(n, n_1, \ldots, n_r) = 1$. Then the genus g of C is

$$g = \frac{1}{2}(r-1) - \frac{1}{2}\left(\sum_{j=1}^{r}\gcd(n, n_j) + \gcd(n, N)\right) + 1,$$

where $N = \sum_{j=1}^{r} n_j$.

2.3 Galois Cohomology

In this section we will describe *twists* of a superelliptic curve C. Given a curve C defined over k, a twist is a curve C' also defined over k such that C and C' become isomorphic over k^s, a separable closure of k. The primary reference for this section is [Ser97].

2.3.1 Basic Definitions

Definition 2.3.1 *A* profinite group *is a topological group G which is the projective limit of finite groups, each given the discrete topology.*

Recall that a group $(G, \cdot)$ is a topological group if it is a topological space such that the maps $(\cdot) : G \times G \to G$, $(\sigma, \tau) \mapsto \sigma \cdot \tau$ and $i : G \to G$, $\sigma \mapsto \sigma^{-1}$ are continuous.

Example 2.3.2 *Let k be a field and let k^s be a separable closure of K. Then $G_k \coloneqq Gal(k^s/k)$, the Galois group of k^s over k is the projective limit of the Galois groups $Gal(L/k)$ of the finite Galois extensions L/k which are contained in k^s/k. It is therefore a profinite group.*

Definition 2.3.3 *Let G be a profinite group. A* discrete G-module *is an abelian group $(A, +)$ on which G acts such that the action is continuous for the profinite topology on G and the discrete topology on A. In other words the stabilizer of each element of A is open in G.*

We will refer to discrete G-modules simply as G-modules throughout. Following Serre ([Ser97]), we write ${}^{\sigma}a$ for the image of an element $a \in A$ under $\sigma \in G$.

2.3.2 H^0 and H^1

Definition 2.3.4 *Let G be profinite group and A a G-module. We define the* 0th cohomology group *to be the set of G-invariant elements of A*

$$H^0(G, A) = A^G := \{a \in A : \ {}^{\sigma}a = a \textit{ for all } \sigma \in G\}.$$

Definition 2.3.5 *Let G be a profinite group and A a G-module. A map $\xi : G \to A$ is a* 1-cocycle *if for all $\sigma, \tau \in G$, $\xi_{\sigma\tau} = \xi_\sigma + {}^{\sigma}\xi_\tau$. A map $\xi : G \to A$ is a* 1-coboundary *if there exists $a \in A$ such that $\xi_\sigma = {}^{\sigma}a - a$ for all $\sigma \in G$.*

Note: For the ease of notation, we write ξ_σ as opposed to $\xi(\sigma)$. The set of continuous 1-cocycles from G to A is denoted by $Z^1_{cont}(G, A)$ and the set of 1-coboundaries is denoted by $B^1(G, A)$. Every 1-coboundary is (automatically) continuous, so we have $B^1(G, A) \subseteq Z^1_{cont}(G, A)$.

Definition 2.3.6 *Let G be a profinite group and A a G-module. The* 1st cohomology group *is the quotient group*

$$H^1(G, A) = \frac{Z^1_{\text{cont}}(G, A)}{B^1(G, A)}.$$

2.3.3 G-sets and an alternate definition of H^1

Definition 2.3.7 *A G-set X is a discrete topological space with a continuous G-action. If X is also a group with operation $\cdot$ such that ${}^{\sigma}(x \cdot y) = {}^{\sigma}x \cdot {}^{\sigma}y$, we say that X is a G-group. Note that a G-module is simply an abelian G-group.*

For any G- set, as before, we define $H^0(G, X)$ to be the set X^G of elements of X fixed by G. For a G-group, we define $H^1(G, X)$ in a similar manner as before (the set of continuous 1-cocycles modulo 1-coboundaries), but note that when X is non-abelian, $H^1(G, X)$ is not a group, but rather a pointed set with a distinguished element (corresponding to the trivial cocycle).

Definition 2.3.8 *Let A be a G-group and X a G-set. We say that A acts on the left (resp. right) on X compatibly with G if*

(i) A acts on the left (resp. right) on X and

(ii) For $a \in A$, $x \in X$, and $\sigma \in G$, ${}^\sigma(a \cdot x) = {}^\sigma a \cdot {}^\sigma x$ (resp. ${}^\sigma(x \cdot a) = ({}^\sigma x) \cdot ({}^\sigma a)$).

Definition 2.3.9 *A right (resp. left) principal homogeneous space over A is a non-empty G-set P on which A acts on the right (resp. left) in a manner compatibly with G such that for each $x, y \in P$, there exists a unique $a \in A$ such that $y = x \cdot a$ (resp. $y = a \cdot x$).*

Having defined G-sets and principal homogeneous spaces for a G-group A, we can now provide an alternate description of $H^1(G, A)$ for a G-group A:

Proposition 2.3.10 *Let A be a G-group. There is a bijection between the pointed set of classes of principal homogeneous spaces over A and the pointed set $H^1(G, A)$.*

For a proof, see [Ser97, I.5.1, Prop. 33].

Given a G-group A and a a G-set X on which A acts on the left compatibly with G, we may obtain a twist X_ξ of X using a 1-cocycle $\xi \in Z^1_{\text{cont}}(G, A)$. The twist X_ξ is the set X on which G acts by the formula

$${}^{\sigma'}x = \xi_\sigma \cdot {}^\sigma x,$$

and we have that X_{ξ_1} and X_{ξ_2} are isomorphic if ξ_1 and ξ_2 are cohomologous ([Ser97, §I.5.3]).

2.3.4 Galois Cohomology of Hyperelliptic and Superelliptic Curves

We fix in this section a number field k of and an algebraic closure $\bar{k}$. The absolute Galois group G of $\bar{k}/k$ is a profinite group. Let $C : y^n = f(x)$ be a superelliptic curve defined over k. We again let τ be the automorphism of $C_{/\bar{k}}$ defined by $\tau(x, y) = (x, \zeta y)$, where ζ is a primitive nth root of unity.

G naturally acts on $C(\bar{k})$ by ${}^\sigma(x, y) = ({}^\sigma x, {}^\sigma y)$ where $P = (x, y) \in C(\bar{k})$. G also acts on the automorphism group $\langle\tau\rangle$ by ${}^\sigma\tau(x, y) = (x, {}^\sigma\zeta y)$. From this action we see that $\langle\tau\rangle$ and μ_n are isomorphic as G-modules. We have ${}^\sigma(\tau(x, y)) = {}^\sigma(x, \zeta y) = ({}^\sigma x, {}^\sigma\zeta {}^\sigma y) = {}^\sigma\tau({}^\sigma x, {}^\sigma y) = {}^\sigma\tau({}^\sigma(x, y))$, so $\langle\tau\rangle$ acts on the left on $C(k^s)$ compatibly with G.

2.4 Twists of Hyperelliptic and Superelliptic Curves

In this section we determine a model for the twist of a superelliptic curve C defined over a number field k. When C admits an affine model $y^n = f(x)$, $f(x) \in k[x]$, we will show that a twist corresponding to a cocycle in $H^1(G_k, \mathrm{Aut}(C))$ admits an affine model of the form $dy^n = f(x)$, where $d \in k^*$ is nth power free.

2.4.1 Kummer Sequences for Fields and Hilbert's Theorem 90

For a number field k with algebraic closure $\bar{k}$, G_k acts on $\bar{k}$ and $\bar{k}^*$ in a natural way such that $\bar{k}$ and $\bar{k}^*$ are G_k-modules. For $\bar{k}^*$, the map $n : \bar{k}^* \to \bar{k}^*$, $z \mapsto z^n$ is a G_k-module homomorphism with kernel μ_n. Thus we have a short exact sequence of G_k-modules:

$$1 \longrightarrow \mu_n \longrightarrow \bar{k}^* \xrightarrow{z \mapsto z^n} \bar{k}^* \longrightarrow 1,$$

which yields a long exact sequence in cohomology:

$$1 \longrightarrow \mu_n(k) \longrightarrow k^* \xrightarrow{z \mapsto z^n} k^* \xrightarrow{\delta} H^1(G_k, \mu_n) \longrightarrow H^1(G_k, \bar{k}^*) \longrightarrow \cdots .$$

By Hilbert's Theorem 90 ([Si97, Prop. B.2.5]), $H^1(G_k, \bar{k}^*) = 0$, so we have $k^*/(k^*)^n \cong H^1(G_k, \mu_n)$, where the isomorphism

$$\delta : k^*/(k^*)^n \longrightarrow H^1(G_k, \mu_n)$$

is given by the formula $\delta(d) =$ the cohomology class of the map $\sigma \mapsto \frac{\beta^\sigma}{\beta}$, where $\beta \in \bar{k}^*$ is any element such that $\beta^n = d$.

We have seen that $H^1(G_k, Aut(C))$ is in bijection with the set of k-isomorphism classes of twists C' of C. Viewing $H^1(G_k, \mu_n) = H^1(G_k, \langle\tau\rangle)$ as a subset of $H^1(G_k, Aut(C))$, we can parameterize k-isomorphism classes of twists of C by nth-power classes of $k^*/(k^*)^n$. From this we will derive an affine model for twists of C, following the approach of [Si97, p.344].

Let $d \in k^*$ and let $\beta \in k^s$ be an nth root of d. Define a cocycle

$$\xi : G_k \longrightarrow \mu_n,$$

$$\xi_\sigma = \frac{\beta^\sigma}{\beta}.$$

Fix an isomorphism

$$[\ ]:\mu_n \longrightarrow \langle\tau\rangle,$$

$$[\zeta](x,y)=(x,\zeta y),$$

where ζ is a primitive nth root of unity. Let C_d be the twist corresponding to the cocycle $(\sigma \mapsto [\xi_\sigma]) \in H^1(G_k,\langle\tau\rangle)$. Write $\bar{k}(C)=\bar{k}(x,y)$ and $\bar{k}(C_d)=\bar{k}(x,y)_\xi$ for the function fields of C and C_d (respectively) over k^s. Since $\tau(x,y)=(x,\zeta y)$, the action of $\sigma \in G_k$ on $\bar{k}(x,y)_\xi$ is determined by the formulas

$$\beta^\sigma=\xi_\sigma\beta, \quad x^\sigma=x, \quad y^\sigma=\xi_\sigma y.$$

Therefore, the subfield fixed by G_k contains the functions

$$X=x \quad \text{and} \quad Y=y/\beta,$$

which satisfy the equation

$$dY^n=f(X),$$

which is the equation for a superelliptic curve defined over k. Identifying $(X,Y)\mapsto(X,Y/\beta)$ shows that this curve is isomorphic to C over $k(\beta)$.

Chapter 3

Main Theorem

In this chapter we prove the main result. The result essentially states that if one assumes the *abc* conjecture, then the family of degree n twists of a superelliptic curve can exhibit one of only two behaviors with respect to Hasse Principle violations: either there are no Hasse Principle violations within the family or there are many Hasse Principle violations within the family. Following Mazur and Rubin ([MR10]), for a given family of twists we say that "many" curves in the family exhibit property P if the number of twists C_d such that $|d| \leq X$ and C_d satisfies property P is $\gg X/(\log X)^\gamma$ for some $\gamma \in \mathbb{R}$. (For functions $N(X)$ and $G(X)$ with $G(X)$ eventually positive, we use Vinogradov's notation and write $G(X) \gg N(X)$ if there exist real numbers x_0 and m such that $|N(X)| \leq mG(X)$ for all $X \geq x_0$.)

We provide criteria for the existence of Hasse Principle violations within a family of twists. A point P fixed under the action of the automorphism group $\langle\tau\rangle$ is either a point lying above ∞ or a point with y-coordinate 0. The quotient map $C \to C/\langle\tau\rangle \xrightarrow{\sim} \mathbb{P}^1$ has a $\bar{\mathbb{Q}}$ branch point above ∞ if and only if $n \nmid \deg(f)$ with the ramification index of the point(s) above infinity being $e = n/\gcd(n, \deg(f))$ ([Ko91]). There are $\gcd(n, \deg(f))$ point(s) above infinity admitting a transitive $\mu_{n/e}$-action; if $1 \leq e < n$, these points are not fixed by τ. A point P with y-coordinate 0 necessarily has as its x-coordinate a root of the defining polynomial. The main theorem states that, assuming the *abc* conjecture over $\mathbb{Q}$, either the family of twists has many Hasse Principle violations, or it cannot have any Hasse Principle violations, and the non-existence of violations occurs because the degree of the polynomial or the existence of $\mathbb{Q}$-rational roots of f force every twist to have $\mathbb{Q}$-rational points.

Every hyperelliptic curve (the case $n = 2$) of genus g over $\mathbb{Q}$ admits an affine model of the form $y^2 = f(x)$ where $f(x)$ has degree $2g+2$, coefficients in $\mathbb{Z}$, and no repeated roots; the hyperelliptic curve admits an affine model over $\mathbb{Q}$ with odd degree $2g+1$ if and only if it admits a $\mathbb{Q}$-rational hyperelliptic branch point. If we write each polynomial of degree $2g+2$ as $f(x) = \sum_{j=0}^{2g+2} f_j x^j$ and order hyperelliptic curves of genus g by $\text{Height}(C) := \max\{|f_j|\}$, then as $X \to \infty$, 100% of hyperelliptic curves C have no $\mathbb{Q}$-rational hyperelliptic branch points since under this ordering 100% of all polynomials of degree $2g+2$ are irreducible ([Ri08]).

3.1 Statement of the Main Theorem

Theorem 3.1.1 *Assume the abc conjecture. Let $C : y^n = f(x)$ where $n \geq 2$ is an integer and $f(x) \in \mathbb{Z}[x]$ has distinct roots in $\bar{\mathbb{Q}}$ and $\deg(f) \geq \frac{4n-2}{n-1}$. Then the following are equivalent:*

(i) The automorphism τ has no $\mathbb{Q}$-rational fixed points.

(ii) There exists $0 \leq \gamma < 1$ such that as $X \to \infty$, the number of nth power free integers d with $|d| \leq X$ such that C_d violates the Hasse Principle is $\gg_C \dfrac{X}{\log(X)^\gamma}$.

(iii) Some degree n twist C_d violates the Hasse Principle.

That (ii) implies (iii) is immediate. For (iii) implies (i), a $\mathbb{Q}$-rational fixed point of τ will remain rational on every twist. It now remains to prove (i) implies (ii). For this, we will require two results. The first is due to Granville and it provides an upper bound on the number of twists that have so-called "nontrivial" $\mathbb{Q}$-rational points. By nontrivial, Granville means a point that is *not* a fixed point of the superelliptic automorphism. In the absence of any $\mathbb{Q}$-rational branch points, Granville's results provides an upper bound on the number of twists which have any $\mathbb{Q}$-rational points at all. The second result is a strengthening of [CW18.2, Thm. 3]. It provides a lower bound on the number of twists of a curve that have points everywhere locally (and in fact shows that there are many such twists).

3.2 Bound on twists with nontrivial global points

The "global" step towards proving the main theorem is a result due to Granville. This results provides an upper bound on the number of twists with nontrivial $\mathbb{Q}$-rational points. It relies on the *abc* theorem to bound the height of the x-coordinate of a point that can appear on a twist C_d.

3.2.1 The *abc* conjecture

One of several equivalent statements of the *abc* conjecture over $\mathbb{Q}$ is as follows:

Conjecture 3.2.1 (*abc* Conjecture, Masser-Oesterlé) *For each $\epsilon > 0$, there exists a constant K depending only on ϵ such that for all triples (a, b, c) of relatively prime integers with $a + b = c$,*

$$\max(|a|, |b|, |c|) \leq K(\prod_{\substack{p \text{ prime} \\ p|abc}} p)^{1+\epsilon},$$

The *abc* conjecture has numerous implications; most relevant to this work is that the *abc* conjecture, if true, allows one to count the number of nth power-free values achieved by a polynomial with integer coefficients.

3.2.2 Granville's Theorem

A theorem of Granville allows us to bound the number of nth power free integers $d \in \mathbb{Z}$ with $|d| \leq X$ and C_d having $\mathbb{Q}$-rational points which are not fixed by the superelliptic automorphism τ.

Theorem 3.2.2 (Granville, [Gr07, §11]) *Assume that the abc-conjecture is true. Fix $\epsilon > 0$. Let $f(x) \in \mathbb{Z}[x]$ have no repeated roots in $\bar{\mathbb{Q}}$. Let $d \in \mathbb{Z}$ be an nth power free integer. Any rational point on $C_d : dy^n = f(x)$ with x-coordinate r/s where* $\gcd(r, s) = 1$ *satisfies*

$$|r|, |s| \ll_{f,\epsilon} |d|^{-\left(nk+i-1-\frac{\gcd(n,i)+1}{n-1}\right)+\epsilon},$$

where $\deg(f) = nk + i$, $1 \leq i \leq n$.

As a consequence, we conclude that as $X \to \infty$, the number of nth power free integers d with $|d| \leq X$ for which C_d has a nontrivial rational point is $\ll_f X^{2/\left(nk+i-1-\frac{\gcd(n,i)+1}{n-1}\right)+\epsilon}$

If $\frac{4n-2}{n-1} < \deg(f)$, then for sufficiently small $\epsilon > 0$, the number of nth power free $d \in \mathbb{Z}$ with $|d| \leq X$ such that C_d has a nontrivial rational point is X^a for some $a < 1$.

3.3 Bound on twists with points everywhere locally

With an eye towards eventually proving the main theorem for arbitrary number fields, in this section we prove that under a mild hypothesis, for a superelliptic curve C which has points everywhere locally, many of its twists have points everywhere locally.

Lemma 3.3.1 *Let $C : y^n = f(x)$ be a superelliptic curve of genus $g \geq 1$ defined over a number field k. Suppose C has points everywhere locally. For an element $d \in \mathcal{O}_k$, let $N(d) = |\mathcal{O}_k/(d)|$. As $X \to \infty$, the number of non-associate elements $\pi \in \mathcal{O}_k$ such that $N(\pi) \leq X$ and C_π has points everywhere locally is $\gg_{C,k} X/\log X$.*

Proof: We begin by constructing a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ such that every prime ideal $\mathfrak{p}$ that splits in the ray class field $k^{(\mathfrak{m})}$ is principally generated by an element $\pi \in \mathcal{O}_k$ having the property that $C_\pi \cong_{k_v} C$ for every prime dividing $\mathfrak{m}_0$. Let $(\pi) = \mathfrak{p} \triangleleft \mathcal{O}_k$ denote a principal maximal ideal of $\mathcal{O}_k$ with π satisfying $\sigma(\pi) > 0$ for every real embedding $\sigma : k \hookrightarrow \mathbb{R}$. These ideals are precisely those which split in the narrow Hilbert Class Field of k ([Ja96, §3])). For any place v of k, if $\pi \in k_v^{*n}$, then $C_\pi \cong C$ over k_v. Thus, if k_v is any archimedean completion of k then $C_\pi \cong C$ over $k_v$and $C_\pi(k_v) \neq \emptyset$. From now on, v will denote a finite place corresponding to a prime ideal $\mathfrak{L}_v$, $\mathcal{O}_v$ will denote the ring of integers of k_v, and $\mathbb{F}_q$ the finite field with q elements will denote the residue field of k_v.

Let $M_1 \in \mathbb{Z}^+$ be such that C extends to a smooth proper relative curve over $\mathcal{O}_v$ for every v such that $\mathrm{char}(\mathfrak{L}_v) > M_1$. Such an M_1 exists for any nice curve $C/_k$ by the openness of the smooth locus.

Suppose $\mathrm{char}(\mathfrak{L}_v) > M := \max\{M_1, 4g^2 - 1, n\}$, $\mathfrak{L}_v \neq \mathfrak{p}$, and $\pi \notin k_v^{*n}$. Then the minimal regular model $C/_{\mathcal{O}_v}$ is smooth. Fix an extension $k_v\left(\sqrt[n]{\pi}\right)/k_v$ which contains an nth root of π. Over $k_v\left(\sqrt[n]{\pi}\right)$, $C \cong C_\pi$. Since $k_v\left(\sqrt[n]{\pi}\right)/k_v$ is unramified for any choice of an nth root of π, and formation of the minimal regular model commutes with étale base change ([Liu02, Prop. 10.1.17]), it follows that the minimal regular model $(C_\pi)_{/\mathcal{O}_v}$ is smooth. By the Riemann hypothesis for curves over a finite field ([Si97, Thm. V.2.2]), since $q \geq 4g^2$, we have $C_\pi(\mathbb{F}_q) \neq \emptyset$, so by Hensel's Lemma ([Ca67]) we have $C_\pi(k_v) \neq \emptyset$.

Suppose now $\mathrm{char}(\mathfrak{L}_v) \leq M$ and $\mathfrak{L}_v \neq \mathfrak{p}$. For each $\mathfrak{L}_v$ there is some θ_v so that if $\pi \equiv 1 \pmod{\mathfrak{L}_v^{\theta_v}}$, then π is an nth power in k_v ([La13, p. 43]). We choose $\mathfrak{m}_0$ such that $\mathrm{ord}_v(\mathfrak{m}_0) = \theta_v$ for each $\mathfrak{L}_v$ with $\mathrm{char}(\mathfrak{L}_v) \leq M$ ([Ch09, Ch. 3, §2]). For each principal maximal prime $\mathfrak{p} = (\pi)$ splitting in $k^{(\mathfrak{m})}$, $C_\pi \cong C$ over k_v for $\mathrm{char}(\mathfrak{L}_v) \leq M$, and thus $C_\pi(k_v) \neq \emptyset$.

Finally, suppose $\mathfrak{L}_v = \mathfrak{p}$. Let $P \in C(\bar{k})$ be a fixed point of τ. We assume $\mathfrak{p}$ splits completely in $K = k(P)$. Then, if $\mathfrak{P}$ is a prime of K lying above $\mathfrak{p}$, since $\mathfrak{p}$ splits completely, the completion $K_{\mathfrak{P}}$ has $[K_{\mathfrak{P}} : k_{\mathfrak{p}}] = 1$, thus K embeds into $k_{\mathfrak{p}}$, and $P \in C_\pi(k_{\mathfrak{p}})$, so $C_\pi(k_{\mathfrak{p}}) \neq \emptyset$. We have imposed finitely many conditions on $\mathfrak{p}$, each requiring that $\mathfrak{p}$ splits completely in a certain number field. Letting L be the Galois closure of the compositum of these finitely many number fields, we have that C_π has points everywhere locally whenever $(\pi) = \mathfrak{p}$ splits completely in L. By the Chebotarev density theorem ([LS96, Appendix]), this set of primes (which we will denote by S and use in the next theorem) has positive density in the set of $\mathcal{O}_k$ primes. By Landau's Prime Ideal Theorem ([La03]), the number of prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$ with $N\mathfrak{p} \leq X$ is asymptotic to $X/\log X$. □

In the case $k = \mathbb{Q}$, having produced a positive density set of primes whose twists have points everywhere locally, we can construct a larger set of nth power free integers $d \in \mathbb{Z}$ such that the twists C_d have points everywhere locally.

Theorem 3.3.2 *Let $C : y^n = f(x)$ be a superelliptic curve of genus $g \geq 1$ defined over $\mathbb{Q}$. Suppose C has points everywhere locally. The number of nth power free integers d with $|d| \leq X$ such that C_d has points everywhere locally is $\gg_C X/\log(X)^\gamma$ for some $0 \leq \gamma < 1$.*

Proof: Denote the set of primes p constructed in Lemma 3.3.1 by S. By construction this set has density $0 < \delta(S) < 1$. Consider the set $\mathcal{D}$ consisting of nth power free integers d, all of whose prime divisors are in S. If n is even we further require that all elements of $\mathcal{D}$ be positive. We will show that for each $d \in \mathcal{D}$, the twist C_d has points everywhere locally.

If n is even then as $d > 0$ and $C(\mathbb{R}) \neq \emptyset$, we have $C_d(\mathbb{R}) \neq \emptyset$. If n is odd or if $f(x)$ has a real root then $C_d(\mathbb{R}) \neq \emptyset$ for every nonzero integer d.

Next, let M be as in Lemma 3.3.1, and let $\ell > M$, $\ell \nmid d$. If $d \in \mathbb{Q}_\ell^{*n}$, then C_d is isomorphic to C over $\mathbb{Q}_\ell$, thus $C_d(\mathbb{Q}_\ell) \neq \emptyset$. So assume $d \notin \mathbb{Q}_\ell^{*n}$. Then $\mathbb{Q}_\ell(\sqrt[n]{d})/\mathbb{Q}_\ell$ is unramified, and as before we conclude that the minimal regular model $(C_d)_{/\mathbb{Z}_\ell}$ is smooth. Then by the Riemann Hypothesis for curves over a finite field, since $\ell \geq 4g^2$, $C_d(\mathbb{F}_\ell) \neq \emptyset$, so by Hensel's Lemma, we again have $C_d(\mathbb{Q}_\ell) \neq \emptyset$.

For $\ell < M$ and $\ell \nmid d$, as $d = p_1^{m_1} \cdots p_r^{m_r}$ with $p_j \in \mathbb{Q}_\ell^{*n}$ for all $1 \leq j \leq r$, $d \in \mathbb{Q}_\ell^{\times n}$, so C_d is isomorphic to C over $\mathbb{Q}_\ell$, thus $_d(\mathbb{Q}_\ell) \neq \emptyset$.

Finally, consider $C_d(\mathbb{Q}_p)$, where $p|d$. Then $p \in S$. By construction, for each $p \in S$, p splits completely in $K = \mathbb{Q}(P)$ where P is a fixed point ofτ. As before, if $\mathfrak{P}$ is a prime of

K lying above p, since p splits completely, the completion $K_{\mathfrak{P}}$ has $[K_{\mathfrak{P}} : \mathbb{Q}_p] = 1$, thus K embeds into $\mathbb{Q}_p$. Since P is a fixed point of τ, it is of the form $P = (\alpha, 0)$, where α is a root of the defining polynomial $f(x)$. Thus $K = \mathbb{Q}(\alpha) \subset \mathbb{Q}_p$. Then $(\alpha, 0)$ is a $\mathbb{Q}_p$-rational point of every degree n twist of C, so in particular $C_d(\mathbb{Q}_p) \neq \emptyset$. Thus C_d. has points everywhere locally for each $d \in \mathcal{D}$.

Let $\gamma = 1 - \delta(S)$. By [Ser76, Thm 2.4], we have that the number of $d \in \mathcal{D}$ with $|d| \leq X$ such that C_d has points everywhere locally is $\gg X/\log(X)^\gamma$. □

3.4 Proof of the Main Theorem

We now complete the proof of the main theorem:

Let $C : y^n = f(x)$ be a superelliptic curve, where $f(x)$ has coefficients in $\mathbb{Z}$, distinct roots in $\bar{\mathbb{Q}}$, no roots in $\mathbb{Q}$, and $\deg(f) > (4n-2)/(n-1)$. If C does not have points everywhere locally, write $f(1) = d_1 d_2^n$ where $d_1, d_2 \in \mathbb{Z}$ and d_1 is nth power free. Then the curve $C' \coloneqq C_{d_1}$ (with model $d_1 y^n = f(x)$) has the $\mathbb{Q}$-rational point $(1, d_2)$ and hence has points everywhere locally. Applying Theorem 3.3.2 to C', we have that the number of nth power free integers d with $|d| \leq X$ such that the twist $C'_{d'}$ of C' with points everywhere locally is $\gg X/\log(X)^\gamma$. As the twist $C'_{d'}$ is a twist of the original curve C, we have that the number of nth power free integers d with $|d| \leq X$ such that C_d has points everywhere locally is still $\gg_C X/\log(X)^\gamma$.

By 3.2.2, we have that the number of nth power free $d \in \mathbb{Z}$ with $|d| \leq X$ such that $C_d(\mathbb{Q}) \neq \emptyset$ is $\ll X^{2/3}$. Thus the number of nth power free d with $|d| \leq X$ such that C_d violates the Hasse Principle is $\gg_C X/\log(X)^\gamma$. □

3.5 Asymptotic Bounds

Assuming the *abc* conjecture, Theorem 3.1.1 shows that the existence of any (equivalently infinitely many) Hasse Principle violations within a family of twists of a curve $C : y^n = f(x)$ depends on the degree of f and whether f possesses any $\mathbb{Q}$-rational roots. By more closely examining the local behavior of f, we can provide more precise bounds on the number of twists violating the Hasse Principle.

Let $\mathfrak{D}_C \coloneqq \{n\text{th power free } d \in \mathbb{Z} : C_d \text{ has points everywhere locally}\}$.
For $X \geq 1$, put $\mathfrak{D}_C(X) = \#\mathfrak{D}_C \cap [-X, X]$. We saw in Thm 3.3.2, that $\mathfrak{D}_C(X) \gg \frac{X}{\log(X)^\gamma}$ for some $\gamma \in (0, 1)$. We will soon see that $\mathfrak{D}_C(X)$ (and hence the number of Hasse Principle violations for C with no $\mathbb{Q}$-rational branch points) depends on the density (within the set of all primes) of the set $\mathcal{S} = \{\ell \text{ prime} : f(x) \text{ has a root modulo } \ell\}$. For the hyperelliptic case $n = 2$, we can provide an unconditional upper bound on the number of twists having points everywhere locally in terms of the density δ of $\mathcal{S}$. For $n \geq 2$, when the density of $\mathcal{S}$ equals 1, we will show that, conditional on the *abc* conjecture, a positive density set of twists have points everywhere locally. Before proceeding we introduce some new terminology:

Definition 3.5.1 *We say a polynomial $f \in \mathbb{Z}[x]$ is* weakly intersective *if $\delta = 1$.*

Theorem 3.5.2 *Let $C : y^n = f(x)$ be a superelliptic curve with $f(x) \in \mathbb{Z}[x]$ squarefree and weakly intersective. Then $\mathfrak{D}_C(X) \gg_C X$.*

As an immediate consequence of Theorem 3.5.2 we have the following corollary:

Corollary 3.5.3 *Let $C : y^n = f(x)$ be a superelliptic curve with $f(x) \in \mathbb{Z}[x]$ squarefree. If C has no $\mathbb{Q}$-rational points fixed by τ and* $\deg(f) > 5$*, then conditionally on the abc conjecture, as $X \to \infty$, the number of degree n twists of $C/_{\mathbb{Q}}$ that violate the Hasse Principle is $\gg_C X$.*

Remark 3.5.4 *Before proving Theorem 3.5.2, we will first show that if $f(x)$ is weakly intersective, then the set of primes ℓ for which $f(x)$ does not have a root $\pmod{\ell}$ is finite.*

(This argument appears in [CW18.2]). Let $f(x) = \sum_{j=1}^{n} a_j x^j \in \mathbb{Z}[x]$ have degree $n \geq 2$ and let Δ be the discriminant of f. Suppose $f(x)$ has distinct roots in $\bar{\mathbb{Q}}$ and let G denote the Galois group of f.

For each prime $\ell \nmid a_n\Delta$, the partition of n given by the cycle type of a Frobenius element σ_ℓ at ℓ coincides with a partition of n given by the degrees of the irreducible factors of the image of f in $(\mathbb{Z}/\ell\mathbb{Z})[x]$. Since $f(x)$ is weakly intersective, by the Frobenius Density Theorem ([LS96, §3]), every $\sigma \in G$ has a fixed point, and thus f has a root $\pmod{\ell}$ for every $\ell \nmid a_n\Delta$. By Hensel's Lemma, $f(x)$ has a root in $\mathbb{Z}_\ell$ for all but finitely many ℓ.

Proof of 3.5.2: By the remark above, if f is weakly intersective, then f has a root modulo ℓ for all but finitely many ℓ and hence has a root in $\mathbb{Z}_\ell$ for all but finitely many primes ℓ. Therefore, the set $\mathcal{P}$ of primes ℓ such that $C(\mathbb{Q}_\ell) = \emptyset$ is finite. For each $\ell \in \mathcal{P}$, we have $C_d(\mathbb{Q}_\ell) \neq \emptyset$ for any d lying in the same $\mathbb{Q}_\ell$-adic nth power class as $f(1)$. The set of integers lying in any given $\mathbb{Q}_\ell$-adic nth power class is a nonempty union of congruence classes modulo $\ell^{2v_\ell(n)}$ if ℓ is odd and modulo $2^{4v_\ell(n)}$ if $\ell = 2$. By the Chinese Remainder Theorem there are $a, N \in \mathbb{Z}^+$ such that if $d \equiv a \pmod{N}$, then $C_d(\mathbb{Q}_\ell) \neq \emptyset$ for all primes ℓ. A result of Prachar ([Pr58]) guarantees that there is a positive density set of $d \equiv a \pmod{N}$ which are squarefree (and thus nth power free), so long as $a \in (\mathbb{Z}/N\mathbb{Z})^*$. If f has a real root, then $C_d(\mathbb{R}) \neq \emptyset$ for all nth power free $d \in Z$. Otherwise, $C_d(\mathbb{R}) \neq \emptyset \iff df(1) > 0$. In either case, $\mathfrak{D}_C(X) \gg_f X$. (The implied constant depends on the discriminant of f.) □

In the hyperelliptic case, a slight modification of work of Sadek building on work of Lorenzini ([Lo90] and [Lo13]) yields the following unconditional result on the number of twists having points everywhere locally:

Theorem 3.5.5 *Let $f(x) \in \mathbb{Z}[x]$ be squarefree of even degree with no $\mathbb{Q}$-rational hyperelliptic branch points. If f is not weakly intersective, let $\beta = 1 - \delta$ so $\beta \in (0, 1)$. Then for the hyperelliptic curve $C : y^2 = f(x)$, we have $\mathfrak{D}_C(X) \ll_C \frac{X}{\log(X)^\beta}$.*

Proof: Let Δ be the discriminant of f and let E' be the set of all squarefree integers d such that for all primes $p \mid d$, either $p \mid 2\Delta$ or f has a root modulo ℓ. Let E be the set of all squarefree integers that do not lie in E'. Thus for all $d \in E$, here is an odd prime $\ell \mid d$ such that the image of f in $\mathbb{Z}/\ell\mathbb{Z}$ is squarefree and f has no root modulo ℓ. By [Sa14, Cor. 4.2] this implies that $C_d(\mathbb{Q}_\ell) = \emptyset$. It follows that

$$\mathfrak{D}_C \subset E'.$$

Let $E'(X)$ be the number of $d \in E'$ with $|d| \leq X$. Then [Ser76, Thm. 2.4] implies that if $0 < \beta < 1$ then there is $c > 0$ such that $E'(X) \sim \frac{cX}{\log^\beta X}$. Thus $\mathfrak{D}_C \ll \frac{X}{\log(X)^\beta}$. □

3.6 Unconditional Results

In this section, we provide an unconditional result on Hasse Principle violations in families of twists of certain superelliptic curves which map to curves of sufficiently large genus and few points. We adapt a theorem of Clark and Stankewicz ([CS18, Thm. 3]) and provide a proof of [Cl08, Thm. 4], to produce many twists which fail to have k-rational points and thus, combined with Lemma 3.3.1 yield many Hasse Principle violations within some families of twists.

Theorem 3.6.1 *Let k be a number field containing the pth roots of unity where p is prime. Let C/k be a smooth, projective, geometrically integeral curve, and let $\psi : C \longrightarrow C$ be a k-rational automorphism of order p. Assume the following hold:*

(i) $\{P \in C(k) : \psi(P) = P\} = \emptyset$.

(ii) $\{P \in C(\bar{k}) : \psi(P) = P\} \neq \emptyset$.

(iii) For some extension $L = k\left(d^{1/p}\right)$, the twist C_d has points everywhere locally.

(iv) The set $(C/\langle\psi\rangle)(k)$ is finite.

Then for all but finitely many d, the twisted curve C_d has no k-rational points.

Proof: Let L/k be a cyclic degree p extension. As k contains the pth roots of unity, by Kummer Theory, $L = k\left(d^{1/p}\right)$, for some pth power free $d \in k$. Let $Y := Y_L$ be the twist of C by ψ with respect to L/k. Then ψ defines a k-rational automorphism on Y. Let $\theta : G_k \longrightarrow Aut(C)$ be the 1-cocycle corresponding to the twist Y. For a generator σ of the Galois group of L/k, we have $\theta(\sigma) = \psi^j$ for some $j = j_\sigma \in (\mathbb{Z}/p\mathbb{Z})^*$. We have that $Y/_L \cong C/_L$, and σ acts on $Y(L)$ by $\sigma^*(P) = \psi^j\sigma(P)$. Thus, for all $P \in Y(A)$ (for any k-algebra A) we have

$$\sigma^*\psi(\sigma^*)^{-1} = (\psi^j\sigma)\psi(\psi^j\sigma)^{-1} = (\psi^j\sigma)\psi(\sigma^{-1}\psi^{-j}) = \psi^j(\sigma\psi\sigma^{-1})\psi^{-j} = \psi^j\psi\psi^{-j} = \psi \qquad .$$

We have natural maps

$$\kappa : Y_L(k) \hookrightarrow C(L)$$

and

$$\lambda : C(L) \to (C/\langle\psi\rangle)(L)$$

so that

$$S_L := (\lambda \circ \kappa)(Y_L(k)) \subseteq (C/\langle\psi\rangle)(k) \text{ and } (C/\langle\psi\rangle)(k) = \psi(C(k)) \cup \bigcup_{L=k(d^{1/p})} S_L.$$

For distinct degree p extensions of k, L_1 and L_2, $P \in S_{L_1} \cap S_{L_2} \implies P \in C(L_1) \cap C(L_2) = C(k)$ (since $[L_i : k]$ is prime and the extensions are distinct, $L_1 \cap L_2 = k$). If $P \in S_L \cap C(k)$, then $P = \lambda(\kappa(Q))$ for some $Q \in Y_L(k)$. As $\lambda(\kappa(Q)) \in (C/\langle\psi\rangle)(L)$, P is a fixed point of ψ, but by hypothesis, no such points are k-rational. Thus $S_{L_1} \cap S_{L_2} = \emptyset$ and $(C/\langle\psi\rangle)(k)$ is a disjoint union of the S_L. Since $(C/\langle\psi\rangle)(k)$ is finite, we conclude that there are only finitely many twists Y_L which have k-rational points. □

Corollary 3.6.2 *Let $C : y^n = f(x)$ be a superelliptic curve defined over a number field k with no k-rational superelliptic fixed points. Suppose $n = pN$ with $1 < N < n$ and p prime, and that k contains the pth roots of unity. Let $N(d) := |\mathcal{O}_k/(d)|$ denote the norm of d. Suppose that $Aut(C/\bar{k}) \cong \mu_n$ and that the curve $C^{(N)} : y^N = f(x)$ has finitely many k-rational points. Then as $X \to \infty$ the number of Nth power free $d \in \mathcal{O}_k$ such that C_d violates the Hasse Principle is $\gg_C \frac{X}{\log(X)}$. In particular, if the genus $g(C^{(N)}) \geq 2$ or if $C^{(N)}$ is an elliptic curve with finite Mordell-Weil rank over k, then C has many twists violating* *the Hasse Principle.*

Proof: We assume without loss of generality that C has points everywhere locally over k. From Lemma 3.3.1, there is a set of non-associate, totally positive prime elements $\pi \in \mathcal{O}_k$ such that C_π has points everywhere locally. We consider now the twists C_d where $d = \pi^p$. As before, there is $M \in \mathbb{Z}^+$ (depending on n and the genus and discriminant of C) such that for every prime ideal $\mathfrak{L}_v \neq (\pi)$, with $N\mathfrak{L}_v > M$, $C_d(k_v) \neq \emptyset$ (where v is the finite place correspdoning to $\mathfrak{L}_v$, and k_v the completion of k at v). For $\mathfrak{L}_v \neq (\pi)$ with $N\mathfrak{L}_v \leq M$, π, and hence d is an nth power in k_v, thus $C/_{k_v} \cong (C_d)/_{k_v}$, so $(C_d)/_{k_v} \neq \emptyset$. Finally, for $\mathfrak{L}_v = (\pi)$, by construction k_v contains a root of $f(x)$, and so $(C_d)/_{k_v} \neq \emptyset$ for every twist of C.

We take for $\langle\psi\rangle$ in Theorem 3.6.1 the unique subgroup of order p in $Aut(C/\bar{k})$. Then $(C/\langle\psi\rangle) \cong C^{(N)}$. By Theorem 3.6.1, only finitely many of the degree p-twists C_d, $d = \pi^p$ have k-rational points. □

3.6.1 Examples of the unconditional result

Examples satisfying the hypotheses of Cor 3.6.2 include hyperelliptic curves of the form $y^2 = x^{2\ell} - A$, where $\ell \geq 5$ (or $\ell = 3, 4$ and the genus 1 curve $y^2 = x^\ell - A$ has finitely many k-rational points) and A is not an 2ℓth power in k. In such cases, $y^2 = x^\ell - A$ has finitely many points, so by Thm. 3.6.1, only finitely many quadratic twists of $y^2 = x^{2\ell} - A$ (with respect to the automorphism $\tau(x, y) = (x, \zeta_\ell y))$ have k-rational points.

Additional examples include superelliptic curves defined by $y^4 = f(x)$ where $\deg(f) = 2m > 4$ (or $\deg(f) = 4$ and $y^2 = f(x)$ is of genus 1 and has only finitely many points k-rational points) and $f(x) \in k[x]$ has no k-rational roots. As the hyperelliptic curve $y^2 = f(x)$ has only finitely many rational points, there are only finitely many quadratic twists corresponding to the automorphism $(x, y^2) \mapsto (x, -y^2)$ which have k-rational points.

Appendix A

Varga's Theorem in Number Fields

A.1 Introduction

In this appendix, we include (with few changes) [CW18.1], joint work with P.L. Clark. In this work we contribute to the study of solution sets of systems of polynomial equations over a finite local principal ring when the input is restricted to some subset of the ring and the output is relaxed. In particular we generalize L. Varga's result on on solutions of polynomial equations with binary input variables and relaxed output variables to arbitrary number fields. We first state the following recent result to give an idea of the setting and scope of our work.

Let $n, a_1, \ldots, a_n \in \mathbb{Z}^+$ and $1 \leq N \leq \sum_{i=1}^n a_i$. Put

$$\mathfrak{m}(a_1, \ldots, a_n; N) = \begin{cases} 1 & \text{if } N < n \\ \min \prod_{i=1}^n y_i & \text{if } n \leq N \leq \sum_{i=1}^n a_i \end{cases};$$

the minimum is over $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ with $1 \leq y_i \leq a_i$ for all i and $\sum_{i=1}^n y_i = N$.

Theorem A.1.1 *([Cl18, Thm. 1.7]) Let R be a Dedekind domain, and let $\mathfrak{p}$ be a maximal ideal in R with finite residue field $R/\mathfrak{p} \cong \mathbb{F}_q$. Let $n, r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $A_1, \ldots, A_n, B_1, \ldots, B_r \subset R$ be nonempty subsets each having the property that no two distinct elements are congruent modulo $\mathfrak{p}$. Let $r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $P_1, \ldots, P_r \in R[t_1, \ldots, t_n]$ be nonzero polynomials, and put*

$$z_{\mathbf{A}}^{\mathbf{B}} := \#\{x \in \prod_{i=1}^{n} A_i \mid \forall 1 \le j \le m \ P_j(x) \in B_j \pmod{\mathfrak{p}^{v_j}}\}.$$

Then $z_{\mathbf{A}}^{\mathbf{B}} = 0$ or

$$z_{\mathbf{A}}^{\mathbf{B}} \ge \mathfrak{m}\left(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - \sum_{j=1}^{r} (q^{v_j} - \#B_j) \deg(P_j)\right).$$

Remark A.1.2 *For every finite local principal ring $\mathfrak{r}$, there is a number field K, a prime ideal $\mathfrak{p}$ of the ring of integers $\mathbb{Z}_K$ of K, and $v \in \mathbb{Z}^+$ such that $\mathfrak{r} \cong \mathbb{Z}_K/\mathfrak{p}^v$ [Ne71], [BC15]. Henceforth we will work in the setting of residue rings of $\mathbb{Z}_K$.*

If in Theorem A.1.1 we take $v_1 = \cdots = v_r = 1$, $A_i = \mathbb{F}_q$ for all i and $B_j = \{0\}$ for all j, then we recover a result of E. Warning.

Theorem A.1.3 *(Warning's Second Theorem [Wa35])*
Let $P_1, \ldots, P_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be nonzero polynomials, and let

$$\mathbf{z} = \#\{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid P_1(\mathbf{x}) = \cdots = P_r(\mathbf{x}) = 0\}.$$

Then $\mathbf{z} = 0$ or $\mathbf{z} \ge q^{n - \sum_{j=1}^{n} \deg(P_j)}$.

By Remark A.1.2, we may write $\mathbb{F}_q$ as $\mathbb{Z}_K/\mathfrak{p}$ for a suitable maximal ideal $\mathfrak{p}$ in the ring of integers $\mathbb{Z}_K$ of a suitable number field K. Having done so, Theorem A.1.3 can be interpreted in terms of solutions to a congruence modulo $\mathfrak{p}$, whereas Theorem A.1.1 concerns congruences modulo powers of $\mathfrak{p}$. At the same time, we are *restricting* the input variables $x_1, \ldots, x_n$ to lie in certain subsets $A_1, \ldots, A_n$ and also *relaxing* the output variables: we do not require that $P_j(x) = 0$ but only that $P_j(x)$ lies in a certain subset B_j modulo $\mathfrak{p}^{v_j}$.

There is however a tradeoff: Theorem A.1.1 contains the hypothesis that no two elements of any A_i (resp. B_j) are congruent modulo $\mathfrak{p}$. Thus, whereas when $v_j = 1$ for all j we are restricting variables *by choice* – e.g. we could take each A_i to be a complete set of coset representatives for $\mathfrak{p}$ in $\mathbb{Z}_K$ as done above – when $v_j > 1$ we are restricting variables *by necessity* – we cannot take A_i to be a complete set of coset representatives for $\mathfrak{p}^{v_j}$ in $\mathbb{Z}_K$.

We would like to have a version of Theorem A.1.1 in which the A_i's can be any nonempty finite subsets of $\mathbb{Z}_K$ and the B_j can be any nonempty finite subsets of $\mathbb{Z}_K$ containing $\{0\}$. However, to do so the degree conditions need to be modified in order to take care of the "arithmetic" of the rings $\mathbb{Z}_K/\mathfrak{p}^{d_j}$. In general this seems like a difficult – and worthy – problem.

An interesting special case was resolved in recent work of L. Varga [Va14]. His degree bound comes in terms of a new invariant of a subset $B \subset \mathbb{Z}/p^d\mathbb{Z} \setminus \{0\}$ called the **price of B** and denoted $\mathrm{pr}(B)$ that makes interesting connections to the theory of integer-valued polynomials.

Theorem A.1.4 *(Varga [Va14, Thm. 6]) Let $P_1, \ldots, P_r \in \mathbb{Z}[t_1, \ldots, t_n] \setminus \{0\}$ be polynomials without constant terms. For $1 \leq j \leq r$, let $d_j \in \mathbb{Z}^+$, and let $B_j \subset \mathbb{Z}/p^{d_j}\mathbb{Z}$ be a subset containing* 0*. If*

$$\sum_{j=1}^{r} \deg(P_j) \, \mathrm{pr}(\mathbb{Z}/p^{d_j}\mathbb{Z} \setminus B_j) < n,$$

then

$$\#\{\mathbf{x} \in \{0,1\}^n \mid \forall 1 \leq j \leq r, \; P_j(\mathbf{x}) \in B_j \pmod{p^{d_j}}\} \geq 2.$$

In this note we will revisit and extend Varga's work. Here is our main result.

Theorem A.1.5 *Let K be a number field of degree N, and let $e_1, \ldots, e_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathbb{Z}_K$, and let $d_1, \ldots, d_r \in \mathbb{Z}^+$. Let $P_1, \ldots, P_r \in \mathbb{Z}_K[t_1, \ldots, t_n]$*

be nonzero polynomials without constant terms. For each $1 \leq j \leq r$*, there are unique* $\{\varphi_{j,k}\}_{1 \leq k \leq N} \in \mathbb{Z}[t_1, \ldots, t_n]$ *such that*

$$P_j(t) = \sum_{k=1}^{N} \varphi_{j,k} e_j. \tag{A.1}$$

For $1 \leq j \leq r$*, let* B_j *be a subset of* $\mathbb{Z}_K/\mathfrak{p}^{d_j}$ *that contains* $0 \pmod{\mathfrak{p}^{d_j}}$*. Let*

$$S := \sum_{j=1}^{r} \left(\sum_{k=1}^{N} \deg(\varphi_{j,k}) \right) \operatorname{pr}(Z_K/\mathfrak{p}^{d_j} \setminus B_j).$$

Then

$$\#\{\mathbf{x} \in \{0,1\}^n \mid \forall 1 \leq j \leq r,\ P_j(\mathbf{x}) \pmod{\mathfrak{p}^{d_j}} \in B_j\} \geq 2^{n-S}.$$

Thus we extend Varga's Theorem A.1.4 from $\mathbb{Z}$ to $\mathbb{Z}_K$ and refine the bound on the number of solutions.

In §A.2 we discuss the price of a subset of $\mathbb{Z}_K/\mathfrak{p}^d$. It seems to us that Varga's definition of the price has minor technical flaws: as we understand it, he tacitly assumes that for an integer-valued polynomial $f \in \mathbb{Q}[t]$ and $m, n \in \mathbb{Z}$, the output $f(n)$ modulo m depends only on the input modulo m. This is not true: for instance if $f(t) = \frac{t(t-1)}{2}$, then $f(n)$ modulo 2 depends on n modulo 4, not just modulo 2. So we take up the discussion from scratch, in the context of residue rings of $\mathbb{Z}_K$.

The proof of Theorem A.1.5 occupies §A.3. After setting notation in §A.3.1 and developing some preliminaries on multivariate Gregory-Newton expansions in §A.3.2, the proof proper occurs in §A.3.3.

A.2 The Price

Consider the ring of **integer-valued polynomials**

$$\mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) = \{f \in K[t] \mid f(\mathbb{Z}_K) \subset \mathbb{Z}_K\}.$$

We have inclusions of rings

$$\mathbb{Z}_K[t] \subset \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \subset K[t].$$

Let

$$\mathfrak{m}(\mathfrak{p}, 0) := \{f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \mid f(0) \equiv 0 \pmod{\mathfrak{p}}\}.$$

Observe that $\mathfrak{m}(\mathfrak{p}, 0)$ is the kernel of a ring homomorphism $\mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \to \mathbb{Z}_K/\mathfrak{p}$: first evaluate f at 0 and then reduce modulo $\mathfrak{p}$. So $\mathfrak{m}(\mathfrak{p}, 0)$ is a maximal ideal of $\mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$. We put

$$\mathcal{U}(\mathfrak{p}, 0) := \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \setminus \mathfrak{m}(\mathfrak{p}, 0) = \{f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \mid f(0) \notin \mathfrak{p}\}.$$

Let $d \in \mathbb{Z}^+$, and let B be a subset of $\mathbb{Z}_K/\mathfrak{p}^d$. We say that $h \in \mathcal{U}(\mathfrak{p}, 0)$ **covers B** if: for all $b \in \mathbb{Z}_K$ such that $b \pmod{\mathfrak{p}^d} \in B$, we have $h(b) \in \mathfrak{p}$.

Definition A.2.1 *The **price of B**, denoted* $\mathrm{pr}(B)$*, is the least degree of a polynomial* $h \in \mathcal{U}(\mathfrak{p}, 0)$ *that covers* B*, or* ∞ *if there is no such polynomial.*

Remark A.2.2 *a) If* B_1*,* B_2 *are subsets of* $\mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$*, then*

$$\mathrm{pr}(B_1 \cup B_2) \leq \mathrm{pr}(B_1) + \mathrm{pr}(B_2):$$

If for $i = 1, 2$ *the polynomial* $h_i \in \mathcal{U}(\mathfrak{p}, 0)$ *covers* B_i *and has degree* d_i*, then* $h_1h_2 \in \mathcal{U}(\mathfrak{p}, 0)$ *covers* $B_1 \cup B_2$ *and has degree* $d_1 + d_2$*.*

b) If $0 \pmod{\mathfrak{p}^d} \in B$*, then* $\operatorname{pr}(B) = \infty$*:*

Since $0 \in B$ *we need* $h(0) \in \mathfrak{p}$*, contradicting* $h \in \mathcal{U}(\mathfrak{p}, 0)$*.*

c) If $d = 1$*, then for any subset* $B \subset \mathbb{Z}_K/\mathfrak{p} \setminus \{0\}$*, we have* $\operatorname{pr}(B) \leq \#B$*:*

Let $\tilde{B}$ *be any lift of* B *to* $\mathbb{Z}_K$*. Then*

$$h = \prod_{x \in \tilde{B}} (t - x) \in \mathbb{Z}_K[t] \subset \operatorname{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$$

covers B *and has degree* $\#B$*. Note that here we use polynoimals with* $\mathbb{Z}_K$*-coefficients. It is clear that* $\#B$ *is the minimal degree of a covering polynomial* h *with* $\mathbb{Z}_K$*-coefficients: we can then reduce modulo* $\mathfrak{p}$ *to get a polynomial in* $\mathbb{F}_q[t]$ *that we want to be* 0 *at the points of* B *and nonzero at* 0*, so of course it must have degree at least* $\#B$*.*

d) If we assume no element of B *is* 0 *modulo* $\mathfrak{p}$*, let* $\overline{B}$ *be the image of* B *under the natural map* $\mathbb{Z}_K/\mathfrak{p}^d \to \mathbb{Z}_K/\mathfrak{p} \cong \mathbb{F}_q$*; then our assumption gives* $0 \notin \overline{B}$*. Above we constructed a polynomial* $h \in \mathbb{Z}_K[t]$ *of degree* $\#\overline{B}$ *such that* $h(0) \notin \mathfrak{p}$ *and for all* $x \in \mathbb{Z}_K$ *such that* $x \pmod{\mathfrak{p}} \in B$*, we have* $h(x) \in \mathfrak{p}$*. This same polynomial* h *covers* B *and shows that* $\operatorname{pr}(B) \leq \operatorname{pr}(\overline{B}) \leq \#B$*.*

For $B \subset \mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$ we define $\kappa(B) \in \mathbb{Z}^+$, as follows. For $1 \leq i \leq d$ we will recursively define $B_i \subset \mathbb{Z}_K/\mathfrak{p}^i \setminus \{0\}$ and $k_{i-1} \in \mathbb{N}$.

- Put $B_d = B$, and let k_{d-1} be the number of elements of B_d that lie in $\mathfrak{p}^{d-1}$.
- Having defined B_i and k_{i-1}, we let B_{i-1} be the set of $x \in \mathbb{Z}_K/\mathfrak{p}^{i-1}$ such that there are more than k_{i-1} elements of B_i mapping to x under reduction modulo $\mathfrak{p}^{i-1}$. We let k_{i-2} be the number of elements of B_{i-1} that lie in $\mathfrak{p}^{i-2}$.

Notice that $0 \notin B_i$ for all i: indeed, B_i is defined as the set of elements x such that the fiber under the map $\mathbb{Z}_K/\mathfrak{p}^{i+1} \to \mathbb{Z}_K/\mathfrak{p}_i$ has more elements of B_{i+1} than does the fiber over 0. We put

$$\kappa(B) := \sum_{i=0}^{d-1} k_i q^i.$$

Lemma A.2.3 *We have $\kappa(B) \le q^d - 1$.*

Proof: Each k_i is a set of elements in a fiber of a q-to-1 map, so certainly $k_i \le q$. In order to have $k_i = q$, then B_{i+1} would need to contain the entire fiber over $0 \in \mathbb{Z}_K/\mathfrak{p}^i$, but this fiber includes $0 \in \mathbb{Z}_K/\mathfrak{p}^{i+1}$, which as above does not lie in B_{i+1}. So

$$\kappa(B) = \sum_{i=0}^{d-1} k_i q^i \le \sum_{i=0}^{d-1} (q-1)q^i = q^d - 1.\square$$

Theorem A.2.4 *For any subset $B \subset \mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$, we have* $\mathrm{pr}(B) \le \kappa(B)$*.*

Proof: Step 1: For $r \ge 1$, let $A = \{a_1, \ldots, a_{q^{d-1}}\} \subset \mathbb{Z}_K/\mathfrak{p}^d$ be a complete residue system modulo $\mathfrak{p}^{d-1}$ none of whose elements lie in $\mathfrak{p}^d$. We will show how to cover A with $f \in \mathcal{U}(\mathfrak{p}, 0)$ of degree q^{d-1}. We denote by $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation on K. Let $\lambda \in \mathbb{Z}_K$ be an element with $v_\mathfrak{p}(\lambda) = \sum_{j=0}^{d-2} q^j$, and let $\beta \in \mathbb{Z}_K$ be an element such that $v_\mathfrak{p}(\beta) = 0$ and for all nonzero prime ideals $\mathfrak{q} \ne \mathfrak{p}$ of $\mathbb{Z}_K$, we have $v_\mathfrak{q}(\beta) \ge v_\mathfrak{q}(\lambda)$. (Such elements exist by the Chinese Remainder Theorem.) Put

$$g_A(t) := \prod_{j=1}^{q^{d-1}} (t - a_j) \in \mathbb{Z}_K[t],\ h_A(t) := \frac{\beta}{\lambda} g_A(t) \in K[t].$$

For all $x \in \mathbb{Z}_K$, $\{x - a_1, \ldots, x - a_{q^{d-1}}\}$ is a complete residue system modulo $\mathfrak{p}^{d-1}$, so in $\prod_{j=1}^{q^{d-1}}(x - a_j)$, for all $0 \le j \le d-1$ there are q^{d-1-j} factors in $\mathfrak{p}^j$, so $v_\mathfrak{p}(g_A(x)) \ge \sum_{j=0}^{d-2} q^j$ and thus $v_\mathfrak{p}(h_A(x)) \ge 0$. For any prime ideal $\mathfrak{q} \ne \mathfrak{p}$ of $\mathbb{Z}_K$, both $v_\mathfrak{q}(g_A(x))$ and $v_\mathfrak{q}(\frac{\beta}{\lambda})$ are non-negative, so $v_\mathfrak{q}(h_A(x)) \ge 0$. Thus $h_A \in \operatorname{Int} \mathbb{Z}_K$. Moreover the condition that no a_j lies in $\mathfrak{p}^d$ ensures that $v_\mathfrak{p}(g_A(0)) = \sum_{j=0}^{d-2} q^j$, so $h_A \in \mathcal{U}(\mathfrak{p}, 0)$. If $x \in \mathbb{Z}_K$ is such that $x \equiv a_j \pmod{\mathfrak{p}^d}$ for some j, then $v_\mathfrak{p}(x - a_j) \ge d$. Since in the above lower bounds of $v_\mathfrak{p}(g_A(x))$ we

obtained a lower bound of at most $d-1$ on the $\mathfrak{p}$-adic valuation of each factor, this gives an extra divisibility and shows that $v_{\mathfrak{p}}(h_A(x)) \geq 0$. Thus h_A covers A with price at most q^{d-1}.
Step 2: Now let $B \subset \mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$. The number of elements of B that lie in $\mathfrak{p}^{d-1}$ is k_{d-1}. For each of these elements x_i we choose a complete residue system A_i modulo $\mathfrak{p}^{d-1}$ containing it; since no x_i lies in $\mathfrak{p}^d$ this system satisfies the hypothesis of Step 1, so we can cover each A_i with price at most q^{d-1} and thus (using Remark A.2.2a)) all of the A_i's with price at most $k_{d-1}q^{d-1}$. However, by suitably choosing the A_i's we can cover many other elements as well. Indeed, because we are choosing k_{d-1} complete residue systems modulo $\mathfrak{p}^{d-1}$, we can cover every element x that is congruent modulo $\mathfrak{p}^{d-1}$ to at most k_{d-1} elements of B. By definition of B_{d-1}, this means that we can cover all elements of B that do not map modulo $\mathfrak{p}^{d-1}$ into B_{d-1}. Now suppose that we can cover B_{d-1} by $h \in \mathcal{U}(\mathfrak{p}, 0)$ of degree κ'. This means that for every $x \in \mathbb{Z}_K$ such that $x \pmod{\mathfrak{p}^{d-1}}$ lies in B_{d-1}, $h(x) \in \mathfrak{p}$. But then every element of B whose image in $\mathfrak{p}^{d-1}$ lies in B_{d-1} is covered by h, so altogether we get

$$\mathrm{pr}(B) \leq k_{d-1}q^{d-1} + \mathrm{pr}(B_{d-1}).$$

Now applying the same argument successively to $B_{d-1}, \ldots, B_1$ gives

$$\mathrm{pr}(B_i) \leq k_{i-1}q^{i-1} + \mathrm{pr}(B_{i-1})$$

and thus

$$\mathrm{pr}(B) \leq \sum_{i=0}^{d-1} k_i q^i = \kappa(B).\Box$$

A.3 Proof of the Main Theorem

A.3.1 Notation

Let K be a number field of degree N, and let $e_1, \ldots, e_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. A $\mathbb{Z}$-basis for $\mathbb{Z}_K[t_1, \ldots, t_n]$ is given by $e_j \underline{t}^I$ as j ranges over elements of $\{1, \ldots, N\}$ and I ranges over elements of $\mathbb{N}^n$. So for any $f \in \mathbb{Z}_K[t_1, \ldots, t_n]$, we may write

$$f = \varphi_1(t_1, \ldots, t_n)e_1 + \ldots + \varphi_N(t_1, \ldots, t_n)e_N, \ \varphi_i \in \mathbb{Z}[t_1, \ldots, t_n]. \qquad \text{(A.2)}$$

Then we have

$$\deg f = \max_i \deg \varphi_i.$$

For a subset $B \subset \mathbb{Z}_K/\mathfrak{p}^d$, we put

$$\overline{B} = \mathbb{Z}_K/\mathfrak{p}^d \setminus B.$$

A.3.2 Multivariable Newton Expansions

Lemma A.3.1

If $f \in \mathbb{Q}[t]$ is a polynomial and $f(\mathbb{N}) \subset \mathbb{Z}$, then $f(\mathbb{Z}) \subset \mathbb{Z}$.

Proof: See e.g. [CC97, p. 2].

Theorem A.3.2

Let $f \in K[t]$.

a) There is a unique function $\alpha_\bullet(f) : \mathbb{N}^N \to K$, $\underline{r} \mapsto \alpha_{\underline{r}}(f)$ such that

(i) we have $\alpha_{\underline{r}}(f) = 0$ for all but finitely many $\underline{r} \in \mathbb{N}^N$, and

(ii) for all $x = x_1e_1 + \ldots + x_Ne_N \in \mathbb{Z}_K$, we have

$$f(x) = \sum_{\underline{r} \in \mathbb{N}^N} \alpha_{\underline{r}}(f) \binom{x_1}{r_1} \cdots \binom{x_N}{r_N}. \qquad \text{(A.3)}$$

b) The following are equivalent:

(i) We have $f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$*.*

(ii) For all $r \in \mathbb{N}^N$*,* $\alpha_{\underline{r}}(f) \in \mathbb{Z}_K$*.*

We call the $\alpha_{\underline{r}}(f)$ *the* ***Gregory-Newton coefficients*** *of* f*.*

Proof: Step 1: Let $f \in K[t]$. Let $e_1, \ldots, e_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. We introduce new independent indeterminates $t_1, \ldots, t_N$ and make the substitution

$$t = \sum_{k=1}^{N} e_k t_k$$

to get a polynomial

$$\tilde{f} \in K[\underline{t}].$$

This polynomial induces a map $K^N \to K$ hence, by restriction, a map $\mathbb{Z}^N \to K$. For $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, write $x = x_1 e_1 + \ldots + x_N e_N \in \mathbb{Z}_K$. Then we have

$$\tilde{f}(\underline{x}) = f(x).$$

Let $\mathcal{M} = \mathrm{Maps}(\mathbb{Z}^N, K)$ be the set of all such functions, and let $\mathcal{P}$ be the K-subspace of $\mathcal{M}$ consisting of functions obtained by evaluating a polynomial in $K[\underline{t}]$ on $\mathbb{Z}^N$, as above. By the CATS Lemma [Cl14, Thm. 12], the map $K[\underline{t}] \to \mathcal{P}$ is an isomorphism of K-vector spaces. Henceforth we will identify $K[\underline{t}]$ with $\mathcal{P}$ inside $\mathcal{M}$.

Step 2: For all $1 \leq k \leq N$, we define a K-linear endomorphism Δ_k of $\mathcal{M}$, the **kth partial difference operator**:

$$\Delta_k(g) : x \in \mathbb{Z}^N \mapsto g(x + e_k) - g(x).$$

These endomorphisms all commute with each other:

$$(\Delta_i \circ \Delta_j)(g) = g(x + e_i + e_j) - g(x + e_j) - g(x + e_i) + g(x) = (\Delta_j \circ \Delta_i)(g).$$

Let Δ_k^0 be the identity operator on $\mathcal{M}$, and for $i \in \mathbb{Z}^+$, let Δ_k^i be the i-fold composition of Δ_k. For $I = (i_1, \ldots, i_N) \in \mathbb{N}^N$, put

$$\Delta^I = \Delta^{i_1} \circ \ldots \circ \Delta^{i_N} \in \operatorname{End}_K(\mathcal{M}).$$

When we apply Δ_k to a monomial $\underline{t}^I$, we get another polynomial. More precisely, if $\deg_{t_k}(\underline{t}^I) = 0$ then $\Delta_k \underline{t}^I$ is the zero polynomial; otherwise

$$\deg_{t_k}(\Delta_k \underline{t}^I) = (\deg_{t_k} \underline{t}^I) - 1; \ \forall l \neq k, \deg_{t_l}(\Delta_k \underline{t}^I) = \deg_{t_l} \underline{t}^I.$$

Thus for each $f \in \mathcal{P}$, for all but finitely many $I \in \mathbb{N}^N$, we have that $\Delta^I(f) = 0$.

For the one variable difference operator, we have

$$\Delta \binom{x}{r} = \binom{x+1}{r} - \binom{x}{r} = \binom{x}{r-1}.$$

From this it follows that for $I, \underline{r} \in \mathbb{N}^N$ we have

$$\Delta^I \left(\binom{x_1}{r_1} \cdots \binom{x_N}{r_N} \right) (\underline{0}) = \binom{0}{r_1 - i_1} \cdots \binom{0}{r_N - i_N} = \delta_{\underline{r}, I} \tag{A.4}$$

So if $\beta_\bullet : \mathbb{N}^N \to K$ is any finitely nonzero function then for all $I \in \mathbb{N}^N$ we have

$$\Delta^I (\sum_{\underline{r} \in \mathbb{N}^N} \beta_{\underline{r}} \binom{x_1}{r_1} \cdots \binom{x_N}{r_N})(\underline{0}) = \beta_I, \tag{A.5}$$

and thus there is at most one such function satisfying (A.3), namely

$$\alpha_\bullet(f) : \underline{r} \mapsto \Delta^{\underline{r}}(f)(\underline{0}).$$

So for any $f \in \mathcal{M}$ and $\underline{r} \in \mathbb{N}^N$, we define the **Gregory-Newton coefficient**

$$\alpha_{\underline{r}}(f) := \Delta^{\underline{r}}(f)(\underline{0}) \in K.$$

We may view the assignment of the package $\{\alpha_{\underline{r}}(f)\}_{\underline{r} \in \mathbb{N}^N}$ of Gregory-Newton coefficients to $f \in \mathcal{M}$ as a K-linear mapping

$$\mathcal{M} \to K^{\mathbb{N}^N}.$$

If we put $\mathcal{M}^+ = \text{Maps}(\mathbb{N}^N, K)$, then we get a factorization

$$\mathcal{M} \to \mathcal{M}^+ \xrightarrow{\alpha} K^{\mathbb{N}^N},$$

where the first map restricts from $\mathbb{Z}^N$ to $\mathbb{N}^N$, and the factorization occurs because the Gregory-Newton coefficients depend only on the values of f on $\mathbb{N}^N$. We make several observations:

First Observation: The map α is an isomorphism. Indeed, knowing all the successive differences at 0 is equivalent to knowing all the values on $\mathbb{N}^N$, and all possible packages of Gregory-Newton coefficients arise. Namely, let S_n be the assertion that for all $x \in \mathbb{N}^N$ with $\sum_k x_k = n$ and all $f \in \mathcal{M}$, then $f(x)$ is a $\mathbb{Z}$-linear combination of its Gregory-Newton coefficients. The case $n = 0$ is clear: $f(0) = \alpha_0(f)$. Suppose S_n holds for n, let $x \in \mathbb{N}^N$ be such that $\sum_k x_k = n + 1$, and choose k such that $x = y + e_k$; thus $\sum_k y_k = n$. Then

$$f(x) = f(y) + \Delta_k f(y).$$

By induction, $f(y)$ is a $\mathbb{Z}$-linear combination of the Gregory-Newton coefficients of f and $\Delta_k f(y)$ is a $\mathbb{Z}$-linear combination of the Gregory-Newton coefficients of $\Delta_k f$. But every Gregory-Newton coefficient of $\Delta_k f$ is also a Gregory-Newton coefficient of f, completing the induction.

Second Observation: The composite map

$$K[\underline{t}] \to \mathcal{M} \to \mathcal{M}^+ \xrightarrow{\alpha} K^{\mathbb{N}^N}$$

is an injection. Indeed, the kernel of $\mathcal{M} \to K^{\mathbb{N}^N}$ is the set of functions that vanish on $\mathbb{Z}^N \setminus \mathbb{N}^N$. In particular, any element of the kernel vanishes on the infinite Cartesian subset $(\mathbb{Z}^{<0})^N$ and thus by the CATS Lemma is the zero polynomial.

Third Observation: For a subring $R \subset K$ and $f \in \mathcal{M}$, we have $f(\mathbb{N}^N) \subset R$ iff all of the Gregory-Newton coefficients of f lie in R. This is a consequence of the First Observation: the Gregory-Newton coefficients are $\mathbb{Z}$-linear combinations of the values of f on $\mathbb{N}^N$ and conversely.

Step 3: For $F \in K[\underline{t}]$, we define the **Newton expansion**

$$T(F) = \sum_{\underline{r} \in \mathbb{N}^N} \alpha_{\underline{r}}(F) \binom{t_1}{r_1} \cdots \binom{t_N}{r_N} \in K[\underline{t}].$$

This is a finite sum. Moreover, by definition of $\alpha_{\underline{r}}(F)$ and by (A.5) we get that for all $r \in \mathbb{N}^N$,

$$\alpha_{\underline{r}}(T(F)) = \alpha_{\underline{r}}(F).$$

It now follows from Step 2 that $T(F) = F \in K[\underline{t}]$. Applying this to the $\tilde{f}$ associated to $f \in K[t]$ in Step 1 completes the proof of part a).

Step 4: If we assume that $f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$ then $\tilde{f}(\mathbb{Z}^N) \subset \mathbb{Z}_K$ so all the Gregory-Newton coefficents lie in $\mathbb{Z}_K$. Conversely, if all the Gregory-Newton coefficients of $\tilde{f}$ lie in $\mathbb{Z}_K$, then for $x = x_1 e_1 + \ldots + x_N e_N \in \mathbb{Z}_K$, by Lemma A.3.1 and (A.3) we have $f(x) = \tilde{f}(x_1, \ldots, x_N) \in \mathbb{Z}_K$, so $f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$.

A.3.3 Proof of Theorem A.1.5

We begin by recalling the following result.

Theorem A.3.3 *Let F be a field, and let $P \in F[t_1, \ldots, t_n]$ be a polynomial. Let*

$$\mathcal{U} \coloneqq \{\mathbf{x} \in \{0,1\}^n \mid P(\mathbf{x}) \neq 0\}.$$

Then either $\#\mathcal{U} = 0$ or $\#\mathcal{U} \geq 2^{n-\deg(P)}$.

Proof: This is a special case of a result of Alon-Füredi [AF93, Thm. 5].

We now turn to the proof of Theorem A.1.5. Put

$$Z \coloneqq \{x \in \{0,1\}^n \mid \forall 1 \leq j \leq r,\ P_j(x) \pmod{\mathfrak{p}^{d_j}} \in B_j\}.$$

Step 0: If $q = \#\mathbb{Z}_K/\mathfrak{p}$ is a power of p, then we have $p^d \in \mathfrak{p}^d$. Therefore in (A.1) if we modify any coefficient of $\varphi_{j,k}(t)$ by a multiple of p^d, it does not change P_j modulo $\mathfrak{p}^d$ and thus does not change the set Z. We may thus assume that every coefficient of every $\varphi_{j,k}$ is non-negative.

Step 1: For $w = \sum_{i=1}^{k} \underline{t}^{I_i}$ a sum of monomials and $0 \leq r \leq k$, we put

$$\Psi_r(w) \coloneqq \sum_{1 \leq i_1 < i_2 < \ldots < i_r \leq k} \underline{t}^{I_{i_1}} \cdots \underline{t}^{I_{i_r}}.$$

For $x \in \{0,1\}^n$, we have $w(x) = \#\{1 \leq i \leq k \mid x^{I_i} = 1\}$, so

$$\Psi_r(w)(x) = \binom{w(x)}{r}.$$

For $f \in \mathbb{Z}_K[t_1, \ldots, t_n]$, write $f = \sum_{k=1}^{N} \varphi_k(t) e_k$ and suppose that all the coefficients of each

φ_k are non-negative – equivalently, each $\varphi_k(t)$ is a sum of monomials. For $\underline{r} \in \mathbb{N}^N$, we put

$$\Psi_{\underline{r}}(f) \coloneqq \Psi_{r_1}(\varphi_1) \cdots \Psi_{r_N}(\varphi_N) \in \mathbb{Z}[\underline{t}].$$

For $h \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$ with Gregory-Newton coefficients $\alpha_{\underline{r}}$, we put

$$\Psi^h(f) \coloneqq \sum_{\underline{r} \in \mathbb{N}^N} \alpha_{\underline{r}} \Psi_{\underline{r}}(f) \in \mathbb{Z}_K[\underline{t}].$$

For $x \in \{0,1\}^n$, we have

$$\Psi_{\underline{r}}(x) = \prod_{k=1}^{N} \binom{\varphi_k(x)}{r_k},$$

so using (A.2) we get

$$\Psi^h(f)(x) = \sum_{\underline{r}} \alpha_{\underline{r}} \Psi_{\underline{r}}(f)(x) = \sum_{\underline{r}} \alpha_{\underline{r}} \binom{\varphi_1(x)}{r_1} \cdots \binom{\varphi_N(x)}{r_N}$$

$$= h(\varphi_1(x)e_1 + \ldots + \varphi_N(x)e_N) = h(f(x)).$$

Step 2: For $1 \leq j \leq r$, let $h_j \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$ have degree $\mathrm{pr}(\overline{B_j})$ and cover $\overline{B_j}$. Put

$$F \coloneqq \prod_{j=1}^{r} \Psi^{h_j}(P_j) \pmod{\mathfrak{p}} \in \mathbb{Z}_K/\mathfrak{p}[\underline{t}] = \mathbb{F}_q[\underline{t}].$$

Note that

$$\deg(F) \leq \sum_{j=1}^{r} \deg \Psi^{h_j}(P_j) \leq \sum_{j=1}^{r} \left(\deg(h_j) \sum_{k=1}^{n} \deg(\varphi_{j,k}) \right) = S.$$

Here is the key observation: for $x \in \{0,1\}^n$, if $F(x) \neq 0$, then for all $1 \leq j \leq r$ we have $\mathfrak{p} \nmid \Psi^{h_j}(P_j)(x) = h_j(P_j(x))$, so $P_j(x) \pmod{\mathfrak{p}^{d_j}} \notin \overline{B_j}$, and thus $x \in Z$.

Step 3: For all $1 \leq j \leq r$ we have $P_j(0) = 0$ and $h_j \in \mathcal{U}(\mathfrak{p}, 0)$, so $h_j(0) \notin \mathfrak{p}$, so

$$F(0) = \prod_{j=1}^{r} \Psi_j^h(P_j(0)) = \prod_{j=1}^{r} h_j(P_j(0)) \pmod{\mathfrak{p}} = \prod_{j=1}^{r} h_j(0) \pmod{\mathfrak{p}} \neq 0.$$

Applying Alon-Füredi to F, we get

$$\#Z \geq \#\{x \in \{0,1\}^n \mid F(x) \neq 0\} \geq 2^{n-\deg F} \geq 2^{n-S},$$

completing the proof of Theorem A.1.5.

Appendix B

Euclid-Mullin-like Sequences

In this appendix, we include joint work with J. Clark ([CWxx]) in which we study variations on the second Euclid-Mullin sequence, an infinite sequence of primes which arises from a variation on Euclid's proof of the infinitude of primes. Booker showed this sequence omits infinitely many primes. Pollack and Treviño reproved the result using completely elementary means. We adapt the Pollack and Treviño argument to show certain related sequences also omit infinitely many primes.

B.1 Introduction

One version of Euclid's well-known proof of the infinitude of primes is as follows: Start with $q_1 = 2$. With a list of primes $q_1, \dots, q_{n-1}$ having been determined, the sequence is continued by choosing the nth prime q_n to be a prime divisor of $1+\prod_{i=1}^{n-1} q_i$. Since $1+\prod_{i=1}^{n-1} q_i$ is relatively prime to the first $n-1$ primes in the sequence, at each step we find a new prime, and we conclude that there must be infinitely many primes.

Note that at a given step, $1 + \prod_{i=1}^{n-1} q_i$ may be composite, and as such there may be several choices for q_n. In 1963, Mullin [Mu63] suggested generating the sequence $\{q_i\}_{i=1}^{\infty}$

by placing some restrictions on the choice of q_n. Rather than allowing *any* choice of prime divisor of $1 + \prod_{i=1}^{n-1} q_i$, one can require that the smallest prime divisor be chosen. In this way, we obtain the first Euclid-Mullin sequence. Alternatively, one can require that at each step the greatest prime divisor is chosen. This leads to the second Euclid-Mullin sequence. For each sequence, Mullin asked whether every prime appears as a term in the sequence. In the case of the first Euclid-Mullin sequence, this question is still open; in fact, it is unknown whether 41 appears as a term in the sequence.

For the second Euclid-Mullin sequence, much more is known. In 1967, Cox and van der Poorten [CV68] showed that the second Euclid-Mullin sequence omits every prime $p \leq 53$ besides $2, 3, 7$, and 43, and they conjectured that infinitely many primes are omitted by the sequence. In 2012, Booker [BO12] proved their conjecture.

In their paper, Cox and van der Poorten showed that if certain primes appeared, the second Euclid-Mullin sequence would satisfy an inconsistent system of congruences. In his proof, Booker used this same essential idea to prove Cox and van der Poorten's conjecture. In 2014 Pollack and Treviño [PT14] provided an elementary version of Booker's argument (again, based on an inconsistent system of congruences). It is this more elementary argument we adapt below for certain Euclid-Mullin-like sequences. Specifically, we construct sequences denoted $EML(a, c; q)$, depending on a given prime q, a scaling factor c, and a "shift" a, which omit infinitely many primes. We then construct a Euclid-Mullin-like sequence in the ring $\mathbb{Z}[i]$ and attempt an adaptation of the Pollack and Treviño proof to this sequence.

B.2 Euclid-Mullin-Like sequences

To construct a Euclid-Mullin-like sequence, we proceed as follows: We fix integers a and c and a prime $q_1 = q$. Having chosen the first $n - 1$ primes of the sequence, we choose the nth prime to be the largest prime divisor of $a + c \prod_{i=1}^{n-1} q_i$. We refer to the sequence arising from these choices as the $EML(a, c; q)$ sequence. The second Euclid-Mullin sequence, for example, is the $EML(1, 1; 2)$ sequence.

B.2.1 The second Euclid-Mullin sequence

Theorem B.2.1 (Booker) *The $EML(1, 1; 2)$ sequence omits infinitely many primes*

Booker's proof has two key components: one being quadratic reciprocity and the other a result on upper bounds for certain character sums. Pollack and Treviño also use quadratic reciprocity, but they exchange the bounds on character sums for simpler-to-prove statements about distributions of squares and non squares modulo a prime. Their elementary proof comes at the expense of worse quantitative bounds. Since our work adapts the elementary argument, presumably each of the bounds given below could be improved by using bounds on character sums.

B.3 EML sequences missing infinitely many primes

In this section, we present a full proof that the sequence $EML(2, c; 3)$ omits infinitely many primes when c is an odd positive integer. We then explain the changes needed to adapt the proof to other EML sequences. To begin with, we state a lemma regarding quadratic residues and non residues.

Lemma B.3.1 (Pollack and Treviño) *If p is an odd prime, then the length of any sequence of consecutive squares modulo p is strictly less than $2\sqrt{p}$.*

Theorem B.3.2 *The sequence $EML(2, c; 3)$ misses infinitely many primes for each $c \in \mathbb{Z}^+$*

The theorem is a consequence of the following proposition:

Theorem B.3.3 *Let $q_1 = 3$ and let c be an odd positive integer. Let $Q_1, \ldots, Q_r$ be the smallest r primes omitted from $EML(2, c; 3)$ (we allow the possibility that $r = 0$, in which case $Q_1 \cdots Q_r$ is the empty product). Then there is another omitted prime smaller than*

$$X = 12^2 \left(\prod_{i=1}^{r} Q_i \right)^2.$$

Proof: Suppose by way of contradiction that every prime $p \leq X$ except $Q_1, \ldots, Q_r$ appears in the sequence. Let p be the prime in $[2, X]$ that is last to appear in the sequence $\{q_i\}$, and say p is the nth term q_n. Then p is the largest prime dividing $2 + cq_1 \cdots q_{n-1}$. Since every prime smaller than p that is not one of the Q_i must be one of $q_1, \ldots, q_{n-1}$, the only other possible prime factors of $2 + cq_1 \cdots q_{n-1}$ are $Q_1, \ldots, Q_r$. So,

$$2 + cq_1 \cdots q_{n-1} = Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r} p^e$$

for some exponents $e_1, \ldots, e_r \geq 0$ and $e \geq 1$. We claim that it is possible to choose a natural number $d \leq X$ satisfying the following conditions

$$d \equiv 5 \pmod 8, \qquad d \equiv 1 \pmod{Q_1 \cdots Q_r} \tag{B.1}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{1}{p}\right). \tag{B.2}$$

Suppose such a d exists. Since $d \leq X$ and d is coprime to $Q_1 \cdots Q_r p$, every prime dividing d is among the primes $q_1, \ldots, q_{n-1}$. So if we write $d = d_0 d_1^2$, where d_0 is squarefree, then $d_0 \mid cq_1 \cdots q_{n-1}$ and $d_0 \equiv 5 (\text{mod } 8)$. Hence,

$$\left(\frac{d}{2+cq_1\cdots q_{n-1}}\right)=\left(\frac{2+cq_1\cdots q_{n-1}}{d}\right)=\left(\frac{2+cq_1\cdots q_{n-1}}{d_0}\right)\left(\frac{2+cq_1\cdots q_{n-1}}{d_1^2}\right)$$
$$=\left(\frac{2}{d_0}\right)\left(\frac{2+cq_1\cdots q_{n-1}}{d_1^2}\right)=\left(\frac{2}{d_0}\right)\left(\frac{2+cq_1\cdots q_{n-1}}{d_1}\right)^2=-1\cdot 1=-1.$$

The first and fourth equality are each using that $d\equiv 5 \pmod 8$. On the other hand, we also have $\left(\frac{d}{Q_i}\right)=\left(\frac{1}{Q_i}\right)$ for each $i=1,2,\ldots,r$, and $\left(\frac{d}{p}\right)=\left(\frac{1}{p}\right)$ by (B.2), so

$$\begin{aligned}\left(\frac{d}{2+cq_1\cdots q_{n-1}}\right)&=\left(\prod_{i=1}^{r}\left(\frac{d}{Q_i}\right)^{e_i}\right)\cdot\left(\frac{d}{p}\right)^e\\&=\left(\prod_{i=1}^{r}\left(\frac{1}{Q_i}\right)^{e_i}\right)\cdot\left(\frac{1}{p}\right)^e\\&=\left(\frac{1}{2+cq_1\cdots q_{n-1}}\right)=1.\end{aligned}$$

This is a contradiction.

We now establish that there is an integer $d\le X$ satisfying (B.1) and (B.2). Condition (B.1) is satisfied for any $d=Mk+A$, where $M:=4Q_1\cdots Q_r$ and $A:=2Q_1\cdots Q_r+1$ (though $Q_1\cdots Q_r$ may be the empty product as noted earlier, in this case as $2+cq_1\cdots q_{n-1}$ is always odd, we take $Q_1=2$). To obtain (B.2), we look for a small nonnegative integer k with $\left(\frac{Mk+A}{p}\right)=\left(\frac{1}{p}\right)$. Equivalently, fixing M' satisfying $MM'\equiv 1 \pmod p$, we seek a nonnegative integer k with

$$\left(\frac{k+AM'}{p}\right)=\left(\frac{M'}{p}\right).$$

By Lemma 3.1 we know the longest run of quadratic residues or non residues is less than

$2\sqrt{p}$, so we can find $0 \leq k < 2\sqrt{p}$. Then the corresponding d satisfies

$$0 < d = Mk + A < 2M\sqrt{p} + M < 3M\sqrt{p} \leq 3M\sqrt{X}.$$

Since $3M = 12Q_1 \cdots Q_r = \sqrt{X}$, we find that $d < X$, thus completing the proof.

Proposition B.3.4 *For a positive odd integer c and a positive integer j, the sequences $EML(1, c; 2)$, $EML(1, 2c; 2)$,$EML(-1, c; 2)$ and $EML(-1, 2^j c; 2)$ omit infinitely many primes.*

Each of the above statements follows from propositions similar to Theorem 3.3. In what follows, we make several conventions. First, $Q_1, \ldots, Q_r$ are the first r primes omitted by the sequence (where we again allow $r = 0$). Second, for each sequence we assume p is the last prime in $[2, X]$ to appear in the sequence (say p is the nth term), where X is some integer depending on the sequence. Third, as $q_1 = 2$, we assume without loss of generality that $n > 1$ so that $q_n = p > 2$ and we can freely use the Jacobi symbol to obtain the necessary contradictions. The other changes needed for each of the proofs are provided below.

(a) For the sequence $EML(1, c; 2)$, Pollack and Treviño's proof works with only cosmetic changes. In place of (B.1) and (B.2) we require $d < X = 12^2 \left(\prod_{i=1}^{r} Q_i\right)^2$ such that

$$d \equiv 1 \pmod{4}, \;\; d \equiv -1 \pmod{Q_1 \cdots Q_r} \tag{B.3}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right). \tag{B.4}$$

The conditions are then satisfied by an integer $d = Mk + A$ where $M \coloneqq 4Q_1 \cdots Q_r$,

$A := 2Q_1 \cdots Q_r - 1$, and $k < 2\sqrt{p}$.

(b) For the sequence $EML(1, 2c; 2)$ we require $d < X = 6^2 \left(\prod_{i=1}^r Q_i\right)^2$ such that

$$d \equiv 2 \pmod{Q_1 \cdots Q_r} \tag{B.5}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right). \tag{B.6}$$

The conditions are satisfied by $d = Mk + 2$, where $M := 2Q_1 \cdots Q_r$ and $k < 2\sqrt{p}$.

(c) For the sequence $EML(-1, c; 2)$ we require $d < X = 12^2 \left(\prod_{i=1}^r Q_i\right)^2$ such that

$$d \equiv 3 \pmod{4} \qquad\qquad d \equiv 1 \pmod{Q_1 Q_2 \cdots Q_r} \tag{B.7}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{1}{p}\right), \tag{B.8}$$

The conditions are satisfied by $d = Mk + A$, where $M := 4Q_1 \cdots Q_r$, $A := 2Q_1 \cdots Q_r + 1$ and $k < 2\sqrt{p}$.

(d) For the sequence $EML(-1, 2^j c; 2)$ we require $d < X = 12^2 \left(\prod_{i=1}^r Q_i\right)^2$ such that

$$d \equiv 1 \pmod{4}, \;\; d \equiv -1 \pmod{Q_1 Q_2 \cdots Q_r} \tag{B.9}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right). \tag{B.10}$$

The conditions are satisfied by $d = Mk + A$, where $M \coloneqq 4Q_1 \cdots Q_r$, $A \coloneqq 2Q_1 \cdots Q_r - 1$ and $k < 2\sqrt{p}$.

B.4 Where Difficulties Arise

B.4.1 $EML(1, 4; 2)$

Suspiciously, we have proofs that the sequences $EML(1, c; 2)$ and $EML(1, 2c; 2)$ omit infinitely many primes for c odd, but have not provided proofs that the sequences $EML(1, 2^j c; 2)$ omit infinitely many primes for $j > 1$. It is in these cases that difficulties begin to arise. In the proofs given above, we arrive at a contradiction by showing that for the denominator $a + cq_1 \cdots q_{n-1}$ and a carefully chosen numerator d the Jacobi symbol is not well-defined. We do this by first flipping the symbol and considering only the value of the Jacobi symbol on the square-free part of d and then by using the multiplicativity of the symbol to show that with the exact same numerator and denominator, the Jacobi symbol takes on the opposite value. To achieve this contradiction, we must be able to show that either due to the shift a in the sequence $EML(a, c; q)$ and/or due to congruence conditions placed on d, the symbol $\left(\frac{d}{a+cq_1\cdots q_{n-1}}\right)$ will, when viewed properly, return a value of -1.

If we look at the proof of Theorem 3.3, for example, we see that with the shift of $a = 2$ and the condition that d (and hence the square-free part of d) is $5 \pmod 8$, the Jacobi symbol returns -1 after we flip the symbol. We can then easily control congruence conditions to force the symbol to return 1 when viewed differently. When we have a sequence $EML(1, 2^j c; 2)$, for $j > 1$, however, the argument breaks down. In this case, since $q_1 = 2$ and $j > 1$, we are ultimately considering how the Jacobi symbol behaves when its denominator $1+2^j cq_1 \cdots q_{n-1}$ is congruent to 1 modulo 8. Crucially, we need d to be small enough so that all of its prime divisors are among the primes $2, q_2, \ldots, q_{n-1}$ and the primes dividing c. If for such a d, we try to invert the symbol and then consider how it behaves we are forced to conclude that $\left(\frac{d}{1+2^j cq_1 \cdots q_{n-1}}\right) = \left(\frac{1}{d_0}\right)$ (d_0 being the square free part of d), which is always 1, no matter what d_0 is. In the other direction, since $1+2^j cq_1 \cdots q_{n-1}$ is $1 \pmod 8$, it is difficult to find a numerator $*$ so that $\left(\frac{*}{1+2^j cq_1 \cdots q_{n-1}}\right)$ is -1. This then hints at a limitation to the arguments used above: when working with the sequence $EML(a, c; q)$, if a is a square and $a + cq_1 \cdots q_{n-1}$ does not have any obvious non-square residue classes, deriving a contradiction using the Jacobi symbol becomes harder. What, then, can be shown?

For $EML(1, 4; 2)$, at least, we can show that not every prime appears in the sequence. To show this, we start with the following lemma:

Lemma B.4.1 *If $t = 1 + 4q_1 \cdots q_n$, then $t \neq x^4$ for any $x \in \mathbb{Z}$.*

Proof: Suppose $t = x^4$. Then $1 + 4q_1 \cdots q_n = x^4$, so:

$$4q_1 \cdots q_n = x^4 - 1 = (x-1)(x+1)(x^2+1)$$

Since t is odd implies x is odd, each of $x-1,\ x+1,\ x^2+1$ must be even. Since then either $(x-1)$ or $(x+1) \equiv 0 (\text{mod } 4)$, the right hand side is divisible by 2^4. But the left hand side is only divisible by 2^3 since $q_1 = 2$ and the other primes are odd.

Proposition B.4.2 *The prime 7 does not appear in the sequence $EML(1, 4; 2)$.*

Proof: One can check that for this sequence, $q_2 = 3$ and $q_3 = 5$. Then since every prime less than 7 appears as some q_i, if 7 appears as the largest prime divisor of $1 + 4q_1 \cdots q_{n-1}$ for some n then 7 must be the only prime divisor. So $1 + 4q_1 \cdots q_{n-1} = 7^m$ for some m. Considering this equality $\pmod 5$, we see that

$$1 + 4q_1 \cdots q_n = 7^m \equiv 2^m \pmod{5}$$

Since q_3=5 we have

$$1 \equiv 2^m \pmod{5},$$

thus $m \equiv 0 \pmod{4}$. Therefore $1 + 4q_1 \cdots q_n$ must be a fourth power, contradicting the lemma.

B.5 Beyond the Integers

Euclid's proof that there are infinitely many primes works with minor changes in rings other than $\mathbb{Z}$ (see for example [Cl17]). One might hope that analogues of Euclid-Mullin-like sequences might arise in other rings as well. To that end we next consider a Euclid-Mullin-like sequence in the ring of Gaussian integers $\mathbb{Z}[i]$. As when working over $\mathbb{Z}$, we can consider sequences of prime elements in $\mathbb{Z}[i]$. Other notions will need to be reinterpreted for our new setting. When constructing our sequence and obtaining the nth prime, say ω, we will need to choose among four associate primes (if ω is prime, then so are $-\omega$ and $\pm i\omega$). We say an integer $\alpha = a + bi \in \mathbb{Z}[i]$, is *odd* if its norm $N(\alpha) = a^2 + b^2$ is odd; we say an odd integer α is *primary* if $\alpha \equiv 1 \pmod{(i+1)^3}$. In our sequence, we will choose at each step the unique primary associate of a prime ω. Rather than using quadratic reciprocity and the Jacobi symbol, we use biquadratic reciprocity and the biquadratic residue symbol, which we review below. The biquadratic residue symbol is best understood when dealing with primary integers; it is for this reason we choose the primary associate of a prime at each step.

B.5.1 Biquadratic Reciprocity

Biquadratic (or quartic) reciprocity is the appropriate tool to use in place of quadratic reciprocity when working with prime elements in $\mathbb{Z}[i]$. Rather than using the Jacobi symbol $\left(\frac{a}{n}\right)$ to detect when an integer a is a quadratic residue modulo an odd prime $n \in \mathbb{Z}$, we use the biquadratic symbol $\left[\frac{\alpha}{\pi}\right]$ to detect wheter an element $\alpha \in \mathbb{Z}[i]$ is a biquadratic residue (i.e., fourth-power) modulo an odd prime $\pi \in \mathbb{Z}[i]$. There is a unique integer $0 \leq k \leq 3$ such that $\alpha^{(N(\pi)-1)/4} \equiv i^k \pmod{\pi}$ and $\left[\frac{\alpha}{\pi}\right]$ is defined to be i^k. In particular, $\left[\frac{\alpha}{\pi}\right] = 1$ if and only if $x^4 - \alpha$ has a solution modulo π. Below, we summarize relevant facts about primary integers and biquadratic reciprocity, and extend the biquadratic symbol to arbitrary primary integers (see [Le00]).

- We extend the symbol so that, if the numerator is kept fixed, then the symbol is totally multiplicative.. That is, if $\beta = \pi_1^{e_1} \cdots \pi_n^{e_n}$, then
$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\pi_1}\right]^{e_1} \cdots \left[\frac{\alpha}{\pi_n}\right]^{e_n}.$$

- An element $\alpha = a + bi$ in $\mathbb{Z}$[i] is primary if and only if either $a \equiv 1 \pmod{4}$ and $b \equiv 0 \pmod{4}$ or $a \equiv 3 \pmod{4}$ and $b \equiv 2 \pmod{4}$.

- If α and β are primary, then $\alpha\beta$ is primary.

- If α and β are primary and relatively prime non-units, then $\left[\frac{\alpha}{\beta}\right] = \left[\frac{\beta}{\alpha}\right] \cdot (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}}$.

- If θ and π are primary primes, then $\left[\frac{\theta}{\pi}\right] = \left[\frac{\pi}{\theta}\right]$ whenever θ or π is $\equiv 1 \pmod{4}$.

- If β is a primary integer, then $\left[\frac{1+i}{\beta}\right] = i^{(Re(\beta)-Im(\beta)-Im(\beta)^2-1)/4}$.

B.5.2 Conditional case of Euclid-Mullin-like Sequences in the Gaussian Integers

Definition B.5.1 (*EML for $\mathbb{Z}[i]$*) *Let $\omega_1 = 1 + i$. Supposing ω_j has been defined for $1 \leq j \leq n$, continue the sequence by choosing ω_{n+1} such that ω_n is a primary prime of largest norm dividing $1 + 2\omega_1 \cdots \omega_{n-1}$. We will call the sequence $\{\omega_n\}_{n=1}^{\infty}$ the Euclid-Mullin-like (EML) sequence.*

Table B.1: First terms in the Euclid-Mullin-like sequence for the Gaussian integers

ω_1	$1 + i$
ω_2	$3 + 2i$
ω_3	$3 + 10i$
ω_4	$-93 + 50i$
ω_5	$-827 + 120i$
ω_6	$477839 - 760062i$
ω_7	$22662669 - 40258594i$
ω_8	$-3085230919875999 - 807504660092300i$

Remark B.5.2 *Throughout, we concern ourselves only with primary primes. We multiply $\omega_1 \cdots \omega_{n-1}$ by 2 to ensure that $1 + 2\omega_1 \cdots \omega_{n-1}$ will be primary. We say that a prime is omitted from the sequence if no associate of the prime is an element of the sequence $\{\omega_n\}_{n=1}^{\infty}$.*

In both [BO12] and [PT14] a key fact used is that intervals of length small relative to p must contain both integers which are quadratic residues modulo p and integers which are non-quadratic residues modulo p. When working over $\mathbb{Z}[i]$ one might hope to prove that balls of small radius (small relative to the norm of a prime π) contain both biquadratic residues and non-residues. Rausch [Ra94] provides a theorem that implies a result in this direction. His bounds on character sums in algebraic number fields can be used to prove that for any $\epsilon \in \{\pm 1 \pm i\}$, for a prime $\pi \in \mathbb{Z}[i]$, and for given $\alpha \in \mathbb{Z}[i]$, there is some $\gamma \in \mathbb{Z}[i]$ in a ball of not-too-large radius about α such that $\left[\frac{\gamma}{\pi}\right] = \epsilon$. To prove that certain Euclid-Mullin-like sequences in the Gaussian integers miss infinitely many prime elements, a slightly stronger result is needed due to the possibility that there may be *two* primes of largest norm dividing $1 + 2\omega_1 \cdots \omega_{n-1}$. To ensure that a contradiction can be achieved regardless of the choice of a prime of largest norm, the following unproven hypothesis is needed.

[**The Strong Close-By Hypothesis**] *There is a constant C such that for any prime $\pi_1 \in \mathbb{Z}[i]$, for any $\alpha \in \mathbb{Z}[i]$, and for any fixed $\epsilon_1, \epsilon_2 \in \{\pm 1, \pm i\}$, there is a $\gamma \in \mathbb{Z}[i]$ with $N(\gamma - \alpha) < CN(\pi_1)^{1/2}$, $\left[\frac{\gamma}{\pi_1}\right] = \epsilon_1$, and $\left[\frac{\gamma}{\pi_2}\right] = \epsilon_2$ (where $\pi_2 = \overline{\pi}_1$).*

The Strong Close-by Hypothesis is only slightly stronger than a result implied by Rausch (Thm. 2, [Ra94]) which gives a bound of $N(\gamma - \alpha) < CN(\pi_1)^{1/2+\delta}$ for each $\delta > 0$. Assuming the hypothesis, we prove the following proposition.

Proposition B.5.3 *Let $Q_1, \ldots, Q_r$ be the smallest (in norm) r primes omitted from the sequence $\{\omega_n\}_{n=1}^{\infty}$, where $r \geq 0$ and let $X = (32C) \cdot N(Q_1 \cdots Q_r)$. Then there is another omitted prime Ω such that $N(\Omega) < X$ and no associate of Ω is contained in $\{\omega_n\}_{n=1}^{\infty}$.*

Proof of the proposition: Suppose by way of contradiction that every prime π with $N(\pi) \leq X$ except $Q_1, \ldots, Q_r$ has an associate appearing in the EML sequence above. Let π be last prime to appear in the sequence with $N(\pi) \in [2, X]$, say $\pi = \omega_n$. Then π is a prime of largest norm dividing $\beta = 1 + 2\omega_1 \cdots \omega_{n-1}$. If there is another prime of norm $N(\pi)$ which is not associate to π, we denote it by π_2 (note that in such a case we have $\pi_2 = \overline{\pi}$). Since any prime with norm smaller than $N(\pi)$ that is not one of the Q_j is one of $\omega_1, \ldots, \omega_{n-1}$, the only possible factors of β are $Q_1, \ldots, Q_r, \pi_2, \pi$, so $\beta = Q_1^{e_1} \cdots Q_r^{e_r} \pi_2^{e_{r+1}} \pi^e$, where $e_1, \ldots, e_r, e_{r+1} \geq 0$

and $e \geq 1$.

We claim we can choose $\lambda \in \mathbb{Z}[i]$ with $N(\lambda) \leq X$ such that :

$$\lambda \text{ is primary} \tag{B.11}$$

$$\lambda \equiv 1 + i \pmod{Q_1 \cdots Q_r} \tag{B.12}$$

and

$$\left[\frac{\lambda}{\pi}\right] = \left[\frac{1+i}{\pi}\right] \text{ and } \left[\frac{\lambda}{\pi_2}\right] = \left[\frac{1+i}{\pi_2}\right]. \tag{B.13}$$

Supposing for the moment this has been proved, since $N(\lambda) \leq X$, and λ is coprime to $Q_1, \dots, Q_r, \overline{\pi}, \pi$, every prime dividing λ is among the primes $\omega_1, \dots, \omega_{n-1}$ (or an associate of one of the ω_j's). Thus, if we write $\lambda = \lambda_0 \lambda_1^2$, with λ_0 square free, then $\lambda_0 | \omega_1 \cdots \omega_{n-1}$, so Biquadratic Reciprocity gives

$$\begin{aligned}
\left[\frac{\lambda}{\beta}\right] &= \left[\frac{\beta}{\lambda}\right] \cdot (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\beta)-1}{4}} \\
&= \left[\frac{\beta}{\lambda_0}\right] \cdot \left[\frac{\beta}{\lambda_1^2}\right] \cdot (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\beta)-1}{4}} \\
&= \left[\frac{1}{\lambda_0}\right] \cdot \left[\frac{\beta}{\lambda_1}\right]^2 \\
&= (1) \cdot (\pm 1) \cdot (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\beta)-1}{4}} \in \{\pm 1\}.
\end{aligned}$$

On the other hand, for each $j = 1, 2, \dots, r$, $\left[\frac{\lambda}{Q_j}\right] = \left[\frac{1+i}{Q_j}\right]$, $\left[\frac{\lambda}{\pi}\right] = \left[\frac{1+i}{\pi}\right]$ and$\left[\frac{\lambda}{\pi_2}\right] = \left[\frac{1+i}{\pi_2}\right]$, so

$$\left[\frac{\lambda}{\beta}\right]=\left(\prod_{j=1}^{r}\left[\frac{\lambda}{Q_j}\right]^{e_j}\right)\cdot\left[\frac{\lambda}{\pi_2}\right]^{e_{r+1}}\left[\frac{\lambda}{\pi}\right]^{e}=\left(\prod_{j=1}^{r}\left[\frac{1+i}{Q_j}\right]^{e_j}\right)\cdot\left[\frac{1+i}{\pi_2}\right]^{e_{r+1}}\left[\frac{1+i}{\pi}\right]^{e}=\left[\frac{1+i}{\beta}\right].$$

Since $\omega_2\cdots\omega_{n-1}=a+bi$ is primary, we have that a is odd, b is even; then for $\beta=1+2\omega_1\cdots\omega_{n-1}$ (recalling that $\omega_1=1+i$), we have $\beta=1+2(1+i)(a+bi)=(1+2a-2b)+i(2a+2b)$, so

$$\frac{Re(\beta)-Im(\beta)-Im(\beta)^2-1}{4}=\frac{1+2a-2b-(2a+2b)-(4a^2+8ab+4b^2)-1}{4}=-b-a^2-2ab-b^2,$$

which is odd, thus

$$\left[\frac{1+i}{\beta}\right]=i^{(Re(\beta)-Im(\beta)-Im(\beta)^2-1)/4}\in\{\pm i\}.$$

This is a contradiction.

It remains to show there is such $\lambda\in\mathbb{Z}[i]$ with $N(\lambda)\leq X$ satisfying (B.11), (B.12), and (B.13). By the Chinese Remainder Theorem, we know there exists some A satisfying conditions (B.11) and (B.12). Then the conditions are also satisfied by any $\lambda=\delta M+A$, where $M=Q_1\cdots Q_r\cdot(1+i)^3$ (where no Q_i or associate of Q_1 is equal to $1+i$). Then finding a λ of sufficiently small norm relative to X satisfying condition (B.13) is equvialent to finding δ of sufficiently small norm such that $\left[\frac{\delta+AM'}{\pi}\right]=\left[\frac{(1+i)M'}{\pi}\right]$, $\left[\frac{\delta+AM'}{\pi_2}\right]=\left[\frac{(1+i)M'}{\pi}\right]$, where $MM'\equiv 1 \pmod{\pi}$ and $MM'\equiv 1 \pmod{\pi_2}$. By the hypothesis, there exists $\gamma\in\mathbb{Z}[i]$ such that $\left[\frac{\gamma}{\pi}\right]=\left[\frac{(1+i)M'}{\pi}\right]$, $\left[\frac{\gamma}{\pi_2}\right]=\left[\frac{(1+i)M'}{\pi_2}\right]$and $N(\gamma-AM')\leq CN(\pi)^{1/2}$. Letting $\delta\coloneqq\gamma-AM'$, we have $\left[\frac{\delta+AM'}{\pi}\right]=\left[\frac{(1+i)M'}{\pi}\right]$; then setting $\lambda\coloneqq\delta M+A$ (and noting that we can choose A with $|A|<|M|$), we have

$$\sqrt{N(\lambda)}=|\lambda|=|\delta M+A|\leq|\delta M|+|A|<|\delta M|+|M|<|M|(|\delta|+1)=(\sqrt{8}\cdot|Q_1\cdots Q_r|)\cdot(|\delta|+1)$$
$$\leq(\sqrt{8}\cdot|Q_1\cdots Q_r|)(2|\delta|)\leq(2\sqrt{8}\cdot|Q_1\cdots Q_r|)\cdot(C^{1/2}|\pi|^{1/2})\leq\sqrt{X^{\frac{1}{2}}}\sqrt{X^{\frac{1}{2}}}=X^{1/2},$$

for X chosen to be large relative to $N(Q_1\cdots Q_r)$. Thus $N(\lambda)<X$, proving the claim. □

Bibliography

[AF93] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes.* Eur. J. Comb. 14, 79-83, 1993.

[Bi67] Birch, B.J. “Cyclotomic fields and Kummer extensions,” in Cassels, J.W.S and Fröhlich, *Algebraic number theory; proceedings of an instructional conference.* Thompson Book Co., Washington, 1967.

[BO12] Booker, A., *On Mullin’s second sequence of primes.* INTEGERS, 12, A4, 10pp, 2012.

[BC15] Brunyate, A. and Clark, P.L., *Extending the Zolotarev-Frobenius approach to quadratic reciprocity.* Ramanujan J. 37, 25-50, 2015.

[CC97] Cahen, P.-J. and Chabert, J.-L., *Integer-valued polynomials.* American Mathematical Society, Providence, RI, Mathematical Surveys and Monographs, 48., 1997.

[Ca67] Cassels, J.W.S., “Global fields, Appendix C,” in Cassels, J.W.S and Fröhlich, *Algebraic number theory; proceedings of an instructional conference.* Thompson Book Co., Washington, 1967.

[Ch09] Childress, N., *Class field theory.* Springer, New York, Universitext, 2009.

[CWxx] Clark, J. and Watson, L.D., *On generalizations of the second Euclid-Mullin sequence.* `https://loridwatson.com/research/`.

[Cl08] Clark, P.L., *Anti-Hasse Principle" for prime twists*. Int. J. of Number Theory 4, 627-637, 2008.

[Cl14] Clark, P.L., *The Combinatorial Nullstellensätze Revisited*. Electronic Journal of Combinatorics. Vol. 21, Issue 4, Paper #P4.15, 2014.

[Cl17] Clark, P.L., *The Euclidean criterion for irreducibles*. Amer. Math. Monthly, 124, 198-216, 2017.

[Cl18] Clark, P.L., *Warning's second theorem with relaxed outputs*. J. Algebraic Combin. 48, no. 2, 325-349, 2018.

[CS18] Clark, P.L. and Stankewicz, J., *Hasse principle violations for Atkin-Lehner twists of Shimura curves*. Proc. Amer. Math. Soc. 146, 2839-2851, 2018.

[CFS17] Clark, P.L., A. Forrow and J.R. Schmitt, *Warning's Second Theorem with restricted variables*. Combinatorica 37, 397-417, 2017.

[CW18.1] Clark, P.L and Watson, L.D., *Varga's theorem in number fields*. INTEGERS, 18, A74, 11pp, 2018.

[CW18.2] Clark, P.L and Watson, L.D., *ABC and the Hasse principle for quadratic twists of hyperelliptic curves*. C. R. Math. Acad. Sci. Paris 356, 911-915, 2018.

[CV68] Cox, C.D. and van der Poorten, A.J., *On a sequence of prime numbers*. J. Aust. Math. Soc., 8, 571-574, 1968.

[El91] Elkies, N., *ABC implies Mordell*. Internat. Math. Res. Notices, 99-109, 1991.

[Gr07] Granville, A., *Rational and integral points on quadratic twists of a given hyperelliptic curve*. Int. Math. Res. Not. IMRN, no. 8, Art. ID 027, 24 pp, 2007.

[Ja96] Janusz, G. *Algebraic number fields (2nd ed.)* American Mathematical Society, Providence, RI, Graduate Studies in Mathematics, Vol 7, 1996.

[Ko91] Koo, J. K., *On holomorphic differentials of some algebraic function field of one variable over* $\mathbb{C}$. Bull. Austral. Math. Soc. 43, 399-405. MR 92e:14019, 1991.

[La03] Landau, E., *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes.* Mathematische Annalen. 56 (4): 645-670, 1903.

[La13] Lang, S., *Algebraic number theory (2nd ed.).* Springer-Verlag, New York, Graduate Texts in Mathematics No. 110, 2013.

[Le00] Lemmermeyer, F., *Reciprocity laws, from Euler to Eisenstein.* Springer-Verlag, New York, 2000.

[LS96] Lenstra Jr., H.W. and Stevenhagen, P., *Chebotarev and his density theorem.* Math. Intell. 18, 26-37, 1996.

[Li40] Lind, C.E., *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins.* Thesis, University of Uppsala, 1940.

[Liu02] Liu, Q., *Algebraic geometry and arithmetic curves.* Oxford University Press, Oxford, Oxford Graduate Texts in Mathematics 6, 2002.

[Lo90] Lorenzini, D., *Dual graphs of degenerating curves.* Math. Ann., 287:135-150, 1990.

[Lo13] Lorenzini, D., *Wild quotient singularities of surfaces.* Math. Zeit. 275 Issue 1, 211-232, 2013.

[Ma93] Mazur, B., *On the passage from local to global in number theory.* Bulletin of the American Mathematical Society, 29(1), 14-50, 1993.

[MR10] Mazur, B. and Rubin, K., *Ranks of twists of elliptic curves and Hilberts tenth problem.* Invent. math., Vol. 181, Issue 3, 541-575, 2010.

[Mu63] Mullin, A.A., *Recursive function theory (a modern look at a Euclidean idea).* Bull. Amer. Math. Soc., Vol 69, 737, 1963.

[Ne71] A.A. Nečaev, *The structure of finite commutative rings with unity.* Mat. Zametki 10, 679-688, 1971.

[PT14] Pollack, P. and Treviño, E., *The primes that Euclid forgot.* Amer. Math. Monthly, 121, no.5, 433-437, 2014.

[Po17] Poonen, B., *Rational points on varieties.* American Mathematical Society, Vol. 186, 2017.

[PS97] Poonen, B. and Schaefer, E.F, *Explicit descent for Jacobians of cyclic covers of the projective line.* J. Reine Angew. Math., 488, 141188, 1997.

[Pr58] Prachar, K., *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe.* Monatsh. Math., 62, 173-176, 1958.

[Ra94] Rausch, U., *Character sums in algebraic number fields.* Journal of Number Theory, 46(2), 179-195, 1994.

[Re42] Reichardt, H., *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen.* J. Reine Angew. Math. 184, 12-18, 1942.

[Ri08] Rivin, I., *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms.* Duke Math. J. Vol.142,, no. 2, 353-379, 2008.

[Sa14] Sadek, M., *On quadratic twists of hyperelliptic curves.* Rocky Mountain J. Math. 44, 1015-1026, 2014.

[Se54] Selmer, E., *The diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. 85, 203-362, 1951, and 92 , 191-197, 1954.

[Ser70] Serre, J.-P., *A course in arithmetic.* Springer-Verlag, New York. Graduate Texts in Mathematics, No. 7, 1970.

[Ser76] Serre, J.-P., *Divisibilité de certaines fonctions arithmétiques.* Enseignement Math. (2) 22, 227–260, 1976.

[Ser97] Serre, J.-P., *Galois cohomology.* Springer-Verlag Berlin Heidelberg, Translated from the French, 1997.

[Si97] Silverman, J., *The arithmetic of elliptic curves (2nd ed.).* Springer-Verlag, New York, Graduate Texts in Mathematics, No. 106, 2009.

[Sk10] Skorobogatov, A. N., *Torsors and rational points.* Cambridge University Press, Cambridge, Cambridge Tracts in Mathematics, Vol. 144, 2001.

[Va14] L. Varga, *Combinatorial Nullstellensatz modulo prime powers and the parity argument.* Electron. J. Combin. 21, no. 4, Paper 4.44, 17 pp., 2014.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.* Abh. Math. Sem. Hamburg 11, 76–83, 1935.