Spring 2015

Irreducibility and Galois Properties of Lifts of Supersingular Polynomials

Rylan Jacob Gajek-Leonard
Bard College

Irreducibility and Galois Properties of Lifts of Supersingular Polynomials

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Rylan Gajek-Leonard

Annandale-on-Hudson, New York
May, 2015

Abstract

It has recently been shown that a rational specialization of Jacobi polynomials, when reduced modulo a prime number p, has roots which coincide with the supersingular j-invariants of elliptic curves in characteristic p. These *supersingular lifts* are conjectured to be irreducible with maximal Galois groups. Using the theory of p-adic Newton Polygons, we provide a new infinite class of irreducibility and, assuming a conjecture of Hardy and Littlewood, give strong evidence for their Galois groups being as large as possible.

Contents

List of Figures

Dedication

To my mother, for always encouraging me to continue the pursuit.

Acknowledgments

I would first like to thank John Cullinan for his support, kindness and clarity. You have shown me that mysteries are plentiful in mathematics and I consider that a great gift.

I also thank my sister, Teighan, for her constant encouragement and my father, Terry, for his open ears and adventurous spirit.

And thanks to Georgia, for her time and inspiration.

1 Introduction

In 2003, Brillhart and Morton proved that a rational specialization of Jacobi polynomials, which we denote $\mathscr{K}_n^{(\lambda,\mu)}(x)$, can be reduced modulo a prime p to the *supersingular* polynomial in characteristic p [2]. This is a significant result; their work expresses a deep characteristic of elliptic curves (the roots of the supersingular polynomial determine isomorphism types) in terms of a fundamental class of orthogonal polynomials that arise both in physics (viz., the Legendre specialization of Jacobi polynomials) and other areas of mathematics. Mahlburg and Ono have conjectured in [18] that the polynomials $\mathscr{K}_n^{(\lambda,\mu)}(x)$ are irreducible over the rational numbers and have Galois groups isomorphic to the symmetric group S_n.

Our goal in this project is to provide evidence in support of this conjecture using p-adic Newton Polygons. We emphasize that the techniques employed here are applicable to any family of rational polynomials and so this project is, in part, an analysis of the usefulness of Newton Polygons in determining polynomial irreducibility and Galois groups. We attempt to exhibit both the far reaching possibilities of the Newton Polygon and also some of its limitations. Included in our results are several new cases of irreducibility and the description of nearly all Newton Polygons for the $\mathscr{K}_n^{(\lambda,\mu)}(x)$ polynomials at primes in specified intervals.

Furthermore, assuming complete irreducibility and a conjecture of Hardy and Littlewood, we give strong evidence that the Galois groups of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ are the full symmetric group. We also present several conjectures (together with evidence, partial proofs and consequences) regarding some special degrees which yield particularly interesting Newton Polygons.

The purpose of the following chapter is to familiarize our reader with the subject, construct framework for our analysis of the $\mathscr{K}_n^{(\lambda,\mu)}(x)$ polynomials and attempt to provide some motivation for the importance of this study. We therefore intend to:

(A) specify sufficient conditions for a rational polynomial to have maximal Galois group,

(B) identify methods to show that a polynomial fulfills these conditions, and

(C) discuss the importance of the family of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ polynomials.

2

Preliminaries

2.1 Irreducible Polynomials and Eisenstein's Criterion

Irreducible polynomials can be viewed as analogues of the rational primes; polynomials, like integers, can be factored into unique (up to constant multiples) products of irreducible elements. Furthermore, irreducible polynomials can be used to construct *extension fields* - fields which are strictly larger than the base field in which the polynomial is defined. Identifying irreducible polynomials is typically a difficult problem. Although polynomial factorization is well-studied, a general algorithm for determining whether a given polynomial with coefficients in a field F is irreducible over F is currently an open problem.

In this section, we present a well-known procedure (which we intend to generalize in Section 2.4) that can be applied to certain polynomials to conclude irreducibility. Recall the following definitions.

Definition 2.1.1. Let K be a commutative ring with 1. If for all nonzero $a \in K$ there exists an element $a^{-1} \in K$ such that $aa^{-1} = 1$ then K is called a *field*. If $F \subseteq K$ is also a commutative ring with 1 under the same operations as K then F is called a *subfield* of K. △

Definition 2.1.2. Let R be a ring and let I be a subset of R. Suppose that the I satisfies the following conditions:

(i) I is an additive subgroup of R

(ii) $a \in I$ and $r \in R$ imply that $ra \in I$.

Then I is called an $ideal$ of R. If $I \neq R$ then I is called a $proper\ ideal$. △

Definition 2.1.3. Let F be a field and let $f(x) = a_0 + a_1x + \cdots a_nx^n \in F[x]$ be a nonzero polynomial with coefficients in F. Let $A = \{(g,h) \in F[x] \times F[x] : f(x) = g(x)h(x)\}$. If every element of A is of the form (c,h) or (g,c'), for some $c,c' \in F$ then $f(x)$ is called an *irreducible* polynomial over F. If $f(x)$ is not irreducible over F we say that $f(x)$ is a *reducible* polynomial over F △

From this definition, we see that if $f(x)$ is irreducible over F then, given any two polynomials $g,h \in F[x]$ which satisfy $g(x)h(x) = f(x)$, we have that either g is a constant or h is a constant in F. Thus, a polynomial $f(x) \in F[x]$ is irreducible if it cannot be written as a product of two non-constant polynomials over F.

Example 2.1.4. Consider the polynomial $3x^2 + 2 \in \mathbf{Q}[x]$. Since this polynomial has roots $\pm\sqrt{-2/3} \not\in \mathbf{Q}$, we see that it must be irreducible over $\mathbf{Q}$. ♢

Example 2.1.5. Let $3x^2 + 2 \in \mathbf{Z}/5\mathbf{Z}$. Observe that elements $1,4 \in \mathbf{Z}/5\mathbf{Z}$ satisfy $3x^2 + 2 = 0$. Therefore $3x^2 + 2 = (x+1)(x+4)$ is reducible over $\mathbf{Z}/5\mathbf{Z}$. ♢

The following Theorem, given by G. Eisenstein in 1850, has proven to be very useful in determining whether certain polynomials with integer coefficients are irreducible over the rational numbers.

Theorem 2.1.6 (Eisenstein's Criterion). *Let $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbf{Z}[x]$. If there exists a prime p such that*

(i) $p \mid a_i$ for all $i \in \{0,\dots,n-1\}$

(ii) $p \nmid a_n$*, and*

(iii) $p^2 \nmid a_0$*,*

then $f(x)$ *is irreducible over* $\mathbf{Q}$*.*

Proof. Suppose that $f(x)$ is reducible over $\mathbf{Q}$ and that there exists a prime which satisfies the above three conditions. Since $f(x)$ is reducible, we know that there exists non constant polynomials $g,h \in \mathbf{Q}[x]$ such that $f(x) = g(x)h(x)$. Without loss of generality, we also see that $1 \le \deg(g) \le \deg(h) \le n = \deg(f)$. Setting $g(x) = b_0 + b_1x + \cdots + b_mx^m$ and $h(x) = c_0 + c_1x + \cdots + c_kx^k$, we obtain

$$p \mid b_0c_0 = a_0.$$

But since $p^2 \nmid a_0$, it must be the case p divides precisely one of b_0 or c_0. Suppose that $p \mid b_0$ and $p \nmid c_0$. We may also observe that

$$p \nmid b_mc_k = a_n,$$

and so $p \nmid b_m$. This means that there must exist some minimum $j \in \{1,\ldots,m\}$ such that $p \nmid b_j$. Now consider that $a_j = b_jc_0 + b_{j-1}c_1 + \cdots + b_0c_k \equiv b_jc_0 \mod p$. But $p \mid a_j$ by hypothesis (i), which is a contradiction. □

Example 2.1.7. The polynomial $2x^6 + 18x^4 + 15x^3 + 3x^2 + 21x + 6 \in \mathbf{Q}[x]$ is irreducible since it is Eisenstein at the prime 3. ◊

We now define some special ideals that will help us see how irreducible polynomials can be used to construct fields.

Definition 2.1.8. Let R be a commutative ring with 1 and let A be a proper ideal of R. If $a,b \in R$ and $ab \in A$ imply that $a \in A$ or $b \in A$ then the ideal A is called a *prime ideal*. If B is an ideal of R and $A \subseteq B \subseteq R$ implies that $B = A$ or $B = R$, then the A is called a *maximal ideal*. △

Example 2.1.9. Let p be any prime. The ideals $p\mathbf{Z}$ are prime ideals in the ring $\mathbf{Z}[x]$. ◊

Theorem 2.1.10. *Let R be a commutative ring with 1 and let A be an ideal of R. Then R/A is a field if and only if A is maximal.*

Proof. [11, Theorem 14.4] □

Theorem 2.1.11. *Let $f(x) \in F[x]$. Then $f(x)$ is irreducible if and only if the ideal $(f(x))$ is maximal in $F[x]$.*

Proof. [11, Theorem 17.5] □

The above two theorems allow us to see a connection between irreducible polynomials and fields. In particular, let $f(x) = a_0 + a_1x + \cdots a_nx^n \in F[x]$ be irreducible, let $I = (f(x))$ be the ideal generated by $f(x)$ and consider the element $r = x + I \in F[x]/I$. Then

$$\begin{aligned}
f(r) &= a_0 + a_1(x+I) + \cdots a_n(x+I)^n \\
&= a_0 + a_1(x+I) + \cdots a_n(x^n+I) \\
&= a_0 + a_1x + \cdots a_nx^n + I \\
&= f(x) + I \\
&= I.
\end{aligned}$$

Since I is the zero element in $F[x]/I$ we see that $F[x]/I$ contains a root of $f(x)$. Thus, for every irreducible polynomial $f(x) \in F[x]$ we can construct a field in which $f(x)$ has a root. This observation is known as *Kronecker's Theorem*.

2.2 Algebraic Extensions and Galois Theory

The fields mentioned in Theorem 2.1.10 are significant since they can be viewed in the following way. Note that $\bar{K}$ refers to the algebraic closure of K (a field which contains the root of every non-constant polynomial with coefficients in K).

Theorem 2.2.1. *Let K be a field and let $f(x) \in K[x]$ be an irreducible polynomial of degree n. If $\alpha \in \bar{K}$ is a root of $f(x)$, then $E = K[x]/(f(x)) \simeq K(\alpha)$ and a basis for L as a vector space over K is $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.*

Proof. [21, Theorem 45] □

Example 2.2.2. Let $f(x) = x^2 + 1 \in \mathbf{F}_3[x]$. It is easy to check that this polynomial is irreducible. We can therefore see that the quotient $\frac{\mathbf{F}_3[x]}{(x^2+1)}$ is a degree 2 extension of $\mathbf{F}_3$ by Theorem 2.2.1. Furthermore, the field $\frac{\mathbf{F}_3[x]}{(x^2+1)}$ is isomorphic to the field obtained by adjoining the root $\sqrt{-1} = i$ of $x^2 + 1$ to $\mathbf{F}_3$ (i.e., we adjoin algebraic object which satisfies $x^2 = -1$). This can be seen by observing that

$$\frac{\mathbf{F}_3[x]}{(x^2+1)} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

and

$$\mathbf{F}_3(i) = \{0, 1, 2, i, i+1, i+2, 2i, 2i+1, 2i+2\}.$$

The two fields are isomorphic under the map $a + bx \mapsto a + bi$ (where $a, b \in \mathbf{F}_3$) which sends x to i and fixes elements in $\mathbf{F}_3$. ◊

Notice from Theorem 2.2.1 that every field extension $K(\alpha)/K$ has degree n as a vector space over K and that this n is the degree of the (minimal) irreducible polynomial having α as a root. If E/K is field extension, we denote its degree by $[E : K]$ and if E is a finite degree extension K then we call E an *algebraic number field*, where the elements $\alpha \in E$ which are roots of some monic polynomial over K are called *algebraic numbers*.

Theorem 2.2.1 allows for the construction of algebraic fields (that are not all of $\mathbf{C}$) wherein a polynomial $f(x) \in K$ factors completely. Supposing that $\deg(f) > 1$, we can factor f into a product of irreducible polynomials $g_1, \ldots, g_k$ and construct a field field $E = K[x]/(g_1(x))$ which contains a root of g_1. After factoring each of $g_1, \ldots, g_k$ in E we can again construct an extension E'/E which contains a root of one of these irreducible polynomials in E. Continuing in this way, we arrive at a field in which $f(x)$ factors completely but is not all of $\mathbf{C}$ since we are only adjoining a finite number of algebraic elements. This field is called the *splitting field* of $f(x) \in K[x]$. If $\alpha_1,\ldots,\alpha_i$ are the roots of $f(x) \in K[x]$ we can see that $f(x)$ must split completely in $E = K(\alpha_1,\ldots,\alpha_i)$ and that $f(x)$ cannot be fully factored in any subfield of K' which is not E itself (if it did then K' would contain each root of f).

Theorem 2.2.3. *Let K,E,L be fields such that $K \subseteq E \subseteq L$. If $[E:K]$ and $[L:E]$ are finite then*

$$[E:K]\cdot[L:E] = [L:K].$$

Proof. [21, Lemma 49] □

We now define the Galois group of an extension L/K.

Definition 2.2.4. Let L/K be a field extension. An *automorphism* of L is an isomorphism $\varphi : L \to L$. Let $A = \{\varphi : \varphi \text{ is an automorphism of } L\}$. The *Automorphism group* of L/K is the set

$$\mathrm{Aut}(L/K) = \{\varphi \in A : \varphi(c) = c \text{ for all } c \in K\}.$$

If $|\mathrm{Aut}(L/K)| = [L:K]$ then $\mathrm{Aut}(L/K)$ is called the *Galois group* of L/K, denoted $\mathrm{Gal}(L/K)$, and the extension L/K is called a *Galois extension*. Furthermore, if $H \leq \mathrm{Gal}(L/K)$ we define the set

$$L^H = \{x \in L : \varphi(x) = x \text{ for all } \varphi \in H\},$$

which is called the *fixed field* of H. △

It is not difficult to check that L^H satisfies the field axioms.

Example 2.2.5. Consider the polynomial $x^2 - 3 \in \mathbf{Q}[x]$. This polynomial has roots $\pm\sqrt{3}$ and is therefore irreducible over $\mathbf{Q}$. By Theorem 2.2.1 we know that $\frac{\mathbf{Q}[x]}{(x^2-3)} \simeq \mathbf{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a,b \in \mathbf{Q}\}$ is a degree 2 extension of $\mathbf{Q}$. If φ is an automorphism $\mathbf{Q}(\sqrt{3})$ then

$\varphi(a + b\sqrt{3}) = \varphi(a) + \varphi(b\sqrt{3}) = a + b\varphi(\sqrt{3})$ since φ fixes $\mathbf{Q}$ and is a homomorphism. To determine $\mathrm{Aut}(\mathbf{Q}(\sqrt{3})/\mathbf{Q})$, we can therefore restrict our attention to the mappings of $\sqrt{3}$. Observe that $3 = \varphi(3) = \varphi(\sqrt{3}\sqrt{3}) = \varphi(\sqrt{3})^2$ and therefore $\varphi(\sqrt{3}) = \sqrt{3}$ or $\varphi(\sqrt{3}) = -\sqrt{3}$. Thus $\mathrm{Aut}(\mathbf{Q}(\sqrt{3})/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}(\sqrt{3})/\mathbf{Q})$ consists of two elements: the identity mapping and the mapping $a + \sqrt{3}b \mapsto a - \sqrt{3}b$.

$\diamondsuit$

The following theorem allows us to see that it also makes sense to speak of the Galois group of a polynomial.

Theorem 2.2.6. *The field extension L/K is Galois if and only if L is the splitting field of a polynomial over K.*

Proof. [6, Thm 4.1] $\square$

Since the splitting field L/K of $f(x) \in K[x]$ is a Galois extension, we henceforth discuss $\mathrm{Gal}(f)$ with the understanding that $\mathrm{Gal}(f)$ is the Galois group of the splitting field L/K of $f(x)$. We now recall some definitions and theorems from group theory.

Definition 2.2.7. Let G be a subgroup of S_n. We say that G acts on the set $X = \{1, 2, \ldots, n\}$ *transitively* if for every distinct $x, y \in X$ there exists some $g \in G$ such that $gx = y$. If G acts on X transitively then G is called a *transitive subgroup*. $\triangle$

Example 2.2.8. Clearly the alternating group A_n is a transitive subgroup of S_n since A_n contains every even permutation of elements in $X = \{1, 2, \ldots, n\}$. Thus, for every pair of elements $x_i, x_j \in X$ there is a permutation $\sigma \in A_n$ (the permutation $(1 x_i x_j)$, for example) such that $\sigma(x_i) = x_j$. $\diamondsuit$

Example 2.2.9. Consider the subgroup $\{(1), (13), (24), (13)(24)\}$ of S_4. This subgroup does not act transitively on the set $\{1, 2, 3, 4\}$ since there is no element that sends 1 to 2. $\diamondsuit$

The following theorem allows us to view every Galois group (of an irreducible polynomial) as a transitive subgroup of the symmetric group.

Theorem 2.2.10. *Let $f(x) \in K[x]$ be a polynomial of degree n. Then $f(x)$ is irreducible if and only if* $\mathrm{Gal}(f)$ *is isomorphic to a transitive subgroup of S_n.*

Proof. [6, Thm. 2.9] □

The following theorem relates the study of groups to fields and the study of fields to groups.

Theorem 2.2.11 (Galois Correspondence)**.** *Suppose that L/K is a Galois extension of finite degree. Let H be a subgroup of $G = \mathrm{Gal}(L/K)$ and let E be an intermediate field $K \subseteq E \subseteq L$. Then*

(i) $[L:E] = |H|$,

(ii) $[E:K] = [G:H] = |G/H|$,

(iii) L/E is a Galois extension, and

(iv) the extension E/K is Galois if and only if $H \lhd G$ (and thus $G/H \simeq \mathrm{Gal}(E/K)$).

Furthermore, there is a one-to-one correspondence between the subgroups of $\mathrm{Gal}(L/K)$ *and the subfields of E of L such that for every subgroup $H \le G$ there is a corresponding subfield $L^H = E$ and for every subfield $E \subseteq L$ there is a corresponding subgroup $H = \mathrm{Aut}(L/E)$.*

Proof. [5, Theorem 5.6, Theorem 4.11] □

We note that the correspondence described above is inclusion-reversing: $E \subseteq L \iff H \le G$ for each subfield $E \subseteq L$ and each subgroup $H \le G$.

Example 2.2.12. We present a standard example using $f(x) = x^3 - 2 \in \mathbf{Q}[x]$ to illustrate the depth of Theorem 2.2.11. Let $\omega = e^{2\pi i/3}$ and observe that the roots of f are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. We can see that $\mathbf{Q}(\sqrt[3]{2}, \omega)$ is the splitting field for $f(x)$ (and is therefore a Galois extension by Theorem 2.2.6) since this field contains each root of f. From Theorem 2.2.1 we see that each of the fields $\mathbf{Q}(\sqrt[3]{2}), \mathbf{Q}(\omega\sqrt[3]{2})$ and $\mathbf{Q}(\omega^2\sqrt[3]{2})$ have degree 3 over $\mathbf{Q}$. Furthermore, observe that the polynomial $(x-\omega)(x-\omega^2) = x^2+x+1$ is irreducible over $\mathbf{Q}(\sqrt[3]{2})$ since ω is complex. Thus $\mathbf{Q}(\sqrt[3]{2})[x]/(x^2+x+1)$ has degree 2 over $\mathbf{Q}(\sqrt[3]{2})$ and since $\mathbf{Q}(\sqrt[3]{2})[x]/(x^2+x+1)$ contains each root of $f(x)$, it is isomorphic to $\mathbf{Q}(\sqrt[3]{2},\omega)$. This also allows us to see that $\mathbf{Q}[x]/(x^2+x+1) \simeq \mathbf{Q}(\omega) \subseteq \mathbf{Q}(\sqrt[3]{2},\omega)$ must be degree 2 extension of $\mathbf{Q}$. Figure 2.2.1 illustrates the subfields of $\mathbf{Q}(\sqrt[3]{2},\omega)$ (on the left) and the subgroups of S_3 (on the right).

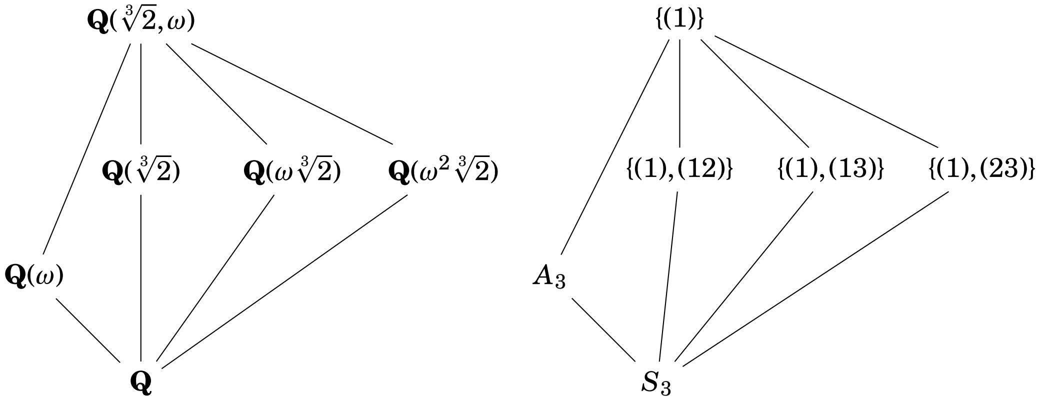

$\mathbf{Q}(\sqrt[3]{2},\omega)$
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\omega\sqrt[3]{2})$
$\mathbf{Q}(\omega^2\sqrt[3]{2})$
$\mathbf{Q}(\omega)$
$\mathbf{Q}$
$\{(1)\}$
$\{(1),(12)\}$
$\{(1),(13)\}$
$\{(1),(23)\}$
A_3
S_3

Figure 2.2.1: Subfields of $\mathbf{Q}(\sqrt[3]{2},\omega)$ and subgroups of S_3 (with inclusion reversed).

Since $\mathbf{Q}(\sqrt[3]{2},\omega)$ is a Galois extension of degree $3\cdot 2 = 6$ (by Theorem 2.2.3) we know $|\operatorname{Gal}(f(x))| = 6$ and therefore that $\operatorname{Gal}(f(x)) \simeq S_3$ by Theorem 2.2.10. The Galois Correspondence states that this diagram of subfields should be the same as the diagram of subgroups of S_3 if we reverse inclusions, as has been done in the figure above. Items (i) and (iii) in Theorem 2.2.11 say that the degree of $\mathbf{Q}(\sqrt[3]{2},\omega)$ over each intermediate field corresponds to the orders of each subgroup of $\operatorname{Gal}(f(x))$ (e.g., $[\mathbf{Q}(\sqrt[3]{2},\omega):\mathbf{Q}(\sqrt[3]{2})] = 2 = |\{(1),(12)\}|$) and furthermore that $\mathbf{Q}(\sqrt[3]{2},\omega)$ is a Galois extension of each intermediate field. From item (ii), we can see that the degree of each intermediate field over $\mathbf{Q}$ corresponds to the *index* of a subgroup in S_3 (e.g., $[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}] = 3 = |S_3/\{(1),(12)\}|$ and $[\mathbf{Q}(\omega):\mathbf{Q}] = 2 = |S_3/A_3|$). Furthermore, we see that each subfield of $\mathbf{Q}(\sqrt[3]{2},\omega)$ corresponds to a subgroup of $\operatorname{Gal}(f(x))$ in that we can write these subfields as fields fixed by some $H \leq \operatorname{Gal}(f(x))$. For example, labeling each root

$\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ as 1, 2 and 3, respectively, observe that the subgroup $\{(1),(23)\}$ is isomorphic to the subgroup $\{1,\sigma\} \le \mathrm{Gal}(f(x))$, where σ is complex conjugation (i.e., σ swaps $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ and fixes $\sqrt[3]{2}$). Thus

$$\mathbf{Q}(\sqrt[3]{2},\omega)^{\{1,\sigma\}} = \{x \in \mathbf{Q}(\sqrt[3]{2},\omega) \colon \sigma(x) = x \text{ for all } \sigma \in \{1,\sigma\}\} = \mathbf{Q}(\sqrt[3]{2}).$$

◊

This correspondence can be very useful when studying more complicated polynomials since it allows properties of field extensions to be studied using groups and, similarly, properties of groups using fields. We now define the discriminant of a polynomial.

Definition 2.2.13. Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree n. If $r_1,\ldots,r_n, \in \bar{F}$ are the roots of f then the *discriminant* of f is defined to be

$$\mathrm{disc}(f) = \prod_{i<j}(r_i - r_j)^2.$$

△

Example 2.2.14. The polynomial $(x-5)(x^2+1) = x^3-5x^2+x-5 \in \mathbf{Q}[x]$ has roots 5 and $\pm\sqrt{-1}$ and so its discriminant is:

$$\left((5-\sqrt{-1})(5+\sqrt{-1})(\sqrt{-1}+\sqrt{-1})\right)^2 = -2704.$$

◊

The following proposition illustrates an unintuitive and important property of the discriminant.

Proposition 2.2.15. *Let* $f(x) \in F[x]$. *Then* $\mathrm{disc}(f) \in F$.

Proof. The discriminant of f can equivalently be defined in terms of a *resultant*, which is, in rough terms, the determinant of a matrix with entries in F. That is,

$$\mathrm{disc}(f) = C \cdot \mathrm{Res}(f, f'),$$

where C is a constant in F and $\operatorname{Res}(f,f')$ is the resultant of f and the derivative of f. This resultant will be the determinant of a matrix whose terms include only the the coefficients of f,f', and zero. Thus $\operatorname{disc}(f) \in F$. For more details see [8]. □

We now develop sufficient criterion for concluding that the Galois group of a polynomial is S_n.

Theorem 2.2.16. *Let* $f(x) \in \mathbf{Q}[x]$. *Then* $\operatorname{Gal}(f) \subseteq A_n$ *if and only if* $\operatorname{disc}(f)$ *is a rational square. In particular, if* $\operatorname{disc}(f)$ *is not a rational square then* $\operatorname{Gal}(f) \not\subseteq A_n$.

Proof. We follow [6, Theorem 4.7]. Observe that $\operatorname{disc}(f)$ is a square in $\mathbf{Q}$ if and only if $\sqrt{\operatorname{disc}(f)} = \prod_{i<j}(r_i - r_j) \in \mathbf{Q}$. Now let $E = \mathbf{Q}(r_1,\ldots,r_n)$ be the splitting field of f and let $\sigma \in \operatorname{Gal}(E/\mathbf{Q}) = \operatorname{Gal}(f)$. Viewing $\operatorname{Gal}(f)$ as subgroup of S_n (by Theorem 2.2.10) allows us to decompose σ into a product of two-cycles, where we let $\epsilon_\sigma = 1$ or -1 depending on whether σ is even or odd. Using the homomorphism properties of σ, we find that

$$\begin{aligned} \sigma\Big(\sqrt{\operatorname{disc}(f)}\Big) &= \sigma\Big(\prod_{i<j}(r_i - r_j)\Big) \\ &= \prod_{i<j}(\sigma(r_i) - \sigma(r_j)). \end{aligned}$$

But since $\sigma \in \operatorname{Gal}(f)$ we know that σ simply permutes the roots of f and thus

$$\prod_{i<j}(\sigma(r_i) - \sigma(r_j)) = \epsilon_\sigma \sqrt{\operatorname{disc}(f)}.$$

Now suppose that $\operatorname{Gal}(f) \subseteq A_n$. Then σ is an even permutation and $\epsilon_\sigma = 1$ which means that $\sigma(\sqrt{\operatorname{disc}(f)}) = \sqrt{\operatorname{disc}(f)}$. Thus σ fixes $\sqrt{\operatorname{disc}(f)}$ and so $\sqrt{\operatorname{disc}(f)} \in \mathbf{Q}$ by definition. If $\sqrt{\operatorname{disc}(f)} \in \mathbf{Q}$ then it is fixed by σ and so $\varepsilon_\sigma = 1$ which means that σ is even. The result now follows. □

Thus, if we can show that the discriminant of a polynomial $f(x) \in \mathbf{Q}[x]$ is not a rational square, we will be able to rule out every subgroup of A_n, including A_n itself, as possibilities for the Galois group of $f(x)$. If we can furthermore show that the Galois group *contains* A_n, it will follow from the next proposition that $\mathrm{Gal}(f)$ is the full symmetric group.

Proposition 2.2.17. *Let $f(x) \in \mathbf{Q}[x]$ be a degree n polynomial and let $G = \mathrm{Gal}(f)$ have finite order. If $G \not\subseteq A_n$ and $G \supseteq A_n$ then $G = S_n$.*

Proof. Let $|G| = m$. By hypothesis, we have that

$$A_n \subsetneq G \subseteq S_n$$

and therefore $|A_n| = n!/2 < m \leq n! = |S_n|$. From Lagrange's Theorem we know that $m|n!$ and so $am = n!$ for some $a \in \mathbf{N}$. If $m < n!$ then $a > 1$ and $n!/2 < m < am = n!$. This implies that $m = n!/a \leq n!/2 < m$, which is a contradiction. Thus $m = n!$ and $G = S_n$. □

To help with showing that $\mathrm{Gal}(f) \supseteq A_n$, we use the following important result of Jordan. We choose to omit the proof of Jordan's Theorem since it is not short and we were unable to find effective way of summarizing it within the general scope of this project.

Theorem 2.2.18 (Jordan)**.** *Let G be a transitive subgroup of S_n. If there exists a prime $p \in (n/2, n-2)$ such that p divides the order of G then $G \supseteq A_n$.*

Proof. See [14, Thm 5.6.2 and Thm 5.7.2]. □

Combining Theorems 2.2.10, 2.2.16, 2.2.18, and Proposition 2.2.17, we now have criterion for showing that the Galois group of a degree n polynomial over $\mathbf{Q}$ is the full symmetric group.

Corollary 2.2.19. *Let $f(x) \in \mathbf{Q}[x]$ be a polynomial of degree n. Suppose that f satisfies the following conditions.*

(i) *$f(x)$ is irreducible over $\mathbf{Q}$.*

(ii) $\mathrm{disc}(f)$ *is not a square in $\mathbf{Q}$.*

(iii) *There exists a prime $p \in (n/2, n-2)$ such that p divides the order of* $\mathrm{Gal}(f)$.

Then $\mathrm{Gal}(f) = S_n$.

We now aim to develop a method for showing that a polynomial satisfies these criterion.

2.3 p-adic Numbers

In this section we provide a basic overview of the p-adic numbers $\mathbf{Q}_p$ with the aim of using them to discuss properties of the *Newton Polygon* in Section 2.4. We provide rigorous definitions of material explicitly used in this project and also present a less formal discussion of the p-adic numbers in general.

The field $\mathbf{Q}_p$ arises by considering the notion of 'distance' in a different way. Due to our familiarity with real numbers, our intuition has been carefully seasoned to measure the interval between two numbers using the absolute value. The traditional absolute value allows us to completely characterization the notion of 'size' in that any real number is a unique distance and direction from zero (positive or negative). The idea of an absolute value turns out to be much more general: given any field K, we can define an absolute value as a function which satisfies certain conditions outlined below. This allows for the definition of a *metric* on K.

Definition 2.3.1. Let K be a field. The function $|\ | : K \to \mathbf{R}$ is called an *absolute value* on K if it satisfies the following conditions.

(i) $|x| = 0$ if and only if $x = 0$.

(ii) $|xy| = |x|\,|y|$ for all $x, y \in K$.

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

If $|\ |$ has the property that $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$ then $|\ |$ is called *non-Archimedean*. If $|\ |$ is not non-Archimedean then we say that $|\ |$ is *Archimedean*. △

The field $\mathbf{Q}_p$ is formed in a similar way to the real numbers: we complete $\mathbf{Q}$ by adjoining to it the limit of every rational Cauchy sequence. The difference is the way in which we define our concept of measure. To construct **R**, we adjoin irrational points on the number line by considering their relative distances from the origin using the absolute value. A different completion arises when we adjoin irrational points using a different unique characteristic of **Q**.

Observe that any integer $m \in \mathbf{Z}$ can be represented uniquely by expanding it in 'base-p' for some prime p (e.g., the integer $242 = 2+3\cdot5+4\cdot5^2+5^3$). We can define an absolute value on **Q**, one which is different from the regular absolute value, that makes use of this 'base-p' expansion. From this alternate absolute value, we may also construct Cauchy sequences and treat their limits (those which do not converge in **Q**) as the formal definitions of p-adic irrational numbers.

Definition 2.3.2. Fix some prime number p and some $n \in \mathbf{Z}-\{0\}$. Let the function $\text{ord}_p : \mathbf{Z}-\{0\} \to \mathbf{Z}$ be defined by

$$\text{ord}_p(n) = \max\{k \in \mathbf{N} : p^k \mid n\},$$

for all $n \in \mathbf{Z}-\{0\}$. We call the integer $\text{ord}_p(n)$ the *p-adic valuation of n.* △

Observe that $\text{ord}_p(n) = \max\{k \in \mathbf{N} : n \equiv 0 \bmod p^k\}$. This allows us to see how the p-adic valuation can intuitively be interpreted as a measure of a number's divisibility by p; larger valuations equate to more factors of p.

The domain of the ord_p function can be extended to include all rational numbers as follows.

Definition 2.3.3. Fix some prime number $p \in \mathbf{Z}$. If $x = a/b \in \mathbf{Q}-\{0\}$ then we define the *p-adic valuation of x* to be

$$\text{ord}_p(x) = \text{ord}_p(a) - \text{ord}_p(b).$$

△

In order to include the number 0 in the domain of ord_p, the convention is often to set $\mathrm{ord}_p(0) = +\infty$. This results from the observation that we can divide 0 by any integer and so $p^k \mid 0$ for every choice of k, no matter how large. In other words, if we look at the 'expression'

$$0 = 0 \cdot (p \cdot p \cdot p \cdots)$$

we see that $p \mid 0$ and so $\mathrm{ord}_p(0) \geq 1$. But $p^2 \mid 0$ also and so $\mathrm{ord}_p(0) \geq 2$. But $p^3 \mid 0$ too and so $\mathrm{ord}_p(0) \geq 3 \ldots$ etc.

We use the following properties of ord_p extensively throughout this project.

Lemma 2.3.4. *Let $x, y \in \mathbf{Q}$. Then*

(i) $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$, *and*

(ii) $\mathrm{ord}_p(x + y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$.

Proof. See [12, Lemma 2.1.3]] □

Using the p-adic valuation, we may now define the p-adic absolute value.

Definition 2.3.5. Fix some prime p and let $x \in \mathbf{Q}$. We define the *p-adic absolute value* of x to be

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p(x)}, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0. \end{cases}$$ △

It is not hard to see that this definition satisfies the criterion outlined in Definition 2.3.1. Similar to the traditional absolute value, the p-adic absolute value also measures the 'closeness' of numbers; p-adic numbers are 'near' one another (have small absolute difference) when they have similar divisibility by a prime p, just as real numbers are near each other when their absolute difference is close to zero.

Example 2.3.6. In $\mathbf{R}$, the numbers -4 and 4 have the same distance from 0 since their absolute values are equal and so both -4 an 4 lie on the perimeter of the closed ball of radius 4 centered at the origin in $\mathbf{R}$. In $\mathbf{Q}_3$ we find a similar phenomena with the numbers

9 and 45. The 3-adic absolute value of both 9 and 45 is $1/3^2$ and so they lie in the closed ball $B = \{x \in \mathbf{Q}_3 : |x| \leq 1/3^2\}$ of radius $1/3^2$ in $\mathbf{Q}_3$. ◊

Example 2.3.7. Observe that the integers $125 = 5^3$ and $1875 = 3 \cdot 5^4$ are not near one another when considered in $\mathbf{Q}$ but are close together in $\mathbf{Q}_5$ since $|5^3 - 3 \cdot 5^4|_5 = |5^3(1-3\cdot 5)|_5 = 5^{-3}$. ◊

Example 2.3.8. We show that $\sqrt{2} \in \mathbf{Q}_7$ by considering the roots of the polynomial $x^2 - 2 \mod 7^n$ for increasing values of n. Observe that 2 is a square modulo 7 since $3^2 \equiv 2 \mod 7$. We can *lift* this solution to higher powers of 7 by observing that

$$\begin{aligned} 3^2 &\equiv 2 \mod 7 \\ (3+7)^2 &\equiv 2 \mod 7^2 \\ (3+7+2\cdot 7^2)^2 &\equiv 2 \mod 7^3. \end{aligned}$$

The process can be continued:

$$\begin{aligned} (3+7+2\cdot 7^2+6\cdot 7^3+7^4+2\cdot 7^5+7^6+2\cdot 7^7+4\cdot 7^8+6\cdot 7^9+6\cdot 7^{10})^2 &\equiv 2 \mod 7^{11} \\ (3+7+2\cdot 7^2+6\cdot 7^3+7^4+2\cdot 7^5+7^6+2\cdot 7^7+4\cdot 7^8+6\cdot 7^9+6\cdot 7^{10}+2\cdot 7^{11})^2 &\equiv 2 \mod 7^{12}. \end{aligned}$$

The fact that a solution to $x^2 - 2 \mod 7^n$ exists for all n is due to *Hensel's Lemma*, which, for our purposes, says that if there is a root of α of $f(x) \mod p$ and $f'(\alpha) \not\equiv 0 \mod p$ then roots of $f(x) \mod p^n$ exist for all powers. Let α_n denote the root of $x^2-2 \mod 7^{n+1}$ (so $\alpha_0 = 3$ and $\alpha_1 = 3+7$) and notice that $\alpha_n \equiv \alpha_{n-1} \mod 7^n$. Thus, $\alpha_n - \alpha_{n-1} \equiv 0 \mod 7^n$ which means that $\alpha_n - \alpha_{n-1}$ has a factor of 7^n and therefore that $|\alpha_n - \alpha_{n-1}|_7 \leq \frac{1}{7^n}$. The non-Archimedean property allows us to state that the sequence $\{\alpha_n\}$ of lifted roots of $x^2 - 2$ forms a Cauchy sequence and so $\{\alpha_n\}$ converges in $\mathbf{Q}_7$. This limit is the 7-adic square root of 2.

◊

Adjoining all limits of Cauchy sequences with respect to a p-adic absolute value results in the field $\mathbf{Q}_p$. We follow Gouvêa [12] in constructing the field of p-adic numbers. If we define the set $\mathscr{C}_p$ by

$$\mathscr{C}_p = \Big\{\{a_n\} : \{a_n\} \text{is a Cauchy sequence with respect to the absolute value } |\ |_p\Big\},$$

let $\{a_n\}, \{b_n\} \in \mathscr{C}_p$ and furthermore define the operations + and $\cdot$ on $\mathscr{C}_p$ by

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}$$

and

$$\{a_n\} \cdot \{b_n\} = \{a_n \cdot b_n\},$$

it can be shown that $\mathscr{C}_p$ is a commutative ring with 1. One can also prove that the set

$$\mathscr{N} = \Big\{\{a_n\} : \lim_{n\to\infty} |a_n|_p = 0\Big\}$$

is a maximal ideal of $\mathscr{C}_p$. Accepting these statements as fact, the p-adic numbers are defined as follows.

Definition 2.3.9. The field $\mathbf{Q}_p$ is defined to be the quotient $\mathscr{C}_p/\mathscr{N}$. △

Note that $\mathbf{Q}$ is necessarily a subfield of $\mathbf{Q}_p$; it is included in $\mathbf{Q}_p$ as the constant Cauchy sequences consisting of rational elements.

We note that every element $x \in \mathbf{Q}_p$ can be written in the form

$$a_{-n_0}p^{-n_0} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots a_n p^n + \cdots$$

where each $a_i \in \mathbf{Z}/p\mathbf{Z}$ and $n_0 = \operatorname{ord}_p(x)$.

The field theory developed in Section 2.2 is also applicable to the p-adic fields. In other words, algebraic extensions of $\mathbf{Q}_p$ can also be formed by taking quotients of irreducible polynomials in $\mathbf{Q}_p$. It turns out that if $K/\mathbf{Q}_p$ is not a Galois extension, then the p-adic absolute value of any $x \in K/\mathbf{Q}_p$ is equal to the absolute value of x in a Galois extension $L/\mathbf{Q}_p$ where $L \supset K$ [12, Lemma 5.3.3.]. It therefore makes sense to define the p-adic absolute value of algebraic elements to be their absolute value in a Galois extension of $\mathbf{Q}_p$.

Definition 2.3.10. Let K be a degree n extension of $\mathbf{Q}_p$. If $x \in K^\times$ then the p-adic valuation $\operatorname{ord}_p(x) \colon K^\times \to \mathbf{Q}$ of x is defined to be

$$\operatorname{ord}_p(x) = \frac{1}{n}\operatorname{ord}_p(\mathbb{N}_{K/\mathbf{Q}_p}(x)).$$

where

$$\mathbb{N}_{K/\mathbf{Q}_p}(x) = \prod_{\sigma \in \operatorname{Gal}(K/\mathbf{Q}_p)} \sigma(x).$$

The *ramification index* of K over $\mathbf{Q}_p$ is defined to be the unique integer e which satisfies

$$\operatorname{ord}_p(K^\times) = \frac{1}{e}\mathbf{Z},$$

where $\operatorname{ord}_p(K^\times)$ is the image of $\operatorname{ord}_p : K^\times \to \mathbf{Q}$. △

Our use of p-adic numbers will mainly be through an object called the *Newton Polygon*, which reveals information about polynomial factorization and Galois groups. Definition 2.3.10 is used in Theorem 2.4.12 to show how the the p-adic Newton Polygon can be used to study Galois groups.

2.4 Newton Polygons

The theory of Newton Polygons is a tool we employ to gain information about a polynomial's algebraic properties. The mathematical machinery behind Newton Polygons is extensive; we offer only a brief summary here, focusing primarily on their usefulness in showing how polynomials can satisfy the criterion outlined in Corollary 2.2.19. We note that Newton Polygons arise through a generalization of the p-adic valuation to polynomials $f(x) \in \mathbf{Q}_p[x]$.

Definition 2.4.1. Fix some prime p and let $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbf{Q}[x]$. The p-adic *Newton Polygon* of f, denoted $\mathtt{NP}_p(f)$, is the lower convex hull of the set of points

$$\{(0, \operatorname{ord}_p(a_0)), (1, \operatorname{ord}_p(a_1)), \ldots, (n, \operatorname{ord}_p(a_n))\}.$$

△

One helpful analogy in picturing the lower convex hull is to imagine the plane $\mathbf{R}^2$ as a cork bulletin board and the points $\{(i, \mathrm{ord}_p(a_i)\}$ above as pins in the board. If we stretch an elastic band around all the pins so that every pin is either inside the band or supporting the band on its perimeter, the lower section of this band (i.e., the lower section connecting the first pin at $(0, \mathrm{ord}_p(a_0))$ and the last pin at $(n, \mathrm{ord}_p(a_n)))$ is the lower convex hull. So for every prime p there exists a p-adic Newton Polygon for a polynomial $f(x) \in \mathbf{Q}[x]$.

Example 2.4.2. Let $f(x) = a_0 + a_1 x + \cdots + a_6 x^6 = 27 + 9x + 4x^2 + 6x^3 + 54x^4 + 3x^5 + 18x^6$. Then $\mathtt{NP}_3(f)$ has the following shape. (Note that we plot all points $(i, \mathrm{ord}_3(a_i))$).

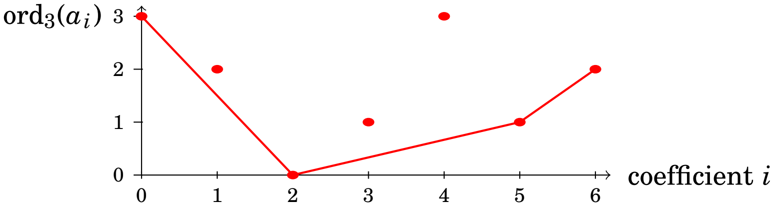


Figure 2.4.1: $\mathtt{NP}_3(27 + 9x + 4x^2 + 6x^3 + 54x^4 + 3x^5 + 18x^6)$

◊

We will often refer to the edges and vertices of a Newton Polygon as *segments* and *breaks*, respectively. The main theorem of Newton Polygons is as follows.

Theorem 2.4.3. *Suppose that $f(x) \in \mathbf{Q}[x]$ is a polynomial of degree n and that $f(x)$ is not divisible by x. Let $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$ denote the vertices of $\mathtt{NP}_p(f)$ and let $m_i = (y_i - y_{i-1})/(x_i - x_{i-1})$ be the slope of the ith segment of $\mathtt{NP}_p(f)$. Then there exists polynomials $f_1, f_2, \ldots, f_r \in \mathbf{Q}_p$ such that:*

(i) *$f(x)$ factors as $f(x) = f_1(x) f_2(x) \cdots f_r(x)$ over $\mathbf{Q}_p$,*

(ii) *the degree of f_i is $x_i - x_{i-1}$ for all $1 \le i \le r$,*

(iii) *every root of f_i in $\bar{\mathbf{Q}}_p$ has p-adic valuation $-m_i$, for all $1 \le i \le r$.*

Proof. [12, Theorem 6.4.7] □

Note that the *length* of a segment is its projection onto the x-axis. Thus we see that $f(x) = 27 + 9x + 4x^2 + 6x^3 + 54x^4 + 3x^5 + 18x^6$ in Example 2.4.2 factors as $f_1(x)f_2(x)f_3(x)$ over $\mathbf{Q}_3$, where $\deg f_1 = 2$, $\deg f_2 = 3$ and $\deg f_3 = 1$. Furthermore, if $\alpha_1, \alpha_2, \alpha_3 \in \bar{\mathbf{Q}}_3$ are respective roots of f_1, f_2 and f_3, then $\operatorname{ord}_p(\alpha_1) = -3/2, \operatorname{ord}_p(\alpha_2) = 1/3$ and $\operatorname{ord}_p(\alpha_3) = 1$.

Definition 2.4.4. Let $f(x) \in \mathbf{Q}[x]$ be a degree n polynomial and let p be a prime number. If $\mathtt{NP}_p(f)$ consists of a single segment of length n with slope $m \neq 0$ then we call the Newton Polygon *pure*. If $\mathtt{NP}_p(f)$ consists of a single segment of length n with slope $m = 0$ then we say that $\mathtt{NP}_p(f)$ is *trivial*. △

It is not apparent, upon preliminary inspection, why a Newton Polygon consisting of a single slope 0 segment should be called trivial. The reason for this denomination is that polynomials with flat Newton Polygons could be either irreducible or reducible and therefore no useful information can be acquired from trivial polygons.

Example 2.4.5. Consider the polynomial $f(x) = 7x^2 - 14$ and $g(x) = 7x^2 + 14$. Both of these polynomials have trivial Newton Polygons at the prime 7. We have shown in Example 2.3.8 that $\sqrt{2} \in \mathbf{Q}_7$ (which implies $-\sqrt{2} \in \mathbf{Q}_7$) and so $f(x)$ splits in $\mathbf{Q}_7$. The second polynomial is irreducible in $\mathbf{Q}_7$ by Hensel's Lemma (see Example 2.3.8) since there is no element in $\mathbf{Z}/7\mathbf{Z}$ which squares to $-2 \equiv 5 \bmod 7$. Thus a flat Newton Polygon can be interpreted in multiple ways: as having multiple slope 0 segments (being reducible) or having a single segment (being irreducible). ♢

The only conclusion that can be made from a trivial Newton Polygon is that the degree d of any irreducible factor of $f(x)$ over $\mathbf{Q}$ must such that $d \geq 1$ (i.e., the degrees of the irreducible factors of $f(x) \in \mathbf{Q}_p$ could combine in any possible way when the polynomial is taken over $\mathbf{Q}$.)

These observations also hold for a slope zero segment of a nontrivial Newton Polygon. We summarize this as a corollary to Theorem 2.4.3.

Corollary 2.4.6. *Let* $\mathtt{NP}_p(f)$ *be the Newton Polygon for* $f(x) \in \mathbf{Q}[x]$ *and let* $g(x) \in \mathbf{Q}[x]$ *be an irreducible factor of* f *with* $\deg g = d$.

(i) If $\mathtt{NP}_p(f)$ *is trivial then* $d \in [1,n]$.

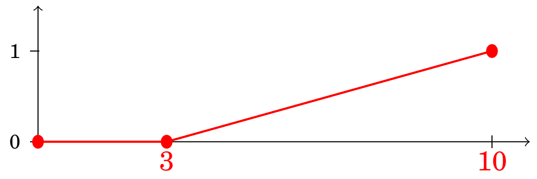
(ii) If $\mathtt{NP}_p(f)$ *has vertices* $(x_0,y_0),(x_1,y_1),\ldots,(x_r,y_r)$ *such that* $y_{i-1} = y_i$ *for some* $i \in (0,r]$ *(i.e.,* $\mathtt{NP}_p(f)$ *has a slope zero segment of length* $L = x_i - x_{i-1}$*) then, recalling that* $f(x) = f_1(x)f_2(x)\cdots f_i(x)\cdots f_r(x) \in \mathbf{Q}_p$, *precisely one of the following holds.*

(a). d *is equal to the sum of any combination of degrees* $\deg f_j$ *(including* $j = i$*),*

(b). d *is equal to the sum of any combination of degrees* $\deg f_j$ *plus some* $a \in [0,L]$, *or*

(c). $d = a$, *for some* $a \in [1,L]$.

Example 2.4.7. Let $f(x) \in \mathbf{Q}(x)$ be a degree 10 polynomial and suppose that there is a prime p for which $\mathtt{NP}_p(f)$ takes on the following shape.



This Newton Polygon tells us that $f(x) = g(x)s(x) \in \mathbf{Q}_p$ where the degree of $g(x)$ is 7 and the degree of $s(x)$ is either 3, or $s(x)$ is the product 3 degree 1 polynomials or it is the product of a degree 1 polynomial and a degree 2 polynomial. Therefore, over the rational numbers, we have the following possible factorizations of $f(x)$ into irreducible polynomials $h(x), r(x), t(x), v(x) \in \mathbf{Q}[x]$. The numbers written underneath each polynomial denote their respective degrees.

$$\underset{10}{h(x)}$$

$$\underset{7}{h(x)}\underset{3}{r(x)}$$

$$\underset{7}{h(x)}\underset{2}{r(x)}\underset{1}{t(x)}$$

$$\underset{7}{h(x)}\underset{1}{r(x)}\underset{1}{t(x)}\underset{1}{v(x)}$$

$$\underset{8}{h(x)}\underset{2}{r(x)}$$

$$\underset{8}{h(x)}\underset{1}{r(x)}\underset{1}{t(x)}$$

$$\underset{9}{h(x)}\underset{1}{r(x)}$$

In accordance with Corollary 2.4.6, the possible degrees for an irreducible factor of $f(x)$ over $\mathbf{Q}$ are 10, 9, 8, 7, 3, 2, or 1. $\Diamond$

Example 2.4.8. Let $f(x) = x^3 + 8x^2 - 2x - 14 = (x^2 - 2)(x + 7)$. Consider the Newton Polygon for f at the prime 7.

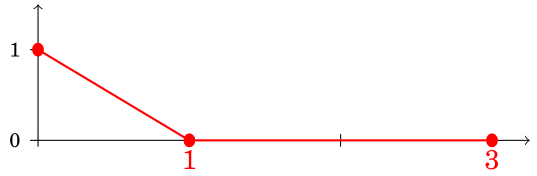


Figure 2.4.2: $\mathtt{NP}_7(x^3 + 8x^2 - 2x - 14)$

This example is different in that we already know the rational factorization of $f(x)$. However, if we were unsure of this polynomial's factorization, the 7-adic Newton Polygon would be of little help; we are only able to conclude that an irreducible factor of $f(x)$ must have degree $d \leq 3$. Note that $f(x)$ actually splits completely in $\mathbf{Q}_7$ since $\pm\sqrt{2} \in \mathbf{Q}_7$. $\Diamond$

If a Newton Polygon at a prime p is pure, we can conclude the 'opposite' of our observations for trivial Newton Polygons. We state this precisely in the following corollary to Theorem 2.4.3.

Corollary 2.4.9. *If there exists some prime number p such that $\texttt{NP}_p(f)$ is pure, then f is irreducible over $\mathbf{Q}$.*

Proof. Suppose that the $\texttt{NP}_p(f(x))$ is pure. It follows from Theorem 2.4.3 (i) that f is irreducible over $\mathbf{Q}_p$. If $f(x)$ is irreducible over $\mathbf{Q}_p$ but reducible over $\mathbf{Q}$ then, since $\mathbf{Q}_p$ contains $\mathbf{Q}$, it must be the case that $f(x)$ is reducible over $\mathbf{Q}_p$ which is a contradiction. □

One useful theorem for determining irreducibility properties of $f(x) \in \mathbf{Q}[x]$ using polynomials that are not pure is seen in the following theorem.

Theorem 2.4.10 (Coleman [4]). *Fix some prime p and let $f \in \mathbf{Q}[x]$ be a polynomial of degree n. If $d \in \mathbf{Z}$ divides the denominator (in lowest terms) of every slope of $\texttt{NP}_p(f(x))$, then d divides the degree of every irreducible factor of f over $\mathbf{Q}$.*

Proof. See the Corollary in [4]. □

The following definition incorporates the slopes of a Newton Polygon at many primes. It is through this definition that we arrive at a satisfactory method for fulfilling item (iii) in the criterion of Corollary 2.2.19 — namely, for showing that Gal$(f) \supseteq A_n$.

Definition 2.4.11. Fix some prime p and let

$$M_p = \{a/b \in \mathbf{Q} \colon a/b \text{ is a slope (in lowest terms) of } \texttt{NP}_p(f)\}.$$

The *Newton Index* of f over $\mathbf{Q}_p$, denoted $\mathcal{N}_f$, is defined to be the least common multiple of every denominator b for all

$$\frac{a}{b} \in \bigcup_p M_p$$

where the union runs over all primes p. △

So $\mathcal{N}_f$ is the least common multiple of all denominators of slopes of every Newton Polygon for f.

Recall from Corollary 2.2.19 that if $f(x) \in \mathbf{Q}[x]$ is irreducible and has discriminant that is not a rational square, then we must only establish the existence of a prime $p \in (n/2, n-2)$, where $n = \deg(f)$, such that p divides the order of $\mathrm{Gal}(f)$ in order to conclude that $\mathrm{Gal}(f) = S_n$. The following theorem hints at a method for this final step.

Theorem 2.4.12. *Let $f(x) \in \mathbf{Q}[x]$ be an irreducible polynomial and let $G = \mathrm{Gal}(f) = Gal(E/\mathbf{Q})$, where E is the splitting field of $f(x)$. Then $\mathscr{N}_f$ divides the order of G. Furthermore, if ℓ is a prime divisor of $\mathscr{N}_f$ in the range $n/2 < \ell < n-2$ then $G \supseteq A_n$.*

Proof. We follow Theorem 2 in [13], filling in some details. Let $m = a/b \in \mathbf{Q}$ be a slope of the Newton Polygon for f at a prime p and let q be a divisor of b. Showing that q divides the order of G will imply that $\mathscr{N}_f$ also divides the order of G since q is chosen arbitrarily (thus the same argument can be repeated for any such divisor of the denominator of a slope, indicating that the least common multiple of these divisors, $\mathscr{N}_f$, must also divide $|G|$). From Theorem 2.4.3(*i*) and (*iii*), we know that there exists an irreducible factor $g(x) \in \mathbf{Q}_p$ of $f(x)$ having root $\gamma \in \bar{\mathbf{Q}}_p$ such that $\mathrm{ord}_p(\gamma) = -m$. Furthermore, letting $d = \deg(g)$, we know that $d \leq \deg(f)$ and that

$$\mathbf{Q}_p(\gamma) \simeq \frac{\mathbf{Q}_p[x]}{(g(x))}$$

is a degree d extension of $\mathbf{Q}_p$ from Theorem 2.2.1. From Definition 2.3.10 we also have that

$$-m = -a/b = \frac{1}{d} \cdot (\mathbb{N}_{\mathbf{Q}_p(\gamma)/\mathbf{Q}_p}(\gamma))$$

and so $-ad = b(\mathbb{N}_{\mathbf{Q}_p(\gamma)/\mathbf{Q}_p}(\gamma))$. Since $q \mid b$ we have that $q \mid ad$. We can see that q does not divide a since a/b is in lowest terms. Thus q divides $d = [\mathbf{Q}_p(\gamma) \colon \mathbf{Q}_p]$. But from Theorem 2.2.3, we also see that d divides $[E_p : \mathbf{Q}_p] = |\mathrm{Gal}(E_p/\mathbf{Q}_p)|$, where E_p is the splitting field of g over $\mathbf{Q}_p$. It is well known that $\mathrm{Gal}(E_p/\mathbf{Q}_p)$ is isomorphic to the decomposition group $D_p = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ where $\mathfrak{p}$ is a prime ideal *lying over* the prime ideal $p\mathbf{Z}$ (this just means that $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$), and furthermore that D_p is a subgroup of $\mathrm{Gal}(E/\mathbf{Q}) = G$ [19, page

99]. Thus $q|d$ implies q divides the order of $\mathrm{Gal}(E_p/\mathbf{Q}_p) \simeq D_p \leq G$ and therefore q divides the order of G by Lagrange's Theorem. Hence we have that $\mathscr{N}_f$ divides the order of the Galois group of $f(x) \in \mathbf{Q}[x]$.

If $q = \ell$ is a prime in the interval $(n/2, n-2)$ then it follows from Jordan's Theorem 2.2.18 that $G \supseteq A_n$. □

2.5 Elliptic Curves and the Supersingular Polynomials

Definition 2.5.1. Let K be a field and let $f(x) \in K[x]$ be a cubic polynomial with no repeated roots. An *elliptic curve*, denoted E/K, is defined by the two variable equation

$$y^2 = f(x).$$

△

The ordered pairs $(x, y) \in K \times K$ which satisfy the above equation are called the K*-points* of the elliptic curve E. These points, together with a special 'point at infinity', denoted O, form an abelian group under a geometric addition law. The point O on E acts as an additive identity in the group structure. Multiplication by some integer m is defined by letting P be a point on E and setting

$$[m]P = \underbrace{P + P \cdots + P}_{m \text{ times}}.$$

We can then ask the question of which points on E have finite order. These points can be considered via the kernel of the multiplication by m map − that is, by considering all the points $P \in E$ for which there exists an integer $m \in \mathbf{Z}$ such that $[m]P = O$. The set $E[m] := \ker[m] = \{P \in E : [m]P = O\}$ is called the *m-torsion subgroup* of E and contains all points of order m on E. It turns out that if the characteristic of K is 0 or p and $p \nmid m$ then $E[m] \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ [17, Page 20]. This seems intuitively clear in the case where $K = \mathbf{C}$ since elliptic curves over $\mathbf{C}$ can be viewed as a complex lattice (this is due to an unintuitive isomorphism between Definition 2.5.1 above and a lattice structure in $\mathbf{C}$ using a complicated change of variables in terms of the *Weierstrass* $\wp$ function and its derivative). Multiplication by m on an elliptic curve $\mathbf{C}/L$, where L is a complex lattice, then maps the points which are on the lattice back to themselves via their coset representation, which is the zero element of $\mathbf{C}/L$.

When $p \mid m$ in characteristic p, it can be shown that either $E[p^r] \simeq \mathbf{Z}/p^r\mathbf{Z}$ or $E[p^r] = \{O\}$ [17, Page 20]. We now define what it means for an elliptic curve to be *supersingular*.

Definition 2.5.2. If $E[p^r](\bar{K}) = \{O\}$ then the elliptic curve E/K is called *supersingular*. △

The following theorem allows us to characterize elliptic curves in a particularly nice way.

Theorem 2.5.3. *Suppose that* $\operatorname{char}(K) \neq 2$*. Then every elliptic curve* E/K *is isomorphic (over* $\bar{K}$*) to an elliptic curve in* Legendre form*:*

$$E_\gamma : y^2 = x(x-1)(x-\gamma),$$

for some $\gamma \in \bar{K}$ *such that* $\gamma \neq 0, 1$.

Proof. [22, Section III, Proposition 1.7] □

Definition 2.5.4. Suppose that $\operatorname{char}(K) \neq 2$ and let E_γ/K be an elliptic curve in Legendre form. The $j-invariant$ of E_γ is defined to be

$$j(E_\gamma) = \frac{2^8(\gamma^2-\gamma+1)^3}{\gamma^2(\gamma-1)^2} \in \mathbf{F}_{p^2}.$$

△

Theorem 2.5.3 now allows us to illustrate the importance of j-invariants.

Theorem 2.5.5. *Suppose that* E_γ *and* E_δ *are two elliptic curves over a field* K*. Then* $j(E_\gamma) = j(E_\delta)$ *if and only if* $E_\gamma \simeq E_\delta$*.*

Proof. [22, Section III, Proposition 1.4(b)] □

We note that the j-invariant of a supersingular elliptic curve is called a *supersingular j-invariant*.

Theorem 2.5.6. *There are only finitely many supersingular elliptic curves in fields of characteristic p.*

Proof. See [22, Section V, Theorem 3.1(a))] and [22, Page 140] □

Theorems 2.5.5 and 2.5.6 imply that there are also only finitely many supersingular j-invariants in characteristic p. This leads to the definition of the supersingular polynomial.

Definition 2.5.7. Let K be a finite field of characteristic $p > 2$, $\gamma \in \bar{K}$ and let $E : y^2 = x(x-1)(x-\gamma)$ be a supersingular elliptic curve. The polynomial

$$\mathfrak{s}_p(x) = \prod_{j(E)} (x - j(E)) \in \mathbf{F}_p$$

is called the *supersingular polynomial* in characteristic p. △

The first 12 supersingular polynomials are

$$\begin{aligned}
\mathfrak{s}_2(x) &= x \\
\mathfrak{s}_3(x) &= x - 1728 \\
\mathfrak{s}_5(x) &= x \\
\mathfrak{s}_7(x) &= x - 1728 \\
\mathfrak{s}_{11}(x) &= x(x - 1728) \\
\mathfrak{s}_{13}(x) &= x - 5 \\
\mathfrak{s}_{17}(x) &= x(x - 8) \\
\mathfrak{s}_{19}(x) &= (x - 7)(x - 1728) \\
\mathfrak{s}_{23}(x) &= x(x - 19)(x - 1728) \\
\mathfrak{s}_{29}(x) &= x(x - 2)(x - 25) \\
\mathfrak{s}_{31}(x) &= (x - 2)(x - 4)(x - 1728) \\
\mathfrak{s}_{37}(x) &= (x - 8)(x^2 - 6x - 6),
\end{aligned}$$

where the coefficients of each $\mathfrak{s}_p(x)$ are taken modulo p. The following Theorem allows us a method for computing the supersingular polynomial.

Theorem 2.5.8. *Let K be a finite field of characteristic $p > 2$.*

(i). Let $m = (p-1)/2$ and define a polynomial

$$H_p(t) = \sum_{j=0}^{m} \binom{m}{j}^2 t^j.$$

Let $\gamma \in \bar{K}$, $\gamma \neq 0, 1$. Then the elliptic curve

$$E : y^2 = x(x-1)(x-\gamma)$$

is supersingular if and only if $H_p(\gamma) = 0$.

(ii). The polynomial $H_p(t)$ has distinct roots in $\bar{K}$. Up to isomorphism, there are precisely

$$\lfloor p/12 \rfloor + \varepsilon_p$$

supersingular elliptic curves in characteristic p, where $\varepsilon_3 = 1$, and for $p \geq 5$,

$$\varepsilon_p = \begin{cases} 0 & \text{if } p \equiv 1 \mod 12, \\ 1 & \text{if } p \equiv 5 \bmod 12 \text{ or } p \equiv 7 \bmod 12, \\ 2 & \text{if } p \equiv 11 \bmod 12. \end{cases}$$

Proof. [22, Section V, Theorem 4.1(ii),(iii)] □

Example 2.5.9. We compute the supersingular j-invariants in characteristic 37. This is an important example since $\mathfrak{s}_{37}(x)$ is the first supersingular polynomial whose roots are not completely contained in $\mathbf{F}_{37}$ (as shown in the list of supersingular polynomials above).

Theorem 2.5.8 tells us that if there exists some $\gamma \in \bar{\mathbf{F}}_{37^k}$ such that $\gamma \neq 0, 1$ and $H_{37}(\gamma) = 0$, then the elliptic curve

$$E_\gamma : y^2 = x(x-1)(x-\gamma)$$

is supersingular. Therefore, if we can find the roots γ of $H_{37}(t)$, then the supersingular j-invariants will be given by

$$j(E_\gamma) = \frac{2^8(\gamma^2 - \gamma + 1)^3}{\gamma^2(\gamma - 1)^2}.$$

The first step is to calculate the polynomial $H_p(t)$, called the *Hasse invariant* of elliptic curves in Legendre form, at the prime $p = 37$ and then reduce this polynomial modulo 37. Direct computation shows that

$$H_{37}(t) = \sum_{j=0}^{18} \binom{18}{j}^2 t^j$$

factors into the following 9 quadratics modulo 37:

$$t^2 + 4t + 33$$

$$t^2 + 2t + 9$$

$$t^2 + 6t + 26$$

$$t^2 + 12t + 34$$

$$t^2 + 23t + 10$$

$$t^2 + 29t + 33$$

$$t^2 + 31t + 1$$

$$t^2 + 33t + 12$$

$$t^2 + 36t + 9.$$

Observe that each of the 18 roots $\gamma_i \in \bar{\mathbf{F}}_{37^k}$ of $H_{37}(t)$ will define a supersingular elliptic curve in characteristic 37. However, since $\varepsilon_{37} = 0$ (because $37 \equiv 1 \mod 12$) we see from Theorem 2.5.8 that all but

$$\lfloor 37/12 \rfloor + \varepsilon_{37} = 3$$

of these elliptic curves will be isomorphic. Equivalently, of the 18 distinct roots of $H_{37}(t)$, we should find that only three are distinct under the image of j, and since two elliptic curves are isomorphic if and only if they have the same j-invariant, this will imply that there can only be three non-isomorphic supersingular elliptic curves in characteristic 37. These observations show that the supersingular polynomial $\mathfrak{s}_{37}(x)$ has degree 3.

We now proceed with the computation. Consider the first factor $t^2+4t+33$. If $\gamma \in \bar{\mathbf{F}}_{37^k}$ is a root of $t^2+4t+33$ then $\gamma^2+4\gamma+33 \equiv 0 \bmod 37$ and so $\gamma^2 \equiv -4\gamma-33 \bmod 37$. Using this fact successively and reducing coefficients modulo 37 yields

$$\begin{aligned}
j(E_\gamma) &\equiv \frac{2^8(\gamma^2-\gamma+1)^3}{\gamma^2(\gamma-1)^2} \bmod 37 \\
&\equiv \frac{2^8((-4\gamma-33)-\gamma+1)^3}{(-4\gamma-33)((-4\gamma-33)-2\gamma+1)} \bmod 37 \\
&\equiv \frac{32\gamma+20}{4\gamma+21} \bmod 37 \\
&\equiv \frac{8(4\gamma+21)-148}{4\gamma+21} \bmod 37. \\
&\equiv 8-37\left(\frac{4}{4\gamma+21}\right) \bmod 37 \\
&\equiv 8 \bmod 37.
\end{aligned}$$

This means that 8 is the supersingular j-invariant of the elliptic curve $E\colon y^2 = x(x-1)(x-\gamma)$, where γ is a root of $t^2+4t+33$ in $\bar{\mathbf{F}}_{37^k}$. Therefore 8 is a supersingular j-invariant in characteristic 37 and $\mathfrak{s}_{37}(x)$ has $(x-8)=(x+29) \mod 37$ as a factor.

We now consider the second factor t^2+2t+9 of $H_{37}(t)$. Similarly to above, we see that if $r \in \bar{\mathbf{F}}_{37^k}$ is a root of t^2+2t+9 then $r^2 \equiv -2r-9 \bmod 37$. From this we find that

$$\begin{aligned}
j(E_r) &\equiv \frac{2^8((-2r-9)-r+1)^3}{(-2r-9)((-2r-9)-2r+1)} \bmod 37 \\
&\equiv 30r+33 \bmod 37.
\end{aligned}$$

Unlike the factor $t^2+4t+33$, whose roots defined two isomorphic elliptic curves, we see that the value of the j-invariant at a root of $t^2+4t+33$ will depend on which of the two roots r is chosen. We know from Definition 2.5.4 that $j(E_r) \in \mathbf{F}_{37^2}$ (note that we have defined the j-invariant in this way, but the fact that $j(E_r) \in \mathbf{F}_{p^2}$ can actually be shown (see [22, page 140])). Observe that $t^2+4t+33$ is irreducible in $\mathbf{F}_{37}$ and so

$$\mathbf{F}_{37^2} \simeq \frac{\mathbf{F}_{37}[t]}{(t^2+4t+33)} \simeq \mathbf{F}_{37}(r)$$

by Theorem 2.2.1.

Solving $r^2 + 4r + 33 = 0$ using the quadratic formula yields $r = (-2 \pm \sqrt{4-36})/2 \equiv -1 \pm 19\sqrt{5} \bmod 37$ and hence we see that $\mathbf{F}_{37}(r) = \mathbf{F}_{37}(-1 \pm 19\sqrt{5}) = \mathbf{F}_{37}(\sqrt{5})$ since $(r+1)/\pm 19 = \sqrt{5}$. Substituting $r = -1 \pm 19\sqrt{5}$ into the formula for $j(E_r)$ above gives

$$\begin{aligned} j(E_r) &= 30(-1 \pm 19\sqrt{5}) + 33 \\ &= 3 \pm 15\sqrt{5} \in \mathbf{F}_{37}(\sqrt{5}) \simeq \mathbf{F}_{37^2} \end{aligned}$$

Thus we see that both $3 + 15\sqrt{5}$ and $3 - 15\sqrt{5}$ are supersingular j-invariants in characteristic 37 and so $(x - (3 + 15\sqrt{5}))(x - (3 - 15\sqrt{5})) = x^2 + 31x + 31 \in \mathbf{F}_{37}$ is also a factor of $\mathfrak{s}_{37}(x)$. Thus we have found the 3 distinct j-invariants in characteristic 37 and

$$\mathfrak{s}_{37}(x) = (x+29)(x^2 + 31x + 31) \in \mathbf{F}_{37}.$$

It can be checked that the other seven factors of $H_{37}(t)$ also define elliptic curves with j-invariant 8 or $3 \pm 15\sqrt{5}$.

◊

2.6 Current Conjectures and Results

The theory presented in the last sections allow us to give motivation for this project and precisely state our goals. We aim to investigate a family of polynomials that reduce to the supersingular polynomials when reduced modulo a prime p. Rational polynomials with this property are called *supersingular lifts*.

Definition 2.6.1. Let $f(x) \in \mathbf{Q}[x]$ and let $g(x) \in \mathbf{F}_p[x]$. If $f(x) \equiv g(x) \bmod p$ then we call $f(x)$ a *rational lift* or *lift* of $g(x)$. △

There have been several well-studied lifts of $\mathfrak{s}_p(x)$. In particular, Mahlburg and Ono have conjectured in [18] that the lifts which we study in this project are irreducible over $\mathbf{Q}$ with maximal Galois groups. In order to define these lifts of $\mathfrak{s}_p(x)$, recall the following definition.

Definition 2.6.2. Let $(\alpha,\beta) \in \mathbf{R}\times\mathbf{R}$. The polynomial

$$P_n^{(\alpha,\beta)}(x) = \sum_{j=0}^{n} \binom{n+\alpha}{n-j}\binom{n+\beta}{j}\left(\frac{x-1}{2}\right)^j\left(\frac{x+1}{2}\right)^{n-j}.$$

is called the nth degree *Jacobi Polynomial.* △

We will focus on the family of polynomials

$$\mathscr{K}_n^{(\lambda,\mu)}(x) = 3^n n! P_n^{(\lambda/3,\mu/2)}(4x+1),$$

where $\lambda,\mu \in \{\pm 1\}$. In order to show that they reduce to $\mathfrak{s}_p(x)$, we present the following Theorem.

Theorem 2.6.3 (Brillhart and Morton [2])**.** *For a prime $p>3$, let $p \equiv \varepsilon_p \bmod 12$, where $\varepsilon_p = 1,5,7,11$ and let $n=(p-\varepsilon_p)/12$. The supersingular j-invariants in characteristic p which are not 0 or 1728 (* mod p*) coincide with the roots in $\bar{\mathbf{F}}_p$ of the polynomial*

$$J_p(x) = (1728)^n P_n^{(\alpha,\beta)}\left(1-\frac{x}{864}\right),$$

where

$$\begin{aligned}
(\alpha,\beta) &= (-1/3,-1/2) \text{ if } \varepsilon_p = 1,\\
(\alpha,\beta) &= (1/3,-1/2) \text{ if } \varepsilon_p = 5,\\
(\alpha,\beta) &= (-1/3,1/2) \text{ if } \varepsilon_p = 7,\\
(\alpha,\beta) &= (1/3,1/2) \text{ if } \varepsilon_p = 11.
\end{aligned}$$

Proof. See [2, Theorem 3] □

Example 2.6.4. We compute $\mathfrak{s}_{37}(x)$ using Brillhart and Morton's J_p function. Since $37 \equiv 1 \bmod 12$ we let $n = (37-1)/12 = 3$ and set $(\alpha,\beta) = (-1/3,-1/2)$. Then

$$\begin{aligned} J_{37}(x) &= (1728)^3 P_3^{(-1/3,-1/2)}\left(1-\frac{x}{864}\right) \\ &= \frac{-14725}{1296}x^3 + 30400x^2 - 21012480x + 2548039680 \\ &\equiv (x+29)(x^2+31x+31) \bmod 37 \\ &= \mathfrak{s}_{37}(x). \end{aligned}$$

$\Diamond$

We now show that the $\mathscr{K}_n^{(\lambda,\mu)}(x)$ polynomials are a shift of $J_p(x)$. Observe that if γ is a root of $J_p(x)$ over a field F (of characteristic 0 or p) then $J_p(\gamma) = (1728)^n P_n^{(\alpha,\beta)}\left(1-\frac{\gamma}{864}\right) = 0$. Solving $4x+1 = 1-\gamma/864$ for x we find that any root γ of J_p is mapped to the root $\gamma' = -\gamma/(4\cdot 864) = -\gamma/3456 \in F$ of $\mathscr{K}_n^{(\lambda,\mu)}(x)$. This can be seen by letting $J_p(\gamma) = 0$ and observing that

$$\begin{aligned} \mathscr{K}_n^{(\lambda,\mu)}(-\gamma/3456) &= 3^n n! P_n^{(\lambda/3,\mu/2)}(4(-\gamma/(4\cdot 864))+1) \\ &= 3^n n! P_n^{(\lambda/3,\mu/2)}(1-\gamma/864) \\ &= \frac{3^n n!}{1728^n} J_p(\gamma) \\ &= 0. \end{aligned}$$

We may therefore describe a bijection between between roots of J_p and $\mathscr{K}_n^{(\lambda,\mu)}$. The map

$$\gamma \mapsto -\gamma/3456$$

sends a root of J_p to a root of $\mathscr{K}_n^{(\lambda,\mu)}$, and the map

$$\gamma' \mapsto -3456\gamma'$$

sends a root of $\mathscr{K}_n^{(\lambda,\mu)}$ to a root of J_p (since $J_p(-3456\gamma') = (1728)^n P_n^{(\alpha,\beta)}(4\gamma'+1) = \mathscr{K}_n^{(\lambda,\mu)}(\gamma') = 0$). Because of this bijection, we see that the polynomials $\mathscr{K}_n^{(\lambda,\mu)}(x)$ have the same irreducibility and Galois properties as the J_p polynomials over F. In particular, if $\mathscr{K}_n^{(\lambda,\mu)}$ is irreducible over $\mathbf{Q}$ then so is J_p. Furthermore, since the roots of J_p correspond to the roots of $\mathfrak{s}_p$ in $\bar{\mathbf{F}}_{p^k}$ (which are the supersingular j-invariants), we are led to the following important remark.

Remark 2.6.5. Let $p \equiv \varepsilon_p \bmod 12$, where $\varepsilon_p = 1, 5, 7, 11$, and $n = (p - \varepsilon_p)/12$. Fix $(\lambda,\mu) = (\pm 1, \pm 1)$ using the same signs as (α,β) in Theorem 2.6.3. Then

(i) $\mathscr{K}_n^{(\lambda,\mu)}(-x/3456) \equiv \mathfrak{s}_p(x) \bmod p$, and

(ii) if $\gamma' \in \bar{\mathbf{F}}_{p^k}$ is a root of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ then $-3456\gamma' \in \mathbf{F}_{p^2}$ is a supersingular j-invariant in characteristic p. $\diamondsuit$

Building on the previous examples, we now present the above two observations using the prime $p = 37$. In order to make computations involving $\mathscr{K}_n^{(\lambda,\mu)}$ easier, we use the fact (see Lemma 3.1.1) that

$$\mathscr{K}_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n} \binom{n}{j} \alpha_j \beta_j x^j,$$

where

$$\alpha_j = \prod_{k=0}^{n-j-1} (3n + \lambda - 3k) = (3n + \lambda)(3n + \lambda - 3 \cdot 1) \cdots (3n + \lambda - 3(n - j - 1)),$$

$$\beta_j = \prod_{k=0}^{j-1} (6n + 6 + \epsilon + 6k) = (6n + 6 + \epsilon)(6n + 6 + \epsilon + 6 \cdot 1) \cdots (6n + 6 + \epsilon + 6(j - 1))$$

and $\epsilon = 2\lambda + 3\mu$.

Example 2.6.6. Let $p = 37$. We begin with observation (i) in Remark 2.6.5 and show that $\mathcal{K}_3^{(-1,-1)}(-x/3456)$ reduces to $\mathfrak{s}_{37}$ modulo 37. Letting $X = -x/3456$, observe that

$$\begin{aligned}
\mathcal{K}_3^{(-1,-1)}(X) &= \sum_{j=0}^{3} \binom{3}{j} \alpha_j \beta_j X^j \\
&= 8 \cdot 5 \cdot 2 + 3(8 \cdot 5)(19)X + 3(8)(19 \cdot 25)X^2 + (19 \cdot 25 \cdot 31)X^3 \\
&= 8 \cdot 5 \cdot 2 - \frac{3(8 \cdot 5)(19)}{3456}x + \frac{3(8)(19 \cdot 25)}{3456^2}x^2 - \frac{19 \cdot 25 \cdot 31}{3456^3}x^3 \\
&\equiv (x+29)(x^2+31x+31) \bmod 37 \\
&= \mathfrak{s}_{37}(x).
\end{aligned}$$

We now consider observation (ii) in Remark 2.6.5 and describe the three supersingular j-invariants in characteristic 37 by finding the roots of $\mathcal{K}_3^{(-1,-1)}(x)$ in characteristic 37. Direct computation shows that

$$\begin{aligned}
\mathcal{K}_3^{(-1,-1)}(x) &= 8 \cdot 5 \cdot 2 + 3(8 \cdot 5)(19)x + 3(8)(19 \cdot 25)x^2 + (19 \cdot 25 \cdot 31)x^3 \\
&= (x+3)(x^2+30x+35) \in \mathbf{F}_{37} \\
&= (x+3)(x-(22+\sqrt{5}))(x-(22-\sqrt{5})) \in \mathbf{F}_{37^2}
\end{aligned}$$

This last equality was found using the same method as in Example 2.5.9, namely, by using the quadratic formula to find the roots of $x^2+30x+35$ and noting that

$$\mathbf{F}_{37^2} \simeq \frac{\mathbf{F}_{37}[x]}{(x^2+30x+35)} \simeq \mathbf{F}_{37}(\sqrt{5}).$$

We know from Example 2.5.9 that the supersingular j-invariants in characteristic 37 are 8 and $3 \pm 15\sqrt{5}$. Since -3 and $22 \pm \sqrt{5}$ at the roots of $\mathcal{K}_3^{(-1,-1)}(x)$ in characteristic 37, the multiplication by -3456 map applied to these roots gives

$$\begin{aligned}
-3456(-3) &\equiv 8 \bmod 37 \\
-3456(22 \pm \sqrt{5}) &= 3 \pm 15\sqrt{5} \bmod 37
\end{aligned}$$

as desired. ♢

We now attempt to explain why it might be important to show that the supersingular lifts $\mathscr{K}_n^{(\lambda,\mu)}(x)$ are irreducible with Galois groups S_n. From topics in algebraic number theory (see [19]), we know that the reduction $\mathscr{K}_n^{(\lambda,\mu)}(x) \equiv \mathfrak{s}_p(x) \bmod p$ gives information about how the prime p splits in the field obtained by adjoining a root $\mathscr{K}_n^{(\lambda,\mu)}(x)$ to $\mathbf{Q}$. Roughly speaking, knowing that the Galois group of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is the full symmetric group allows us to gauge the number of primes with the same splitting behaviour as p by invoking a result known as the *Chebotarev Density Theorem* [19, page 240]. Furthermore, an S_n Galois group indicates that the roots of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ are as 'unstructured as possible', meaning that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ has an inherent 'randomness' amongst its roots.

Mahlburg and Ono have given many values of n for which the discriminant of $\mathscr{K}_n^{(\lambda,\mu)}$ is not a rational square. More recently, techniques from analytic number theory have permitted the same result for all n [9]. We give some details of this proof here.

A well-known formula for the discriminant (see [23, Theorem 6.71]) of the nth Jacobi polynomial is given by

$$\operatorname{disc} P_n^{(\alpha,\beta)}(x) = 2^{-n(n-1)} \prod_{k=1}^{n} k^{k-2n+2}(k+\alpha)^{k-1}(2k+\beta)^{k-1}(n+k+\alpha+3\beta)^{n-k}. \tag{2.6.1}$$

Formula 2.6.1, used in conjunction with basic equalities regarding the discriminant of both shifted and scaled polynomials, allows for the conclusion that $\operatorname{disc}\mathscr{K}_n^{(\lambda,\mu)}(x) \in \mathbf{Z}$. The proof given in [9] proceeds to construct an argument regarding the prime divisors of $\operatorname{disc}\mathscr{K}_n^{(\lambda,\mu)}(x)$. In particular, they show that for every n and $\lambda, \mu \in \{\pm 1\}$ there exists a prime p such that $\operatorname{ord}_p(\operatorname{disc}\mathscr{K}_n^{(\lambda,\mu)}(x))$ is an odd integer, which therefore implies that $\operatorname{disc}\mathscr{K}_n^{(\lambda,\mu)}(x)) \notin \mathbf{Q}^{\times 2}$. The basic details are as follows. From [19] we have the following equalities for all $a, b, c \in \mathbf{R}$:

$$\operatorname{disc} f(x+a) = \operatorname{disc} f(x) \ \text{ and } \ \operatorname{disc} b f(cx) = (b^2 c^n)^{n-1} \operatorname{disc} f(x).$$

These properties, together with formula (2.6.1), can be used to show that

$$\operatorname{disc}\mathscr{K}_n^{(\lambda,\mu)}(x) = 3^{n^2-n} \prod_{k=1}^{n} k^k (3k+\lambda)^{k-1}(2k+\mu)^{k-1}(6n+6k+2\lambda+3\mu)^{n-k}.$$

Now, if there exists some prime $p \in [6n+6+2\lambda+3\mu, 12n+2\lambda+3\mu]$ then

$$\begin{aligned} \mathrm{ord}_p\left(3^{n^2-n}\prod_{k=1}^{n} k^k(3k+\lambda)^{k-1}(2k+\mu)^{k-1}\right) &= \mathrm{ord}_p(3^{n^2-n}) + \mathrm{ord}_p\left(\prod_{k=1}^{n} k^k(3k+\lambda)^{k-1}(2k+\mu)^{k-1}\right) \\ &= 0, \end{aligned}$$

since p is greater than every term in rightmost product above. Furthermore, if $p = 6n + 6k' + 6 + 2\lambda + 3\mu$ for some $k' \in [1, n-1]$ then

$$\begin{aligned} \mathrm{ord}_p(\mathrm{disc}\,\mathscr{K}_n^{(\lambda,\mu)}(x)) &= \mathrm{ord}_p\left(\prod_{k=1}^{n}(6n+6k+2\lambda+3\mu)^{n-k}\right) \\ &= n-k'. \end{aligned}$$

In the case of $\lambda = \mu = 1$, it is not difficult to see that $[6n+11, 12n+5] \supseteq [6n+11, 1.9(6n+11)]$ whenever $n \geq 27$. Letting $x = 6n+11$, our goal is therefore to find primes $p = 6n+6k'+6+2\lambda+3\mu = 6(n+k'+1)+5 \in [x, 1.9x]$ such that the value $n-k'$ is odd. Consider that $n-k'$ is odd whenever $n+k'+1$ is even and that $n+k'+1$ is even whenever $p \equiv 5 \bmod 12$. It follows from [7, Theorem 1], and a variation on the results presented there, that for all $x > 479$ (and therefore all $n > (479-11)/6 = 78$), the interval $[x, 1.9x]$ contains a prime $p \equiv 5 \bmod 12$. The remaining cases can be checked via direct computation in the computer algebra system Pari/GP. We can therefore state the following Theorem.

Theorem 2.6.7. *Fix n and $\lambda, \mu \in \{\pm 1\}$. Then the discriminant of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is not a square in $\mathbf{Q}$ and therefore $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}) \not\subseteq A_n$.*

Theorem 2.6.7 satisfies item (ii) of the criterion stated in Corollary 2.2.19. Thus, if we can show that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ satisfies items (i) and (iii) of the same Corollary (namely, that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible and that $\mathscr{K}_n^{(\lambda,\mu)}(x) \supseteq A_n$) it will follow that $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) = S_n$. We investigate both of these questions using the theory of Newton Polygons outlined in Section 2.4. Our results encompass new cases of irreducibility and the description of many Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes in the interval $(n, 12n+2\lambda+3\mu]$. Furthermore, our work with Newton Polygons used together with a conjecture of Hardy and Littlewood gives strong evidence that the Galois group of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ over $\mathbf{Q}$ is S_n. We also present several conjectures regarding $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at some special degrees that yield particularly interesting p-adic factorizations.

3
Newton Polygons

3.1 General Observations

In this section we specify intervals that contain primes for which $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ is trivial, therefore allowing us to determine the primes for which interesting Newton Polygons arise. We begin by presenting a formula for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ (which we have already seen in Example 2.6.6) that allows us to study the polynomial's coefficients more easily.

Lemma 3.1.1. *Let*

$$\alpha_j = \prod_{k=0}^{n-j-1}(3n+\lambda-3k) \quad \textit{and} \quad \beta_j = \prod_{k=0}^{j-1}(6n+6+\epsilon+6k)$$

where $\epsilon = 2\lambda + 3\mu$. Define both α_n and β_0 to be 1. Then

$$\mathscr{K}_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n}\binom{n}{j}\alpha_j\beta_j x^j.$$

Proof. We use the following identity given in [23, page 62]:

$$P_n^{(\alpha,\beta)}(x) \quad = \quad \sum_{j=0}^{n}\binom{n+\alpha}{n-j}\binom{n+\alpha+\beta+j}{j}\Big(\frac{x-1}{2}\Big)^j. \tag{3.1.1}$$

Letting $S = n+\lambda/3+\mu/2+j$, we have that

$$
\begin{aligned}
\mathscr{K}_n^{(\lambda,\mu)}(x) &= 3^n n! P_n^{(\lambda/3,\mu/2)}(4x+1)\\
&= 3^n n! \sum_{j=0}^{n} \binom{n+\lambda/3}{n-j}\binom{S}{j}(2x)^j
\end{aligned}
$$

from equation (3.1.1). Expanding the binomial coefficients and moving $n!$ (which is a constant since n is fixed) into the sum yields

$$
\mathscr{K}_n^{(\lambda,\mu)}(x) = 3^n \sum_{j=0}^{n} \frac{n!}{j!(n-j)!} \overbrace{(n+\lambda/3)(n+\lambda/3-1)\cdots(\lambda/3+j+1)}^{n-j\text{ terms}}\overbrace{S(S-1)\cdots(S-(j-1))}^{j\text{ terms}}(2x)^j.
$$

Furthermore, after multiplying $3^n = 3^{n-j}3^j$ into the sum we obtain

$$
\begin{aligned}
\mathscr{K}_n^{(\lambda,\mu)}(x) &= \sum_{j=0}^{n}\binom{n}{j}\Big[(3n+\lambda)(3n+\lambda-3)\cdots(\lambda+3j+3)\Big]3^j2^j\Big[S(S-1)\cdots(S-(j-1))\Big]x^j\\
&= \sum_{j=0}^{n}\binom{n}{j}\prod_{k=0}^{n-(j+1)}(3n+\lambda-3k)\prod_{k=0}^{j-1}(6S-6(j-1)+6k)x^j\\
&= \sum_{j=0}^{n}\binom{n}{j}\prod_{k=0}^{n-(j+1)}(3n+\lambda-3k)\prod_{k=0}^{j-1}(6(n+\lambda/3+\mu/2+j)-6(j-1)+6k)x^j\\
&= \sum_{j=0}^{n}\binom{n}{j}\prod_{k=0}^{n-(j+1)}(3n+\lambda-3k)\prod_{k=0}^{j-1}(6n+2\lambda+3\mu+6+6k)x^j\\
&= \sum_{j=0}^{n}\binom{n}{j}\alpha_j\beta_jx^j.
\end{aligned}
$$

□

Example 3.1.2. Let $n=4$ and let $\lambda=\mu=1$. Then

$$
\begin{aligned}
\mathscr{K}_4^{(1,1)}(x) &= \sum_{j=0}^{4}\binom{3}{j}\alpha_j\beta_jx^j\\
&= \alpha_0+\binom{4}{1}\alpha_1\beta_1x+\binom{4}{2}\alpha_2\beta_2x^2+\binom{4}{3}\alpha_3\beta_3x^3+\beta_4x^4,
\end{aligned}
$$

where this last expression is equal to

$$
13\cdot10\cdot7\cdot4+4(13\cdot10\cdot7)(35)x+6(13\cdot10)(35\cdot41)x^2+4(13)(35\cdot41\cdot47)x^3+35\cdot41\cdot47\cdot53x^4.
$$

Multiplying through yields

$$
\mathscr{K}_4^{(1,1)}(x) = 3640+127400x+1119300x^2+3507140x^3+3574585x^4.
$$

◊

For ease of notation, we denote the jth coefficient of $\mathscr{K}_n^{(\lambda,\mu)}$ (which we now know to be $\binom{n}{j}\alpha_j\beta_j$) by A_j. It will later become useful to look at specific terms in the products α_j and β_j. We therefore present the following definitions.

Definition 3.1.3. Let $a_k = 3n+\lambda-3k$ and $b_k = 6n+6+\epsilon+6k$ to be the kth terms in the products α_j and β_j, respectively. In accordance with Lemma 2.0.1, we define $\alpha_n = a_{-1} = 1$ and $\beta_0 = b_{-1} = 1$. △

Thus,

$$\alpha_j = \prod_{k=0}^{n-j-1} a_k \text{ and } \beta_j = \prod_{k=0}^{j-1} b_k.$$

Note that $a_k \in [\lambda+3, 3n+\lambda]$ and that $b_k \in [6n+\epsilon+6, 12n+\epsilon]$, since the index k runs through $0,\ldots,n-1$. Furthermore, it is helpful to keep in mind that $\{a_k\}$ forms a decreasing sequence and $\{b_k\}$ forms an increasing sequence.

Remark 3.1.4. For reference, we collect the definitions discussed above.

- $\mathscr{K}_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n} A_j x^j = \sum_{j=0}^{n} \binom{n}{j} \alpha_j \beta_j x^j.$
- $\alpha_j = a_0 a_1 \cdots a_{n-j-1} = (3n+\lambda)(3n+\lambda-3\cdot 1)\cdots(3n+\lambda-3(n-j-1)).$
- $\beta_j = b_0 b_1 \cdots b_{j-1} = (6n+6+\epsilon)(6n+6+\epsilon+6\cdot 1)\cdots(6n+6+\epsilon+6(j-1)).$

◊

Lemma 3.1.1 allows us to make some general observations regarding the prime divisors of the jth coefficient A_j of $\mathscr{K}_n^{(\lambda,\mu)}(x)$. Upon preliminary inspection, we see that any prime divisor p of α_j must have the property that $p \leq 3n+\lambda = a_0$ (or else p would be greater than α_j). Furthermore, if q is a prime divisor of β_j then it must also be true that $q \leq 12n+\epsilon = b_{n-1}$ for the same reason. Restrictions regarding the the prime divisors of $\binom{n}{j}$ can also be seen in the following lemma.

Lemma 3.1.5. *Let p be a prime and let $n \in \mathbf{N}$. If $p > n$ then* $\operatorname{ord}_p(\binom{n}{j}) = 0$.

Proof. Since $p > n \geq j$ we have that

$$\begin{aligned} \operatorname{ord}_p\left(\binom{n}{j}\right) &= \operatorname{ord}_p\left(\frac{n!}{j!(n-j)!}\right) \\ &= \operatorname{ord}_p(n!) - \operatorname{ord}_p(j!) - \operatorname{ord}_p((n-j)!) \\ &= 0. \end{aligned}$$

□

It must also be the case that, if p is a prime divisor of α_j or β_j, then p must divide one of the terms a_k or b_k respectively. This is obvious, though we make it clear in the following lemma.

Lemma 3.1.6. *Let p be a prime and let $\{m_j\}_{j=0}^{n}$ be a sequence of integers . If* $\operatorname{ord}_p(\prod_{j=0}^{n} m_j) \geq 1$ *then there exists some $i \leq n$ such that $p \mid m_i$.*

Proof. Suppose that $n = 1$ and that $\operatorname{ord}_p(m_0 m_1) \geq 1$. If we write m_0 and m_1 in their respective prime factorizations we see that p must be a term in at least one of these factorizations and thus that $p \mid m_0$ or $p \mid m_1$. The result now follows from induction on n. □

Though subtle, Lemma 3.1.6 allows us to definitively see that any prime divisor of $\alpha_j = \prod a_k$ or $\beta_j = \prod b_k$ must be a prime divisor of one of the terms a_k or b_k for some $k \in [0, n-1]$ (this k need not be the same for a_k or b_k). This observation implies that every non-trivial Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes in the interval $[b_0, b_{n-1}] = [6n+\epsilon+6, 12n+\epsilon]$ will be determined only by the terms b_k in the expansion of β_j since these primes are greater than each term in the expansions of α_j and $\binom{n}{j}$. Furthermore, we see that the Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes strictly larger than $12n+\epsilon$ must be trivial. We record this observation for later reference.

Remark 3.1.7. If p is a prime in the interval $[6n+\epsilon+6, 12n+\epsilon]$ then $\operatorname{ord}_p(\alpha_j) = \operatorname{ord}_p(\binom{n}{j}) = 0$ for all $j \in [0,n]$ $\diamondsuit$

It can also be noted that primes in the range $[2, a_0] = [2, 3n+\lambda]$ may divide either α_j, β_j or $\binom{n}{j}$, but that primes in the range $(n, 3n+\lambda]$ can only divide α_j or β_j (since each prime in the latter interval is greater than n and therefore cannot divide $\binom{n}{j}$). Consequently, it is possible for primes in either of these intervals to yield non-trivial Newton Polygons, though we presently have no criterion allowing us to distinguish between the interesting primes and the trivial ones. We now prove a lemma which formalizes our discussion above and allows us to further focus our range of possible prime divisors of the coefficients A_j in $\mathscr{K}_n^{(\lambda,\mu)}(x)$.

Lemma 3.1.8. *Let p be a prime number. If $3n+\lambda < p < 6n+6+\epsilon$ or $p > 12n+\epsilon$, then $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ is trivial.*

Proof. Since the coefficients A_j of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ are integers we know that $\operatorname{ord}_p(A_j) \geq 0$ for all j and so it will be sufficient to show that $\operatorname{ord}_p(A_0) = \operatorname{ord}_p(A_n)$. From our discussion above, we know that if $p > 12n+\epsilon$ then p clearly does not divide α_j, β_j or $\binom{n}{j}$ for any $0 \leq j \leq n$. In this case, it follows that $\operatorname{ord}_p(A_0) = \operatorname{ord}_p(A_n)$ and so $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)})$ is therefore trivial.

Now suppose that $3n+\lambda < p < 6n+6+\epsilon$. Similar to the first case, it is evident that p does not divide α_j or $\binom{n}{j}$. It will therefore be sufficient to show that $\operatorname{ord}_p(\beta_0) = \operatorname{ord}_p(\beta_n)$. Since $\beta_0 = 1$, it is obvious that $\operatorname{ord}_p(\beta_0) = 0$. If $\operatorname{ord}_p(\beta_n) > 0$ then, from Lemma 3.1.6, there must an exist integer $0 \leq k < n$ such that $b_k = 6n+6+\epsilon+6k = mp$ for some $m \in \mathbf{N}$. Clearly m is not equal to 1 or 2 since $b_k > p$ for every k and every $b_k = 2(3n+3+\lambda+\mu-3k)+\mu$ is odd. If $m = 3$ then $b_k = 6n+6+\epsilon+6k \equiv 0 \mod 3$ which implies that $\epsilon = 2\lambda + 3\mu \equiv 0 \mod 3$ and thus that $2\lambda \equiv 0 \mod 3$, a contradiction. If $m = 4$ then $b_k = (4n+4-4k)+2n+2-2k+\epsilon \equiv 2(n+1+k)+\epsilon \mod 4 \equiv 0 \mod 4$ which is also a contradiction since $\epsilon = 2(\lambda+\mu)+\mu$ is always odd. Finally, if $m \geq 5$ then $p > 15n + 5\lambda$ and so p is greater than each term b_k (recall that

$\max\{b_k\} = 12n+\epsilon$) and so $p \nmid \beta_j$ for all $j \in [0,n]$. Thus $\mathrm{ord}_p(\beta_n) = 0 = \mathrm{ord}_p(\beta_0)$ and we see that $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)})$ at primes in the ranges $3n+\lambda < p < 6n+6+\epsilon$ or $p > 12n+\epsilon$ are trivial. □

Hence, all primes which yield nontrivial Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ must lie in the interval $[2, 3n+\lambda]$ or $[6n+\epsilon+6, 12n+\epsilon]$. As noted above, it is helpful to partition the first of these intervals since primes $p \le n$ may divide $\binom{n}{j}$ in addition to α_j and β_j and so determining $\mathrm{ord}_p(A_j)$ for such primes is a more delicate problem. We now aim to determine the shape of Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes in the ranges $[6n+\epsilon+6, 12n+\epsilon]$, $(n, 3n+\lambda]$ and some conjectured cases for primes $[2,n]$.

3.2 Primes in the Interval $[6n+6+\epsilon, 12n+\epsilon]$

In this section we determine the Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes in the interval $[6n+6+\epsilon, 12n+\epsilon]$. Note that for these primes, $\mathrm{ord}_p(\binom{n}{j}) = \mathrm{ord}_p(\alpha_j) = 0$ for all $j \in [0,n]$ since $p > 3n+\lambda > n$ (see Remark 3.1.7). We first prove a lemma showing that every nontrivial Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ occurs at a prime of the form $p = 6n+6+\epsilon+6k \in [6n+6+\epsilon, 12n+\epsilon]$ for some $k \in [0, n-1]$.

Lemma 3.2.1. *Fix n and let $p \in [6n+6+\epsilon, 12n+\epsilon]$ be a prime such that $p \ne 6n+6\epsilon+6k$ for any $k \in [0, n-1]$. Then $\mathrm{ord}_p(A_j) = 0$ for all $j \in [0,n]$.*

Proof. Suppose that p is not of the form $6n+6+\epsilon+6k$ and that $\mathrm{ord}_p(A_j) > 0$ for some $j \in [0,n]$. Since $\mathrm{ord}_p(A_j) = \mathrm{ord}_p(\beta_j)$ for all j due to the size of p (Remark 3.1.7), we know from Lemma 3.1.6 that there must exist some $m \in [0, j-1]$ such that $p \mid b_m$, where b_m is the mth term in the expansion of β_j. This means that $b_m = sp$ for some integer $s > 1$ (since

$p \neq b_m$ by hypothesis). Recalling that $p \in [6n+6+\epsilon, 12n+\epsilon]$, we obtain

$$\begin{aligned}
6n+6+\epsilon &\leq p \\
&= \frac{b_m}{s} \\
&= \frac{6n+6+\epsilon+6m}{s} \\
&\leq \frac{6n+6+\epsilon+6m}{2} \\
&= 3n+3+\epsilon/2+3m,
\end{aligned}$$

which implies that $6n+6+\epsilon \leq 3n+3+\epsilon/2+3m$ and therefore that $m \geq n+1+\epsilon/6$, which is a contradiction since the maximum value of m is $n-1$. It follows that if $p \in [6n+6+\epsilon, 12n+\epsilon]$ divides A_j then p is of the form $6n+6+\epsilon+6k$ for some $k \in [0, n-1]$. □

We now state some preliminary observations regarding primes $p = 6n+6+\epsilon+6k$. Note that primes of this form must appear in the expansion of β_n since

$$\beta_n = (6n+6+\epsilon)(6n+6+\epsilon+6\cdot 1)\cdots(6n+6+\epsilon+6k)\cdots(12n+\epsilon),$$

and therefore the p-adic valuation of the leading coefficient of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ (which is $A_n = \beta_n$) is at least 1 for such primes. Recalling that $6n+6+\epsilon+6k = b_k$ is the kth term in the expansion of β_j, we can also see that primes of the form $p = b_k$ must divide β_j for all $j \in [k+1, n]$. This can be seen by noting that, since $\beta_j = b_0 \cdots b_{j-1} = (6n+6+\epsilon)(6n+6+\epsilon+6\cdot 1)\cdots(6n+6+\epsilon+$

$6(j-1)$), we have

$$\begin{aligned}
\beta_0 &= 1\\
\beta_1 &= b_0\\
&\vdots\\
\beta_k &= b_0\cdots b_{k-1}\\
\beta_{k+1} &= b_0\cdots b_{k-1}\cdot p\\
\beta_{k+2} &= b_0\cdots b_{k-1}\cdot p\cdot b_{k-1}\\
&\vdots\\
\beta_{n-1} &= b_0\cdots b_{k-1}\cdot p\cdot b_{k-1}\cdots b_{n-2}\\
\beta_n &= b_0\cdots b_{k-1}\cdot p\cdot b_{k-1}\cdots b_{n-2}\cdot b_{n-1}.
\end{aligned}$$

Since p is greater than terms in both α_j and $\binom{n}{j}$, we see that the sum of the p-adic valuations of each term on the right hand side of the above equations will be the precise valuation of the jth coefficient A_j (for example, the valuation of $A_3 = \text{ord}_p(b_0)+\text{ord}_p(b_1)+\text{ord}_p(b_2)$). Given this, the above equations also suggest a plausible shape for Newton Polygons at primes $p = b_k$. Since the terms b_m in the expansion of β_j form an increasing sequence, we can see that $p = b_k$ does not divide any terms b_m for all $m < k$ since $p > b_m$ for each of these m values. Therefore, we see that a break must occur in $\texttt{NP}_{p=b_k}(\mathscr{K}_n^{(\lambda,\mu)}(x))$ at the point $(k, \text{ord}_p(A_k))$. These observations hint toward the following theorem, which we now prove.

Theorem 3.2.2. *Let p be a prime such that $p = b_k = 6n+6+\epsilon+6k$ for some $k \in [0,n)$. Then the vertices of the Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at p are*

$$(0,0),(k,0),(n,1).$$

In particular, the Newton Polygon at p consists of two segments with respective slopes 0 and $1/(n-k)$. (Note that if $k=0$ the middle vertex coincides with the outer left vertex resulting in a pure Newton Polygon with slope with $1/n$).

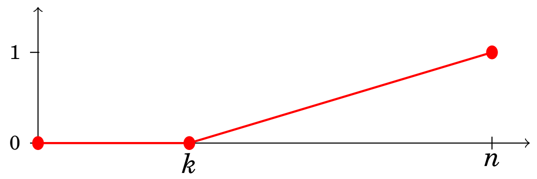


Figure 3.2.1: $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ described in Theorem 3.2.2.

Before proceeding with a proof of Theorem 3.2.2, observe that the described Newton Polygon shape will follow if we can show that

(a) $\operatorname{ord}_p(A_0) = 0$,

(b) $\operatorname{ord}_p(A_k) = 0$,

(c) $\operatorname{ord}_p(A_n) = 1$,

(d) $\operatorname{ord}_p(A_j) \geq 0$, for all $j \in (0,k)$, and that

(e) $\operatorname{ord}_p(A_j) \geq 1$, for all $j \in (k,n)$.

Items (a), (b) and (c) above will show that the breaks of the Newton Polygon are in the correct positions. Items (d) and (e) will show that every term in between the breaks has a higher divisibility by p than terms at the breaks, and therefore that the lower convex hull of the points $(j, \operatorname{ord}_p(A_j))$ is described by the edges connecting each indicated break. We now proceed with the proof of Theorem 3.2.2.

Proof of Theorem 3.2.2. Fix n and some choice of $\lambda, \mu \in \{\pm 1\}$, and suppose that there exists some $k \in [0,n)$ such that $p = b_k = 6n + 6 + \epsilon + 6k$ is prime. We prove statements (a) through (e) as listed above to obtain the result. Lemma 3.1.5 and Remark 3.1.7 state that $\operatorname{ord}_p(\binom{n}{j}) = \operatorname{ord}_p(\alpha_j) = 0$ for all j and so we omit discussion of these terms in our cases below.

(a). We have that $\operatorname{ord}_p(A_0) = \operatorname{ord}_p(\alpha_0) = 0$ from Remark 3.1.7.

(b). We show that $\operatorname{ord}_p(A_k) = 0$. Since $\operatorname{ord}_p(A_k) = \operatorname{ord}_p(\beta_k)$ and $\beta_k = b_0 \cdots b_{k-1}$, we see that every term in β_k is less than $p = b_k = 6n + 6 + \epsilon + 6k$ and therefore that $\operatorname{ord}_p(A_k) = 0$.

(c). We show that $\operatorname{ord}_p(A_n) = 1$. Since $p = b_k$ we know that $\beta_n = b_0 \cdots b_k \cdots b_{n-1} = b_0 \cdots p \cdots b_{n-1}$ and therefore $\operatorname{ord}_p(\beta_n) \geq 1$. If $\operatorname{ord}_p \beta_n > 1$ then it must be the case that $\beta_n = b_0 \cdots p \cdots mp \cdots b_{n-1}$, for some integer $m > 1$ since the terms in the expansion of β_n form an increasing sequence. If $m = 2$ consider that

$$\begin{aligned} 2p &= 2b_k \\ &= 2(6n + 6 + \epsilon + 6k) \\ &= 12(n + k + 1) + 2\epsilon) \\ &> 12n + \epsilon \\ &= b_{n-1}, \end{aligned}$$

which is a contradiction. It is clear that any multiple of p greater than $2p$ will also yield a similar contradiction. Thus $\operatorname{ord}_p(A_n) = \operatorname{ord}_p(\beta_n) = 1$.

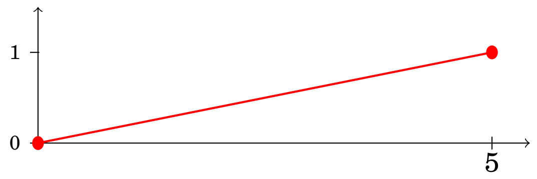
(d). We now show that $\operatorname{ord}_p(A_j) \geq 0$ for all $j \in (0, k)$. Since $\operatorname{ord}_p(A_j) = \operatorname{ord}_p(\beta_j) = b_0 \cdots b_{j-1}$ we see that each term in this product will be less than $p = b_k$ and therefore that $\operatorname{ord}_p(A_j) \geq 0$ for every $j \in (0, k)$.

(e). We conclude by showing that $\operatorname{ord}_p(A_j) \geq 1$ for all $j \in (k, n)$. Since $\operatorname{ord}_p(A_j) = \operatorname{ord}_p(\beta_j) = b_0 \cdots b_k \cdots b_{j-1} = b_0 \cdots p \cdots b_{j-1}$ we know that $\operatorname{ord}_p(A_j) \geq 1$. (Though not necessary, it follows from the discussion in part (c) of this proof that $\operatorname{ord}_p(A_j) = 1$ for all $j \in (k, n)$). □

Example 3.2.3. Let $n = 5$ and $\lambda = \mu = 1$. Observe that $b_0 = 6 \cdot 5 + 5 + 6 + 6 \cdot 0 = 41$ is a prime. Theorem 3.2.2 allows us to conclude that the Newton Polygon for the polynomial

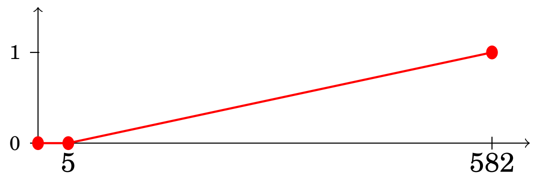
$$\mathcal{K}_5^{(1,1)}(x) = 391672385x^5 + 482058320x^4 + 212432480x^3 + 40081600x^2 + 2984800x + 58240$$

at the prime 41 has the following shape.



This Newton Polygon is pure and so $\mathscr{K}_5^{(1,1)}(x)$ is irreducible over $\mathbf{Q}_{41}$ and thus over $\mathbf{Q}$ by Theorem 2.4.9. ♢

Example 3.2.4. We now consider a higher degree polynomial. Let $n = 582$ and let $\lambda = -1$ and $\mu = 1$. (To grasp the magnitude of this polynomial, a computation in Pari/GP shows that the coefficient A_{582} is in the vicinity of 10^{2159}. Printing the entire polynomial would require over 400 pages of single-spaced text in size 12 font!). Observe that $b_5 = 6 \cdot 582 + 1 + 6 + 6 \cdot 5 = 3529$ is prime. By Theorem 3.2.2 we find that $\mathtt{NP}_{3529}(\mathscr{K}_{582}^{(-1,1)})$ has the following shape.



The slope of the nonzero segment of this polygon is $1/(n-k) = 1/577$. Therefore, 577 divides the Newton Index $\mathscr{N}_{\mathscr{K}_{582}^{(-1,1)}}$ which in turn divides the order of $\mathrm{Gal}(\mathscr{K}_{582}^{(-1,1)})$ over $\mathbf{Q}$ (see Theorem 2.4.12). Furthermore, since 577 is a prime in the interval $(n/2, n-2) = (291, 580)$, if we assume a priori that $\mathscr{K}_{582}^{(-1,1)}$ is irreducible, we may also conclude using Theorem 2.4.12 that $\mathrm{Gal}(\mathscr{K}_{582}^{(-1,1)}) \simeq S_{582}$.

In order to show irreducibility, it is enough to note that $b_0 = 6 \cdot 582 + 1 + 6 = 3499$ is also a prime and therefore that $\mathtt{NP}_{3499}(\mathscr{K}_{582}^{(-1,1)})$ is pure. Thus $\mathscr{K}_{582}^{(-1,1)}(x)$ is irreducible over $\mathbf{Q}$ by and has Galois group S_{582}.

Furthermore, we note that $\mathscr{K}_{582}^{(-1,1)}$ is a lift of the supersingular polynomial $\mathfrak{s}_{6991}(x)$. This can be seen from Theorem 2.6.3 since $n = 582 = (6991-7)/12$ where 7 is the residue of 6991 modulo 12, implying that $\lambda = -1$ and $\mu = 1$ as desired (by the criterion outlined by Brillhart and Morton in Theorem 2.6.3). $\diamondsuit$

The above two examples allow us to see how Theorem 3.2.2 can be used to determine irreducibility and Galois properties of $\mathscr{K}_n^{(\lambda,\mu)}(x)$. In particular, Theorem 3.2.2 allows us to clearly see that the Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes of the form $p = 6n + \epsilon + 6$ will be pure and therefore that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible over $\mathbf{Q}$ for these particular n values. Furthermore, the conclusion that $\mathrm{Gal}(\mathscr{K}_{582}^{(-1,1)}) \simeq S_{582}$ reached in Example 3.2.4 relied on the fact that we were able to find three primes of a certain type. The first two primes, of the form $p = 6n+\epsilon+6k$ (used to define the Newton Polygon) and $q = n-k$ (a denominator of the slope of the nonzero segment), were used *together* to conclude that the Galois group of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ was S_n. The third prime (of the form $\ell = 6n+\epsilon+6$) was used only to conclude irreducibility. This example hints toward a relationship between primes of the form $6n+\epsilon+6k$ and $n-k$ and the Galois group of $\mathscr{K}_n^{(\lambda,\mu)}(x)$; we explore this connection more thoroughly in Section 5.2.

3.3 Primes in the Interval $(n, 3n+\lambda]$

We now aim to describe the Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at primes in the interval $(n, 3n+\lambda]$. Unlike Section 3.2, the primes $p \in (n, 3n+\lambda]$ which divide A_j may also divide both $\mathrm{ord}_p(\alpha_j)$ and $\mathrm{ord}_p(\beta_j)$ (though we still have that $\mathrm{ord}_p(\binom{n}{j}) = 0$ for all $j \in [0,n]$ since $p > n$). We focus on describing the Newton Polygons for primes of the form $p = 3n+\lambda-3k$.

Similarly to Section 3.2, we observe that if p is a prime of the form $p = 3n+\lambda-3k$ then p must appear in the expansion α_0 since

$$\alpha_0 = (3n+\lambda)(3n+\lambda-3\cdot 1)\cdots(3n+\lambda-3k)\cdots(\lambda+3),$$

and therefore $\mathrm{ord}_p(A_0) = \mathrm{ord}_p(\alpha_0) \geq 1$ for these primes. Furthermore, since $3n+\lambda-3k = a_k$ is the kth term in the expansion of α_j, we can also see that primes of the form $p = a_k$ must divide α_j for all $j \in [0, n-k)$. Recalling that $\alpha_j = a_0 \cdots a_{n-j-1} = (3n+\lambda)(3n+\lambda-3\cdot 1)\cdots(3n+$

$\lambda - 3(n-j-1))$, we can see this by noting that

$$\begin{aligned}
\alpha_0 &= a_0 \cdots a_{k-1} \cdot p \cdot a_{k+1} \cdots a_{n-1} \\
\alpha_1 &= a_0 \cdots a_{k-1} \cdot p \cdot a_{k+1} \cdots a_{n-2} \\
&\vdots \\
\alpha_{n-k-2} &= a_0 \cdots a_{k-1} \cdot p \cdot a_{k+1} \\
\alpha_{n-k-1} &= a_0 \cdots a_{k-1} \cdot p \\
\alpha_{n-k} &= a_0 \cdots a_{k-1} \\
&\vdots \\
\alpha_{n-1} &= a_0 \\
\alpha_n &= 1.
\end{aligned}$$

The above equations allow us to conclude that if $p = 3n + \lambda - 3k$ for some $k \in [0, n-1]$ then $\mathrm{ord}_p(A_j) = \mathrm{ord}_p(\alpha_j) + \mathrm{ord}_p(\beta_j) \geq 1$ for all $j \in [0, n-k)$. In order to refine this inequality, we seek criterion for determining when a prime of the form $p = a_k$ divides β_j. That is, we wish to know how the value $\mathrm{ord}_{p=3n+\lambda-3k}(\beta_j)$ changes as j runs through $\{0, \ldots, n\}$. This question is answered in the following lemma.

Lemma 3.3.1. *Fix n and suppose that there exists a prime $p = a_k = 3n + \lambda - 3k \in (n, 3n+\lambda]$. Let $k' = (-k - 1 - \mu/2) \mod p$. If $k' \in [0, n)$ then $\mathrm{ord}_p(\beta_j) = 0$ for all $j \in [0, k']$ and $\mathrm{ord}_p(\beta_j) = 1$ for all $j \in (k', n]$. Furthermore, if $k' \in [n, p)$ then $\mathrm{ord}_p(\beta_j) = 0$ for all $j \in [0, n]$.*

Proof. There are two cases. First, suppose that $k' = ((-k - 1 - \mu/2) \bmod p) \in [0, n)$. Then

$$k + 1 + \mu/2 + k' \equiv 0 \bmod p$$

and

$$3k \equiv 3n + \lambda \mod p$$

because $p = 3n + \lambda - 3k \equiv 0 \bmod p$. Using these facts, we obtain

$$\begin{aligned} 0 &\equiv k + 1 + \mu/2 + k' \bmod p \\ &\equiv 6k + 6 + 3\mu + 6k' \bmod p \\ &\equiv (3k) + (3k) + 6 + 3\mu + 6k' \bmod p \\ &\equiv (3n+\lambda) + (3n+\lambda) + 6 + 3\mu + 6k' \bmod p \\ &\equiv 6n + 6 + (2\lambda + 3\mu) + 6k' \bmod p \\ &\equiv 6n + 6 + \epsilon + 6k' \bmod p \\ &\equiv b_{k'} \bmod p. \end{aligned}$$

The above congruences show that the term $b_{k'}$ in the expansion of β_j is divisible by p. Furthermore, since k' is unique (it is just the value $(-k-1-\mu/2) \in \mathbf{Z}/p\mathbf{Z}$), it follows that $b_{k'}$ is the *only* term appearing in β_j which is divisible by p. This can be seen explicitly by supposing we had another term $b_{k''}$ (for some $k'' \in [0,n), k'' \neq k'$) in β_j such that $p \mid b_{k''}$. The above congruences tell us that $k'' \equiv (-k-1-\mu/2) \bmod p$ (this is seen by following the congruences above bottom-to-top, replacing k' with k''). Since $k'' \neq k'$ it must be the case that $k'' = sp + k'$ for some integer $s > 0$ (i.e., k'' is an integer lift of k') in order to have the same reduction modulo p. Then

$$\begin{aligned} b_{k''} &= b_{sp+k'} \\ &= 6n + 6 + \epsilon + 6(sp + k') \\ &\geq 6n + 6 + \epsilon + 6(p + k') \quad \text{(since } s \geq 1) \\ &\geq 6n + 6 + \epsilon + 6p \qquad \text{(since } k' \geq 0) \\ &> 6n + 6 + \epsilon + 6n \qquad \text{(since } p > n) \\ &= 12n + 6 + \epsilon. \end{aligned}$$

Thus $b_{k''} > 12n+6+\epsilon$, which contradicts the fact that the maximum value of b_m is $12n+\epsilon$. Hence $b_{k'}$ is the only term in β_j which is divisible by p. Now consider that $\beta_{k'+1} = b_0 b_1 \cdots b_{k'}$ and so $\beta_j = b_0 \cdots b_{k'} \cdots b_{j-1}$ whenever $j > k'$. It follows that $\operatorname{ord}_p(\beta_j) = 1$ for all $j \in (k', n]$.

Still under the hypothesis that $k' \in [0,n)$, we see that $\beta_{k'} = b_0 b_1 \cdots b_{k'-1}$ and thus that whenever $j \leq k'$ there is no $b_{k'}$ term in the product β_j. It follows (from both the uniqueness of k' and the fact that the terms b_m form an increasing sequence) that if $j \leq k'$ then there is no term in β_j which is divisible by p. Therefore $\operatorname{ord}_p(\beta_j) = 0$ for all $j \in [0, k']$.

If we now suppose that $k' \in [n,p)$, we see that $\beta_{k'} = b_0 b_1 \cdots b_{n-1} b_n \cdots b_{k'-1} \geq \beta_n$. But clearly β_n is the largest possible value of β_j since n is the degree of the polynomial and thus it does not make sense to consider values $\beta_{k'}$ which are strictly greater than β_n (in this case, the unique term $b_{k'}$ which is divisible by p would always appear *after* the term $b_{n-1} = \max\{b_m\}$ in the expansion of β_j). It follows from the uniqueness of k' that there is no term in the product β_n which is divisible by p and therefore that if $k' \in [n,p)$ then $\operatorname{ord}_p(\beta_j) = 0$ for every $j \in [0,n]$. □

We are now able to describe the shape of $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ at primes of the form $3n+\lambda-3k$ in the interval $(n, 3n+\lambda]$.

Theorem 3.3.2. *Fix n and suppose that there exists a prime* $p = a_k = 3n+\lambda-3k \in (n, 3n+\lambda]$. *Let* $k' = (-k-1-\mu/2) \mod p$.

(1). *If* $k' \in [n,p)$ *then the vertices of the Newton Polygon for* $\mathscr{K}_n^{(\lambda,\mu)}(x)$ *at p are*

$$(0,1), (n-k, 0), (n, 0).$$

In particular, the Newton Polygon consists of 2 segments with slopes $-1/(n-k)$ *and* 0. *Note that when* $k = 0$ *the middle vertex coincides with the end point yielding a pure Newton Polygon with slope* $-1/n$.

(2). *If* $k' \in [n-k, n)$ *then the vertices of the Newton Polygon for* $\mathscr{K}_n^{(\lambda,\mu)}(x)$ *at* p *are*

$$(0,1), (n-k, 0), (k', 0), (n, 1).$$

In particular, the Newton Polygon consists of 3 segments with slopes $-1/(n-k)$*,* 0 *and* $1/(n-k')$*, respectively. Note that when* $k' = n-k$ *the middle vertices coincide yielding a Newton Polygon with 2 segments and slopes* $-1/(n-k)$ *and* $1/k$*.*

(3). *If* $k' \in [0, n-k)$ *then the Newton Polygon for* $\mathscr{K}_n^{(\lambda,\mu)}(x)$ *at* p *is trivial.*

Figures 3.3.1, 3.3.2, 3.3.3, 3.3.4 and 3.3.5 below illustrate the different Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ given by Theorem 3.3.2.

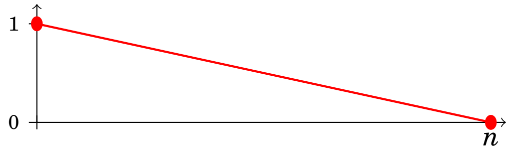


Figure 3.3.1: $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ when $k' \in [n, p)$ and $p = 3n + \lambda$.

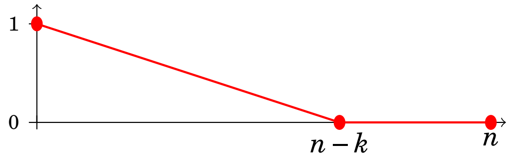


Figure 3.3.2: $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ when $k' \in [n, p)$ and $p = 3n + \lambda - 3k$ $(k \neq 0)$.

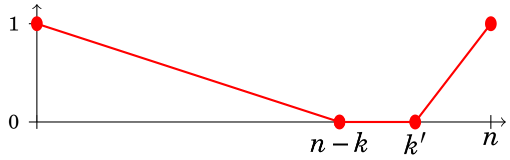


Figure 3.3.3: $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ when $k' \in (n-k, n)$ and $k' \neq n-k$.

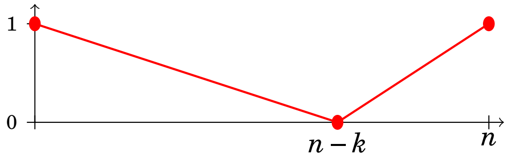


Figure 3.3.4: $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ when $k' \in (n-k,n)$ and $k' = n-k$.

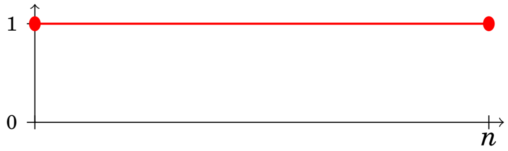


Figure 3.3.5: Trivial $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ when $k' \in [0,n-k)$.

Proof. We prove parts (1), (2) and (3) separately. Throughout the proof it may be helpful to recall that

$$\mathscr{K}_n^{(\lambda,\mu)}(x) = \sum_{j=0}^{n} \binom{n}{j} \underbrace{\prod_{k=0}^{n-j-1} (3n+\lambda-3k)}_{\alpha_j} \underbrace{\prod_{k=0}^{j-1} (6n+6+\epsilon+6k)}_{\beta_j} x^j,$$

where $\epsilon = 2\lambda + 3\mu$.

It is also helpful to remember that j refers to the index on α_j and β_j as being part of the product of the jth degree coefficient in $\mathscr{K}_n^{(\lambda,\mu)}(x)$ and that k or i will generally be used to index a term in the products α_j and β_j.

Proof of (1). Suppose that $k' \in [n,p)$. The described Newton Polygon shape will follow if we can show that

(1a) $\operatorname{ord}_p(A_0) = 1$,

(1b) $\operatorname{ord}_p(A_{n-k}) = 0$,

(1c) $\operatorname{ord}_p(A_n) = 0$,

(1d) $\operatorname{ord}_p(A_j) \geq 1$, for all $j \in (0,n-k)$, and that

(1e) $\operatorname{ord}_p(A_j) \geq 0$, for all $j \in [n-k,n)$.

Before we begin, note that since $k' \in [n,p)$, Lemma 3.3.1 tells us that $\mathrm{ord}_p(\beta_j) = 0$ for all $j \in [0,n]$ and we therefore omit discussion of this valuation while proving item (1).

(1a). Observe that $A_0 = \binom{n}{0}\alpha_0\beta_0 = \alpha_0 = a_0 \cdots a_k \cdots a_{n-1}$. Since $a_k = p$ we know that $p \mid A_0$ and thus that $\mathrm{ord}_p(A_0) \geq 1$. Clearly $p \nmid a_i$ for all $i \in [k+1,n)$ since each term $a_i < p$. If $p \mid a_i$ for some $i \in [0,k-1]$ then $3n + \lambda - 3i \equiv 0 \bmod p$. But since $3n + \lambda \equiv 3k \mod p$ we have that $3k - 3i \equiv 0 \bmod p$ and so $i \equiv k \bmod p$. Because $i,k \in [0,n-1] \subseteq \mathbf{Z}/p\mathbf{Z}$ the above congruence implies $i = k$, which contradicts our assumption that $i \neq k$. Thus $\mathrm{ord}_p(A_0) = 1$.

(1b). Observe that $\mathrm{ord}_p(A_{n-k}) = \mathrm{ord}_p(\binom{n}{k}\alpha_{n-k}\beta_{n-k}) = \mathrm{ord}_p(\alpha_{n-k})$. Since $\alpha_{n-k} = a_0 \cdots a_{k-1}$ and every term in this product is less than $a_k = p$, we see that $\mathrm{ord}_p(\alpha_{n-k}) = 0$ and thus that $\mathrm{ord}_p(A_{n-k}) = 0$.

(1c). It follows from Lemma 3.3.1 that $\mathrm{ord}_p(A_n) = \mathrm{ord}_p(\binom{n}{n}\alpha_n\beta_n) = \mathrm{ord}_p(\beta_n) = 0$.

(1d). Let $j \in (0,n-k)$ and observe that $\mathrm{ord}_p(A_j) = \mathrm{ord}_p(\binom{n}{j}\alpha_j\beta_j)\mathrm{ord}_p(\alpha_j)$. Since $\alpha_1 = a_0 \cdots a_k \cdots a_{n-2}$ and $\alpha_{n-k-1} = a_0 \cdots a_k$, we see that $p = a_k \mid \alpha_j$ for all $j \in (0,n-k)$ and thus $\mathrm{ord}_p(A_j) = \mathrm{ord}_p(\alpha_j) \geq 1$.

(1e). Let $j \in (n-k,n)$ and observe that $\mathrm{ord}_p(A_j) = \mathrm{ord}_p(\alpha_j)$. Since $\alpha_{n-k+1} = a_0 \cdots a_{k-2}$ and $\alpha_n = 1$, we know that $\alpha_j = a_0 \cdots a_i$ for some $i \in [0,k-1]$. It follows from the discussion in (1a) that $p \nmid a_i$ for all $i \in [0,k-2]$ and so $\mathrm{ord}_p(\alpha_j) = 0$ for all $j \in (n-k,n)$.

Proof of (2). Suppose that $k' \in (n-k, n)$. Following the method outlined above, we show that

$$\begin{aligned}
&(2a) \quad \operatorname{ord}_p(A_0) = 1,\\
&(2b) \quad \operatorname{ord}_p(A_{n-k}) = 0,\\
&(2c) \quad \operatorname{ord}_p(A_{k'}) = 0,\\
&(2d) \quad \operatorname{ord}_p(A_n) = 1,\\
&(2e) \quad \operatorname{ord}_p(A_j) \geq 1, \text{ for all } j \in (0, n-k),\\
&(2f) \quad \operatorname{ord}_p(A_j) \geq 0, \text{ for all } j \in (n-k, k'), \text{ and that}\\
&(2g) \quad \operatorname{ord}_p(A_j) \geq 1, \text{ for all } j \in (k', n).
\end{aligned}$$

$(2a)$. The fact that $\operatorname{ord}_p(A_0) = 1$ is independent of k' and has been shown in $(1a)$.

$(2b)$. Observe that $\operatorname{ord}_p(A_{n-k}) = \operatorname{ord}_p(\alpha_{n-k}) + \operatorname{ord}_p(\beta_{n-k})$. From $(1b)$ we have that $\operatorname{ord}_p(\alpha_{n-k}) = 0$. Lemma 3.3.1 states that $\operatorname{ord}_p(\beta_j) = 0$ for all j such that $0 \leq j \leq k'$. Letting $j = n-k$ we see that $\operatorname{ord}_p(\beta_{n-k}) = 0$ since $n-k < k'$.

$(2c)$. Observe that $\operatorname{ord}_p(A_{k'}) = \operatorname{ord}_p(\alpha_{k'}) + \operatorname{ord}_p(\beta_{k'})$. Consider that $\alpha_{\min\{k'\}} = \alpha_{n-k+1} = a_0 \cdots a_{k-2}$ and $\alpha_{\max\{k'\}} = \alpha_{n-1} = a_0$. This allows us to see that every term a_i (where $i \in [0, k-2]$) in the expansion of $\alpha_{k'}$ is strictly greater than $p = a_k$. It follows from the discussion in $(1a)$ that $p \nmid a_i$ for all $i \in [0, k-2]$ and so $\operatorname{ord}_p(\alpha_{k'}) = 0$. Lemma 3.3.1 implies that $\operatorname{ord}_p(\beta_{k'}) = 0$.

$(2d)$. Lemma 3.3.1 states that $\operatorname{ord}_p(\beta_j) = 1$ for all j such that $k' < j \leq n$. Letting $j = n$, since we see that $k' < n$ by hypothesis and it follows that $\operatorname{ord}(A_n) = \operatorname{ord}_p(\beta_n) = 1$.

$(2e)$. Let $j \in (0, n-k)$ and observe that $\operatorname{ord}_p(A_j) = \operatorname{ord}_p(\binom{n}{j}\alpha_j\beta_j) = \operatorname{ord}_p(\alpha_j) + \operatorname{ord}_p(\beta_j)$. It follows from the discussion in $(1d)$ that $\operatorname{ord}_p(\alpha_j) \geq 1$ and so $\operatorname{ord}_p(A_j) \geq 1$. (It actually follows from Lemma 3.3.1 that $\operatorname{ord}_p(A_j) = 1$ since $\operatorname{ord}_p(\beta_j) = 0$).

$(2f)$. Let $j \in (n-k, k')$ and observe that $\text{ord}_p(A_j) = \text{ord}_p(\alpha_j) + \text{ord}_p(\beta_j)$. We know from Lemma 3.3.1 that $\text{ord}_p(\beta_j) = 0$. Consider that $\alpha_{\max\{k'\}} = \alpha_{n-1} = a_0$ and $\alpha_{\min\{k'\}} = \alpha_{n-k+1} = a_0 \cdots a_{k-2}$ and therefore the terms in $\alpha_j = a_0 \cdots a_i$ for some $i \in [0, k-2]$. It follows from section $(1a)$ that $p \nmid a_i$ for all $i \in [0, k-2]$ and so $\text{ord}_p(\alpha_j) = 0$ for all $j \in (n-k, n)$.

$(2g)$. Let $j \in (k', n)$ and observe that $\text{ord}_p(A_j) = \text{ord}_p(\alpha_j) + \text{ord}_p(\beta_j)$. We know from Lemma 3.3.1 that $\text{ord}_p(\beta_j) = 1$ and thus $\text{ord}_p(A_j) \geq 1$.

Proof of (3). Suppose that $k' \in [0, n-k)$. In order to show that the lower convex hull of the set of ordered pairs $(j, \text{ord}_p(A_j))$ for $j \in [0, n]$ is a single line of slope zero, it will be sufficient to show that

$$(3a) \quad \text{ord}_p(A_0) = 1,$$

$$(3b) \quad \text{ord}_p(A_n) = 1, \text{ and that,}$$

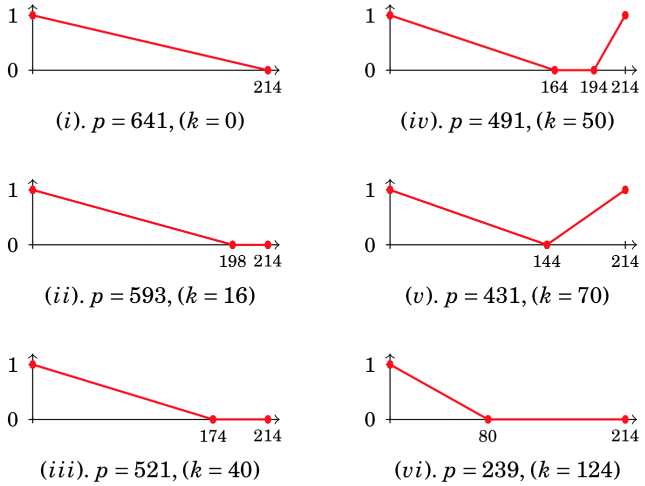
$$(3c) \quad \text{ord}_p(A_j) \geq 1, \text{ for all } j \in (0, n).$$

$(3a)$. This has been shown in $(1a)$.

$(3b)$. Since $k' \in [0, n-k)$, we see that $\text{ord}_p(A_n) = \text{ord}_p(\beta_n) = 1$ follows from Lemma 3.3.1.

$(3c)$. Observe that $\text{ord}_p(A_j) = \text{ord}_p(\alpha_j) + \text{ord}_p(\beta_j)$. We know from Lemma 3.3.1 that $\text{ord}_p(\beta_j) = 1$ for all $j \in (k', n]$. Since $p = a_k$ and $\alpha_j = a_0 \cdots a_k \cdots a_{n-j-1}$ for all $j \in [0, n-k-1] \supseteq [0, k']$, we see that $\text{ord}_p(\alpha_j) \geq 1$ for all $j \in [0, k']$. Thus $\text{ord}_p(A_j) \geq 1$ for all $j \in [0, n]$ and we are done. □

Example 3.3.3. The six Newton Polygons in shown below in Figure 3.3.6 illustrate how $\mathtt{NP}_p(\mathscr{K}_{208}^{(-1,1)}(x))$ varies for different primes of the form $p = 3 \cdot 214 - 1 - 3 \cdot k = 641 - 3k$. Each Newton Polygon is determined using Theorem 3.3.2.



(i). $p = 641, (k = 0)$

(iv). $p = 491, (k = 50)$

(ii). $p = 593, (k = 16)$

(v). $p = 431, (k = 70)$

(iii). $p = 521, (k = 40)$

(vi). $p = 239, (k = 124)$

Figure 3.3.6: Newton Polygons for $\mathscr{K}_{208}^{(-1,1)}(x)$ at various primes of the form $p = 641 - 3k$.

$\Diamond$

Note that the denominators $n-k$ of the Newton Polygons described in Theorem 3.3.2 are always divisible by 2 since $p - \lambda \equiv 0 \bmod 2$ in the numerator of $n - k = (p-\lambda)/3$.

A natural question to ask is whether Theorem 3.3.2 describes every $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ (as was the case in Section 3.2) at primes in the interval $(n, 3n+\lambda]$. Notice that each prime of the form $p = 3n + \lambda - 3k$ is congruent to λ mod 3. Thus, once a choice of λ is selected, Theorem 3.3.2 describes the Newton Polygons for primes of a single congruence class. We suspect that primes $q \in (n, 3n+\lambda]$ that are not of the same congruence class as p yield few Newton Polygons; computations in Pari/GP suggest that they only account for about 10% of the total number of nontrivial Newton Polygons at primes in the interval $(n, 3n+\lambda]$. Furthermore, the Newton Polygons at such primes q are 'barely' nontrivial in that, from the examples that we have computed, they each appear in a similar form to the Newton Polygon shown in Figure 3.3.7 below.

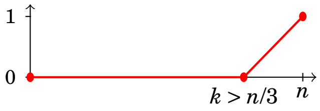


Figure 3.3.7

4
Irreducibility Results

4.1 Pure Newton Polygons

We have seen in Examples 3.2.3 and 3.2.4 that special cases of Theorems 3.2.2 and 3.3.2 yield pure Newton Polygons. As noted in both of those Theorems, the primes for which $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ is pure are of the form $p = 6n+6+\epsilon = 6n+6+2\lambda+3\mu$ and $p = 3n+\lambda$. Solving these equations for n in terms of p allows us to see several infinite classes of degrees for which $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible. We note that Corollary 4.1.1 below gives a new case of irreducibility for $\mathscr{K}_n^{(\lambda,\mu)}(x)$. The reformulation of these results in Remark 4.1.4(i) of this section therefore yields new irreducibility results for lifts of the supersingular polynomials. Furthermore, Corollary 4.1.1 below recovers several cases of irreducibility found by Mahlburg and Ono in [18], where they used a different interpretation of the $\mathscr{K}_n^{(\lambda,\mu)}(x)$ polynomials (as hypergeometric series, rather than Jacobi polynomials) and proved Eisenstein properties explicitly. We state these results as corollaries since they follow directly from the Newton Polygon arguments made in Theorems 3.2.2 and 3.3.2.

Corollary 4.1.1. *Let p be an odd prime. If $n = \frac{p-\lambda}{3}$, where $\lambda \in \{\pm 1\}$ is chosen with the same sign as $p \equiv \lambda \bmod 3 \equiv \pm 1 \bmod 3$, then $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible over $\mathbf{Q}$.*

Proof. If $n = \frac{p-\lambda}{3}$ then $p = 3n + \lambda = a_0$ is the first term in the product α_0 and irreducibility follows from Theorem 3.3.2 (1). □

Corollary 4.1.2. *Let p be an odd prime. If $p \geq 12 + 2\lambda + 3\mu$ and $n = \frac{p-6-2\lambda-3\mu}{6}$, where λ and μ are chosen according to $p \equiv 2\lambda + 3\mu \bmod 6 \equiv \pm 1 \bmod 6$, then $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible over* $\mathbf{Q}$.

Proof. Requiring $p \geq 12 + 2\lambda + 3\mu$ and fixing λ and μ by the reduction $p \equiv 2\lambda + 3\mu \bmod 6$ ensures that n is always an integer. We know that $p = 6n + 6 + \epsilon = b_0$ is the first term in the product β_0 and irreducibility follows directly from Theorem 3.2.2 since $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ is pure. □

It is important to notice that because $n = \frac{p-6-2\lambda-3\mu}{6}$ depends on both λ and μ, we can conclude only one irreducible specialization (i.e., one choice of $(\lambda,\mu) \in \{\pm 1\} \times \{\pm 1\}$) for each degree $n = \frac{p-6-2\lambda-3\mu}{6}$ of $\mathscr{K}_n^{(\lambda,\mu)}(x)$. This is different from the case in Corollary 4.1.1 where n depends only on λ, allowing us to conclude two irreducible specializations (corresponding to $\mu = 1$ and $\mu = -1$) for each degree $n = \frac{p-\lambda}{3}$. We therefore find that any odd prime p yields the following irreducible degrees and specializations of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ (remembering that $p \geq 12 + 2\lambda + 3\mu$ when the denominator of n is 6).

- If $p \equiv 1 \bmod 3$ then $\mathscr{K}_{\frac{p-1}{3}}^{(1,\mu)}(x)$, $\mathscr{K}_{\frac{p-7}{6}}^{(1,1)}(x)$ and $\mathscr{K}_{\frac{p-1}{6}}^{(1,-1)}(x)$ are irreducible.
- If $p \equiv -1 \bmod 3$ then $\mathscr{K}_{\frac{p+1}{3}}^{(-1,\mu)}(x)$, $\mathscr{K}_{\frac{p-11}{6}}^{(-1,-1)}(x)$ and $\mathscr{K}_{\frac{p-5}{6}}^{(-1,1)}(x)$ are irreducible.

Example 4.1.3. Let $p = 31$. From Corollary 4.1.1 we know that $\mathscr{K}_{10}^{(1,1)}(x)$ and $\mathscr{K}_{10}^{(1,-1)}(x)$ are irreducible since $31 \equiv 1 \bmod 3$ and $10 = (31-1)/3$. From Corollary 4.1.2 we can also see that $\mathscr{K}_{5}^{(-1,-1)}(x)$ and $\mathscr{K}_{4}^{(-1,1)}(x)$ are both irreducible since $31 \equiv 2(-1) + 3(-1) \bmod 6 = 2(-1) + 3(1) \bmod 6$. ◊

We relate these irreducibility results back to the supersingular polynomials in the following way. Let $q \equiv \varepsilon_q \bmod 12$ be a prime (so $\varepsilon_q = 1, 5, 7, 11$). Recall from Remark 2.6.5 that

$\mathscr{K}_n^{(\lambda,\mu)}(-x/3456)$ is a supersingular lift of $\mathfrak{s}_q(x)$ whenever $n=(q-\varepsilon_q)/12$ and

$$(\lambda,\mu)=\begin{cases}(-1,-1) & \text{if } \varepsilon_q=1,\\ (1,-1) & \text{if } \varepsilon_q=5,\\ (-1,1) & \text{if } \varepsilon_q=7,\\ (1,1) & \text{if } \varepsilon_q=11.\end{cases}$$

Therefore, if we fix q and find another prime p_1 which reduces to λ modulo 3 (where λ is fixed according to the value of ε_q above) which satisfies $(p_1-\lambda)/3=(q-\varepsilon_q)/12=n$, then it follows from Corollary 4.1.1 that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible and therefore that $\mathscr{K}_n^{(\lambda,\mu)}(-x/3456)\equiv \mathfrak{s}_q(x) \bmod q$ is irreducible. Note that the polynomial $\mathscr{K}_n^{(\lambda,\mu)}(-x/3456)$ would be irreducible for either choice of $\mu=\pm1$ but that $\mathscr{K}_n^{(\lambda,\mu)}(-x/3456)$ will only reduce to $\mathfrak{s}_q(x)$ modulo q when μ is fixed according to the value of ε_q. Hence, if there exists a prime $p_1\equiv\lambda \bmod 3$ such that $\varepsilon_q-4\lambda=q-4p_1$ then $\mathscr{K}_n^{(\lambda,\mu)}(-x/3456)$ is an irreducible lift of $\mathfrak{s}_q(x)$.

Corollary 4.1.2 can similarly be used to deduce cases where $\mathscr{K}_n^{(\lambda,\mu)}(-x/3456)$ is both irreducible and reduces to $\mathfrak{s}_q(x)$ modulo q. If we fix $q\equiv\varepsilon_q \bmod 12$ and find a prime $p_2\equiv 2\lambda+3\mu \bmod 6$ which satisfies $\frac{p_2-6-2\lambda-3\mu}{6}=(q-\varepsilon_q)/12=n$ then it follows from Corollary 4.1.2 that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is an irreducible lift of $\mathfrak{s}_q(x)$. We collect these observations in the following corollary.

Corollary 4.1.4. *Fix some prime* $q\equiv\varepsilon_q \bmod 12$*, where* $\varepsilon_q=1,5,7,11$*, and let*

$$(\lambda,\mu)=\begin{cases}(-1,-1) & \textit{if } \varepsilon_q=1,\\ (1,-1) & \textit{if } \varepsilon_q=5,\\ (-1,1) & \textit{if } \varepsilon_q=7,\\ (1,1) & \textit{if } \varepsilon_q=11.\end{cases}$$

(i) *Suppose there exists a prime* $p\equiv\lambda \bmod 3$ *satisfying*

$$q-4p=\varepsilon_q-4\lambda.$$

Then $\mathscr{K}_{\frac{p-\lambda}{3}}^{(\lambda,\mu)}(-x/3456)$ *is irreducible and* $\mathscr{K}_{\frac{p-\lambda}{3}}^{(\lambda,\mu)}(-x/3456)\equiv\mathfrak{s}_q(x) \bmod q$.

(ii) *Suppose there exists a prime* $p\equiv 2\lambda+3\mu \bmod 6$ *satisfying*

$$q-2p=\varepsilon_q-12-4\lambda-6\mu.$$

Then $\mathscr{K}^{(\lambda,\mu)}_{\frac{p-6-2\lambda-3\mu}{6}}(-x/3456)$ *is irreducible and* $\mathscr{K}^{(\lambda,\mu)}_{\frac{p-6-2\lambda-3\mu}{6}}(-x/3456) \equiv \mathfrak{s}_q(x) \bmod q$.

Example 4.1.5. In further continuation of Examples 2.5.9 and 2.6.6, we consider the prime $q = 37$. Since $37 \equiv 1 \bmod 12$ we choose the specialization $(\lambda,\mu) = (-1,-1)$ and $n = (37-1)/2$ for the lift $\mathscr{K}^{(-1,-1)}_3(-x/3456)$ of $\mathfrak{s}_{37}(x)$. In order to conclude that this lift is irreducible, we seek a prime p such that either

- $p \equiv \lambda \bmod 3$ and $\varepsilon_{37} - 4\lambda = 37 - 4p$, or
- $p \equiv 2\lambda + 3\mu \bmod 6$ and $\varepsilon_{37} - 12 - 4\lambda - 6\mu = q - 2p$.

There is no prime which satisfies the first item since substituting $(\lambda,\mu) = (-1,-1)$ into $\varepsilon_{37} - 4\lambda = 37 - 4p$ implies that $p = 8$. Considering the second item in a similar way allows us to see that $p = 19$ works since $19 \equiv 2(-1) + 3(-1) \bmod 6$ and satisfies $\varepsilon_{37} - 12 - 4\lambda - 6\mu = -1 = 37 - 2 \cdot 19 = q - 2p$. Hence

$$\mathscr{K}^{(-1,-1)}_3(-x/3456) = 80 - \frac{95}{144}x + 475497664x^2 - \frac{14725}{41278242816}x^3$$

is irreducible over $\mathbf{Q}$ (because $\mathtt{NP}_{19}(\mathscr{K}^{(-1,-1)}_3(x))$ is pure) and reduces to $\mathfrak{s}_{37}(x)$ modulo 37.

◊

We now discuss how often the properties of $\mathtt{NP}_p(\mathscr{K}^{(\lambda,\mu)}_n(x))$ stated in Corollaries 4.1.1 and 4.1.2 can be applied to conclude that $\mathscr{K}^{(\lambda,\mu)}_n(x)$ is an irreducible lift of a supersingular polynomial. In other words, we consider the number of primes q less than some integer k for which the lift of $\mathfrak{s}_q(x)$ is irreducible. We proceed by comPari/GPng the value of the prime counting function $\pi(k)$ to the total number of primes p which satisfy either of the criterion stated in Remark 4.1.4 for some fixed prime q. In order to do this, fix some $k \in \mathbf{N}$ and consider the sets $C_{\varepsilon_q}(k)$ (one for each of the four values of ε_q) which we define to be

$$\{\text{primes } q \equiv \varepsilon_q \bmod 12 < k : \exists p \equiv \lambda \bmod 3 \text{ satisfying } \varepsilon_q - 4\lambda = q - 4p \text{ or } \exists p \equiv 2\lambda + 3\mu \bmod 6 \text{ satisfying } \varepsilon_q - 12 - 4\lambda - 6\mu = q - 2p\},$$

For the reader's convenience, we write $C_{\varepsilon_q}(k)$ explicitly for each $\varepsilon_q = 1,5,7,11$:

$$\begin{aligned}
C_1(k) &= \{q \equiv 1 \bmod 12 < k : \exists p \equiv -1 \bmod 3 \text{ satisfying } 5 = q-4p \text{ or } \exists p \equiv 1 \bmod 3 \text{ satisfying } -1 = q-2p\} \\
C_5(k) &= \{q \equiv 5 \bmod 12 < k : \exists p \equiv 1 \bmod 3 \text{ satisfying } 1 = q-4p \text{ or } \exists p \equiv -1 \bmod 3 \text{ satisfying } -5 = q-2p\} \\
C_7(k) &= \{q \equiv 7 \bmod 12 < k : \exists p \equiv -1 \bmod 3 \text{ satisfying } 11 = q-4p \text{ or } \exists p \equiv 1 \bmod 3 \text{ satisfying } -7 = q-2p\} \\
C_{11}(k) &= \{q \equiv 11 \bmod 12 < k : \exists p \equiv 1 \bmod 3 \text{ satisfying } 7 = q-4p \text{ or } \exists p \equiv -1 \bmod 3 \text{ satisfying } -11 = q-2p\}
\end{aligned}$$

Note that we have replaced the congruence $2\lambda + 3\mu \bmod 6$ (as stated above in the definition of $C_{\varepsilon_q}(k)$) with $-\lambda \bmod 3$ since for any choice of λ, μ we obtain $2\lambda + 3\mu \bmod 6 \equiv 2\lambda \bmod 3 \equiv -\lambda \bmod 3$. Thus the value of μ is seen to be relevant only when specializing a lift of $\mathfrak{s}_q(x)$.

Example 4.1.6. We compute $C_1(20)$ and $C_1(100)$. The only prime $q < 20$ congruent to 1 modulo 12 is $q = 13$. Observe that $p = 7 \equiv 1 \bmod 3$ satisfies $-1 = 13 - 2 \cdot 7 = q - 2p$ and therefore $C_1(20) = \{13\}$.

The primes $q < 100$ ($q \equiv 1 \bmod 12$) are 13, 37, 61, 73 and 97 and so $|C_1(100)| \leq 5$. For the primes 13, 37, 61 and 73, observe that $p = 7$, 19, 31 and 37 (all $\equiv 1 \bmod 3$) each respectively satisfy $-1 = q - 2p$ and so $13, 37, 61, 73 \in C_1(100)$. We also see that $97 \in C_1(100)$ since $p = 23 \equiv -1 \bmod 3$ satisfies $5 = q - 4p$. Hence $C_1(100) = \{13, 37, 61, 73, 97\}$ and each $\mathfrak{s}_{q \in C_1(100)}(x)$ can be lifted to the irreducible polynomial $\mathscr{K}^{(-1,-1)}_{(q-1)/12}(-x/3456)$. (Notice that we could also have used $p = 17 \equiv -1 \bmod 3$ to show that $73 \in C_1(100)$ because $5 = 73 - 4 \cdot 17 = q - 4p$). $\Diamond$

Observe that the sum of the orders of C_1, C_5, C_7 and C_{11} will give the total number of primes q less than some integer k for which the lift of $\mathfrak{s}_q(x)$ is irreducible. We therefore compare the order of the set

$$C(k) = \bigcup_{\varepsilon_q} C_{\varepsilon_q}(k),$$

(where this union is taken over all $\varepsilon_q = 1,5,7,11$) to $\pi(k)$. We present some data in the table below which captures the growth of $|C_{\varepsilon_q}(k)|$.

k	$\pi(k)$	$\lvert C(k)\rvert$	$\lvert C_1(k)\rvert$	$\lvert C_5(k)\rvert$	$\lvert C_7(k)\rvert$	$\lvert C_{11}(k)\rvert$
100	25	22	5	6	5	6
1 000	168	121	27	34	32	28
10 000	1 229	691	162	183	174	172
100 000	9 592	4 233	1 014	1 121	1 075	1 023
1 000 000	78 498	28 409	6 708	7 459	7 194	7 048

Figure 4.1.1: $\pi(k)$ compared to the number of primes $q < k$ for which the lift of $\mathfrak{s}_q(x)$ is irreducible.

This table shows the number of primes for which Corollaries 4.1.1 and 4.1.2 can be used to conclude that $\mathcal{K}_n^{(\lambda,\mu)}(x)$ is an irreducible lift of a supersingular polynomial. The last entry states that about 36% of supersingular polynomials at primes $q < 1000000$ have an irreducible lift $\mathcal{K}_n^{(\lambda,\mu)}(x)$. We expect that a conjecture of Hardy and Littlewood in [15] can be used to estimate the growth of $|C(k)|$.

We now state the necessary conditions for $\mathcal{K}_n^{(\lambda,\mu)}(x)$ to be irreducible (using Corollaries 4.1.1 and 4.1.2) at every specialization of (λ,μ).

Remark 4.1.7. If there exists two primes of the form $p_1 = 3n+1$ and $p_2 = 3n-1$ then $\mathcal{K}_n^{(\lambda,\mu)}(x)$ is irreducible for every specialization $\lambda,\mu \in \{\pm 1\}$. ◊

Remark 4.1.8. If there exists four primes of the form $q_1 = 6n+1$, $q_2 = 6n+5$, $q_3 = 6n+7$ and $q_4 = 6n+11$ then $\mathcal{K}_n^{(\lambda,\mu)}(x)$ is irreducible for every specialization $\lambda,\mu \in \{\pm 1\}$. ◊

These remarks follow directly from Corollaries 4.1.1 and 4.1.2 where each distinct prime will corresponds to a specialization of $\mathcal{K}_n^{(\lambda,\mu)}(x)$. Note that the primes in either remark can be used simultaneously to show irreducibility. For example, if we fix n and suppose there exists two primes $p = 3n+1$ and $q = 6n+1$ then $\mathcal{K}_n^{(\lambda,\mu)}(x)$ is irreducible since p corresponds to the specialization $(\lambda,\mu) = (1,\pm 1)$ and q to $(-1,-1)$.

Other cases of irreducibility can likely be shown using different (non-pure) Newton Polygons given by Theorems 3.2.2 and 3.3.2. We explore several of these possibilities in Chapter 6.

5
Galois Groups

5.1 Slopes with Prime Denominator

In this section we aim to identify Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ which have a slope $1/q$ segment for some prime $q \in (n/2, n-2)$. The existence of such polygons will allow us to invoke Theorem 2.4.12, which says that if q is a prime divisor of the Newton Index $\mathscr{N}_{\mathscr{K}_n^{(\lambda,\mu)}}$ and q is in the interval $n/2 < q < n-2$ (which we call the *Jordan interval* due to Theorem 2.2.18) then the Galois group of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ contains the alternating group A_n. Therefore, if there exists a prime p for which $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ has a segment of slope $1/q$, with q in the appropriate range, then $q \mid \mathscr{N}_{\mathscr{K}_n^{(\lambda,\mu)}}$ (recall that the Newton Index is the least common multiple of every denominator of all slopes of $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)})$ for all primes p) and $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) \supseteq A_n$. Furthermore, since $\mathrm{disc}(\mathscr{K}_n^{(\lambda,\mu)}(x)) \notin\in \mathbf{Q}^{\times 2}$ by Theorem 2.6.7, identifying Newton Polygons with such slopes will allow us to conclude (via Proposition 2.2.17) that $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) = S_n$. Theorems 2.4.12, 2.2.18, 2.6.7 and 2.2.17 therefore give the following corollary.

Corollary 5.1.1. *Fix $n \in \mathbf{N}$, $\lambda, \mu \in \{\pm 1\}$, and suppose that there exists a prime p for which $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ has a segment of slope $1/q$, where q is a prime in the interval $(n/2, n-2)$. Then $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) = S_n$.*

In order to identify these Newton Polygons, recall from Theorem 3.2.2 that if the term $b_k = 6n+6+\epsilon+6k$ in $\beta_j = b_0 \cdots b_k \cdots b_{j-1}$ is prime then the Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ takes on the following shape:

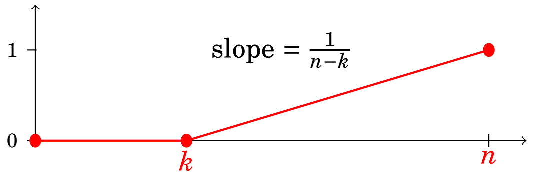


Figure 5.1.1: Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ at a prime $p = 6n+6+\epsilon+6k$

Unlike the Newton Polygons described in Theorem 3.2.2 whose slopes had denominators which were divisible by 2, we see that the denominator $n-k$ shown above may take on a prime value since $k \in \{0,\cdots,n-1\}$ (so $n-k$ could be any positive integer less than n). Hence, if for every degree n we are able to produce a prime pair p and q such that $q = n-k \in (n/2, n-2)$ and $p = 6n+6+\epsilon+6k = 6n+6+\epsilon+6(n-q) = 12n+6+\epsilon-6q$, then $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ will have a slope $1/q$ segment with q in the Jordan interval. We now state some useful equivalences.

Lemma 5.1.2. *Let $p = 6n+6+\epsilon+6k$ and let $q = n-k$. Then $n/2 < q < n-2$ if and only if $6n+18+\epsilon < p < 9n+6+\epsilon$ if and only if $2 < k < n/2$.*

Proof. We exhibit only the right implication fully; the left is not difficult and can be seen by following our statements bottom-to-top. If $n/2 < q < n-2$ then

$$\begin{aligned} p &= 6n+6+\epsilon+6k \\ &= 6n+6+\epsilon-6(n-q) \\ &= 12n+6+\epsilon-6q \\ &< 12n+6+\epsilon-6(n/2) \\ &= 9n+6+\epsilon, \end{aligned}$$

and

$$\begin{aligned} 6n+18+\epsilon &= 12n+6+\epsilon-6(n-2) \\ &< 12n+6+\epsilon-6q \\ &= p. \end{aligned}$$

Hence $6n+18+\epsilon < p < 9n+6+\epsilon$. We furthermore see that $p = 6n+6+\epsilon+6k < 9n+6+\epsilon$ implies $k < n/2$ and $6n+18+\epsilon < p = 6n+6+\epsilon+6k$ implies $2 < k$. □

Fixing $n \in \mathbf{N}$ and $\lambda, \mu \in \{\pm 1\}$, we therefore aim to determine the number of primes p and q (with either prime in the correct range due to Lemma 5.1.2) which satisfy

$$12n+6+\epsilon = p+6q.$$

Finding a single pair p and q for every n will be sufficient conclude that $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) = S_n$ since we only require the existence of one Newton Polygon with slope $1/q$ and q in the Jordan interval.

Example 5.1.3. Let $n = 50$ and $(\lambda,\mu) = (-1,1)$. Observe that the prime pair $(p,q) = (349,43)$ satisfy

$$\begin{aligned} 12n+6+\epsilon &= 12\cdot 50+6+(-1)\cdot 2+(1)\cdot 3 \\ &= 607 \\ &= 349+6\cdot 43 \\ &= p+6q. \end{aligned}$$

It now follows from Theorem 3.2.2 that $\mathtt{NP}_{349}(\mathscr{K}_{50}^{(-1,1)}(x))$ has a segment of slope $1/(n-(n-q)) = 1/43$ (since the term $b_{n-q} = b_7 = 6n+6+\epsilon+6\cdot 7 = 6\cdot 50+6+1+6\cdot 7 = 349 = p$). Thus 43 divides the Newton Index of $\mathscr{K}_{50}^{(-1,1)}(x)$ and, because $43 \in (n/2, n-2) = (25,48)$, it follows that $\mathrm{Gal}(\mathscr{K}_{50}^{(-1,1)}(x)) = S_{50}$ (assuming $\mathscr{K}_{50}^{(-1,1)}(x)$ is irreducible). Irreducibility can be seen from

Corollary 4.1.1 since $3n+\lambda = 149$ is a prime and so $\mathtt{NP}_{149}(\mathscr{K}_{50}^{(-1,1)}(x))$ is pure. (Note that the pairs $(p,q) = (421,31)$ and $(433,29)$ also satisfy $12n+6+\epsilon = p+6q$ and thus either of these pairs could also have been used to conclude the same results). ◊

We now show that it is always possible to find a prime p of the form $6n+6+\epsilon+6k$ in the interval $(6n+18+\epsilon, 9n+6+\epsilon)$. Note that proving this existence will only tell us that for every n we will be able to produce a Newton Polygon that has a slope $1/(n-k)$ segment with $n-k$ in the Jordan interval, not that $n-k$ is a prime. The existence of prime values of $n-k$ will be considered in Section 5.2.

Observe that for every choice of λ and μ we have $p = 6n+6+2\lambda+3\mu+6k \equiv 1$ or $5 \bmod 6$. It is therefore possible to write every prime in the range $6n+18+\epsilon < p < 9n+6+\epsilon$ as $p = 6n+6+2\lambda+3\mu+6k$ for some $k \in (2, n/2)$ where the specialization $(1,\mu)$ will give primes congruent to 1 mod 3 and $(-1,\mu)$ the primes congruent to 2 mod 3. Thus, it will suffice to show that we can always find a prime $p \in (6n+18+\epsilon, 9n+6+\epsilon)$ since any such prime can be written in the form $6n+6+2\lambda+3\mu+6k$. We show this using the following Theorem regarding the existence of primes in a prescribed congruence class.

Theorem 5.1.4 (Cullinan and Hajir [7])**.** *Suppose $1 \leq m \leq 72$, and a is any integer coprime to m. If $x \geq N(m)$ then the interval $(x, 1.048x]$ contains a prime congruent to a* mod *m.*

Proof. See [7, Theorem 1]. Note that $N(3) = 532$ from the table given in [7]. □

Let $x = 6n+18+\epsilon$ and consider that $x < p < 3x/2 - 9 - \epsilon/2 < 3x/2$. Theorem 5.1.4 states that for all $x \geq N(3) = 532$, the interval $(x, 1.048x] \subseteq (x, 3x/2)$ contains a prime congruent to both 1 and 2 modulo 3. Hence, for all $n \geq (532-18-\epsilon)/6 > 86$ we know that there exists a prime $p = 6n+6+\epsilon+6k \in (6n+18+\epsilon, 9n+6+\epsilon)$. We record this for future reference.

Corollary 5.1.5. *Fix some $n > 86$. Then the interval $(6n+18+\epsilon, 9n+6+\epsilon)$ contains a prime p of the form $6n+6+\epsilon+6k$.*

To see the number of such primes, we define the quantity

$$\pi_{p,\epsilon}(n) = |\{\text{primes } p = 6n+6+\epsilon+6k \colon 6n+18+\epsilon < p < 9n+6+\epsilon\}| \tag{5.1.1}$$

The value of $\pi_{p,\epsilon}(n)$ at n will give the number of Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ which have a slope $1/(n-k)$ segment with $n-k$ in the Jordan interval. We compare $\pi_{p,\epsilon}(n)$ to the quantity

$$\pi_{p,q,\epsilon}(n) = |\{\text{primes pairs } (p,q) \colon 12n+6+\epsilon = p+6q\}|, \tag{5.1.2}$$

where $q = n-k$ and $6n+18+\epsilon < p < 9n+6+\epsilon$ as above. Observe that we have defined $\pi_{p,q,\epsilon}(n)$ to give the number of Newton Polygons which have a $1/q$ segment, where q is a prime in the Jordan interval. We list the magnitude of $\pi_{p,1}(n)$ and $\pi_{p,q,1}(n)$ for several values of n in Figure 5.1.2. These values were computes using Pari/GP [20].

n	$\pi_{p,1}(n)$	$\pi_{p,q,1}(n)$
10	0	0
100	20	5
1 000	168	18
10 000	1 324	131
100 000	11 074	900
1 000 000	94 792	6 388

Figure 5.1.2: The number $\pi_{p,1}(n)$ of Newton Polygons for $\mathscr{K}_n^{(-1,1)}(x)$ which have a slope $1/(n-k)$ segment versus the number $\pi_{p,q,1}(n)$ of Newton Polygons with a slope $1/q$ segment, where both $n-k$ and q are in the Jordan interval.

As previously noted, we only need a single value $n-k$ to be a prime in the Jordan interval (which will follow from the restrictions on p) in order to conclude that $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x))$ is the full symmetric group. This is encapsulated in the following remark.

Remark 5.1.6. Fix $n \in \mathbf{N}$ and $\lambda, \mu \in \{\pm 1\}$. If there exists a prime $p \in (6n+18+\epsilon, 9n+6+\epsilon)$ such that

$$12n+6+\epsilon = p+6q \tag{5.1.3}$$

for some prime q (which is necessarily in the Jordan interval), then $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) = S_n$. ◊

As a logical statement, this Remark 5.1.6 could be presented as a theorem since it follows directly from Lemma 5.1.2 and Corollary 5.1.1. We choose to present it as a remark since it acts primarily as a summary of our discussion above; a criterion rather than a theorem. In other words, we may only conclude $\mathrm{Gal}(\mathcal{K}_n^{(\lambda,\mu)}(x)) = S_n$ if we can guarantee the *existence* of primes p and q in the appropriate ranges that satisfy the decomposition in (5.1.3). Therefore, note that Remark 5.1.6 is not is equivalent to showing $\pi_{p,q,\epsilon}(n) \geq 1$ for every n since this would establish the existence of such primes, which we presently cannot conclude. Even though Corollary 5.1.5 says that we can always find a prime p in the desired interval once n surpasses 86 (i.e., that $\pi_{p,\epsilon}(n) \geq 1$ for all $n > 86$), we cannot verify the existence of primes q which satisfy the decomposition in 5.1.3. We are hence led to the following conjecture, whose proof would imply that $\mathrm{Gal}(\mathcal{K}_n^{(\lambda,\mu)}(x)) = S_n$ via Remark 5.1.6.

Conjecture 5.1.7. *Fix $n \in \mathbf{N}$ and $\lambda, \mu \in \{\pm 1\}$. Then there exists a prime $p \in (6n+18+\epsilon, 9n+6+\epsilon)$ and a prime q, necessarily in the Jordan interval, such that*

$$12n + 6 + \epsilon = p + 6q.$$

5.2 Theorem 3.2.2 and Conjecture C of Hardy and Littlewood

In their celebrated 1922 paper [15], G. H. Hardy and J. E. Littlewood present many elegant conjectures regarding the decomposition of numbers into sums of primes. We assume one of these conjectures and use it to estimate how often the denominator $n-k$ of the Newton Polygon slope described in Theorem 3.2.2 is prime. This is done by considering the number of decompositions of

$$12n + 6 + \epsilon = p + 6q,$$

where $p = 6n + 6 + \epsilon + 6k \in (6n + 18 + \epsilon, 9n + 6 + \epsilon)$ and $q = n - k$. In other words, we analyze the growth of $\pi_{p,q,\epsilon}(n)$, where this value is defined to be the order of the set $\{\text{primes pairs } (p,q) \colon 12n + 6 + \epsilon = p + 6q\}$ where p and q are of the form described above.

Below is stated *Conjecture C* from [15] in its original form. Note that ω and ω' are primes.

Conjecture 5.2.1 (Conjecture C [15])**.** *If a, b are fixed positive integers and $(a,b) = 1$, and $\mathcal{N}(n)$ is the number of representations of n in the form*

$$n = a\omega + b\omega',$$

then

$$\mathcal{N}(n) = o\left(\frac{n}{(\log n)^2}\right)$$

unless $(n,a) = 1$, $(n,b) = 1$, and one and only one of n, a, b is even. But if these conditions are satisfied then

$$\mathcal{N}(n) \sim \frac{2C_2}{ab}\frac{n}{(\log n)^2}\prod_{\substack{\mathfrak{p}|nab \\ \mathfrak{p}\ odd}}\frac{\mathfrak{p}-1}{\mathfrak{p}-2},$$

where

$$C_2 = \prod_{odd\ primes\ p}\left(1 - \frac{1}{(p-1)^2}\right).$$

We can estimate the growth of $\pi_{p,q,\epsilon}(n)$ by employing this Conjecture as follows. We let $a = 1$, $b = 6$ and replace the value n in $\mathcal{N}(n)$ above with $12n + 6 + \epsilon$ to see that the number of ways we can write $12n + 6 + \epsilon$ as $p + 6q$ is asymptotically equivalent to

$$\frac{C_2}{3}\frac{12n{+}6{+}\epsilon}{(\log(12n{+}6{+}\epsilon))^2}\prod_{\substack{\mathfrak{p}|6(12n+6+\epsilon) \\ \mathfrak{p}\ \text{odd}}}\frac{\mathfrak{p}-1}{\mathfrak{p}-2}. \tag{5.2.1}$$

Letting $x = 12n + 6 + \epsilon$, observe that the quantity $\mathcal{N}(x)$ in (5.2.1) gives the total number of representations of $x = p + 6q$ where $p, q < x$. Thus, $\mathcal{N}(x)$ in its current form will be greater than $\pi_{p,q,\epsilon}(n)$ since it will also be counting the pairs p and q where p is outside the interval $(6n + 18 + \epsilon, 9n + 6 + \epsilon)$ and therefore q is not in the Jordan range. This is roughly illustrated in the following figure, where the pairs p, q being counted by $\pi_{p,q,\epsilon}(n)$ are in the green and red intervals.

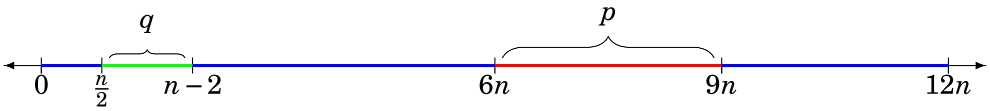


Figure 5.2.1: Primes counted by $\pi_{p,q,\epsilon}(n)$ (in green and red) versus those counted by $\mathcal{N}(x)$ (in green, red and blue).

To overcome this difficulty, we notice that $3x/4 = 9n + 9/2 + \epsilon/4 \approx 9n$ and that $x/2 = 6n + 3 + \epsilon/2 \approx 6n$. Hence, the difference $\mathcal{N}(3x/4) - \mathcal{N}(x/2)$ will give a good approximation of the number of desired decompositions.

Example 5.2.2. Let $n = 100$ and $\epsilon = 1$. We calculate both $\mathcal{N}(x)$ and $\mathcal{N}(3x/4) - \mathcal{N}(x/2)$. Note that $\pi_{p,q,1}(100) = 5$ from Table 5.1.2. Observe that $x = 12 \cdot 100 + 6 + 1 = 1207$ and $6x = 2 \cdot 3 \cdot 17 \cdot 71$. Multiplying the product

$$\prod_{\text{odd primes } p} \left(1 - \frac{1}{(p-1)^2}\right)$$

over all odd primes $p < 1\,000\,000$ gives $C_2 \approx 0.66016$. Using this approximation, we obtain

$$\begin{aligned} \mathcal{N}(x) &= \left(\frac{0.66016}{3}\right)\left(\frac{1207}{(\log 1207)^2}\right) \cdot 2(16/15)(70/69) \\ &\approx 11.416, \end{aligned}$$

which, as expected, is larger than $\pi_{p,q,1}(100)$.

To calculate $\mathcal{N}(3x/4) - \mathcal{N}(x/2)$, we choose to round down $3/4 \cdot 1207 = 905.25 \approx 905$ and $1207/2 = 603.5 \approx 603$. Using the same method and approximation of C_2 as above, we find that $\mathcal{N}(3x/4) \approx 11.5222$ and $\mathcal{N}(x/2) \approx 6.5745$. Thus $\mathcal{N}(3x/4) - \mathcal{N}(x/2) = 4.9477 \approx 5 = \pi_{p,q,1}(100)$.

Similar calculations can be done to show that, when $n = 10\,000$, we obtain $\mathcal{N}(3x/4) - \mathcal{N}(x/2) \approx 117.315$ (compare this value to $\pi_{p,q,1}(10\,000) = 131$). ♢

Assuming the Hardy-Littlewood Conjecture 5.2.1, we now provide some observations in support of Conjecture 5.1.7. First, note that because $\frac{x}{(\log(x))^2}$ is increasing and unbounded for $x > 1$ it seems plausible that both $\mathscr{N}(3x/4)$ and $\mathscr{N}(x/2)$ are increasing and unbounded as well since $C_2/3$ is constant and the product

$$\prod_{\substack{\mathrm{p}|6X \\ \mathrm{p}\text{ odd}}} \frac{\mathrm{p}-1}{\mathrm{p}-2},$$

(where $X = 3x/4$ or $x/2$), is always greater than 1. It therefore does not seem inconceivable to purpose that $\mathscr{N}(3/4x) - \mathscr{N}(x/2)$ is increasing and unbounded as well, though this certainly does not follow directly. If we suppose this were true, we now present the following argument in favour of Conjecture 5.1.7.

Letting $x = 12n+6+\epsilon$, Hardy-Littlewood Conjecture 5.2.1 says that the function $\pi_{p,q,\epsilon}(n)$ is asymptotically equivalent to $\mathscr{N}(3x/4)-\mathscr{N}(x/2)$. Corollary 5.1.5 states that for every $n > 86$ there exists a prime p in the range $6n+18+\epsilon < p < 9n+6+\epsilon$ which can be written as $p = 6n+6+\epsilon+6k$. If $\mathscr{N}(3/4x)-\mathscr{N}(x/2)$ were increasing and if we could produce some $x_0 = f(n)$ such that for all $x > x_0$ it were true that $\mathscr{N}(3/4x) - \mathscr{N}(x/2) > \pi_{p,q,\epsilon}(n)$ then because of the (conjectured) asymptotic equivalence, it should then follow that for all $n > 86$, $\pi_{p,q,1}(n) > \pi_{p,q,1}(86) > 1$. Accepting this, we would obtain the desired decomposition $12n+6+\epsilon = p + 6q$ with q in the Jordan interval, thus establishing Conjecture 5.1.7. It would follow that $\mathrm{Gal}(\mathscr{K}_n^{(\lambda,\mu)}(x)) = S_n$ (for $n > 86$) by Lemma 5.1.2 (implies $q \in (n/2, n-2)$), Theorem 3.2.2 (implies $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$ has a slope $1/q$ segment) and Corollary 5.1.1.

6

Conjectures and Partial Results

6.1 Irreducibility Using V-Shaped Polygons

Recall from Theorem 3.3.2 that Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ consisting of two opposite slopes can occur under certain conditions. Using an irreducibility result given by Bush and Hajir in [3], it is likely possible for us to use such polygons to conclude irreducibility. The applicable theorem is as follows.

Theorem 6.1.1 (Hajir [3]). *Let $f(x) \in \mathbf{Q}[x]$. Suppose that m is the maximum of the absolute values of slopes of $\mathtt{NP}_p(f(x))$ and that L is the length of the slope zero segment of $\mathtt{NP}_p(f(x))$. If $g(x) \in \mathbf{Q}[x]$ is a polynomial of degree d which divides $f(x)$ then $d \notin (L, 1/m)$.*

Proof. See [3, Lemma 2.5] □

Conjecture 6.1.2. *Fix $n \in \mathbf{N}$ and $\lambda, \mu \in \{\pm 1\}$. Suppose that there exists some $s, k \in [0, n-1]$ such that $p = 3n + \lambda - 3s$ and $q = 3n + \lambda - 3k$ are both prime. If $q = 2n + 2 + \mu$ and $(-s - 1 - \mu/2 \bmod p) \in [n, p)$ then $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible over $\mathbf{Q}$.*

If we assume the additional hypothesis that $s < k$ for every choice of $p = 3n + \lambda - 3s$ and $q = 3n + \lambda - 3k$ which satisfy the above criterion, then the proof outlined below should hold.

However, it is our belief that $s < k$ should follow from the requirement that $q = 2n+2+\mu$, though we have not yet worked out these details.

Proof. Suppose $p = 3n+\lambda-3s$ satisfies $(-s-1-\mu/2 \bmod p) \in [n,p)$, that $q = 3n+\lambda-3k$ can be written as $2n+2+\mu$ and that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is reducible over $\mathbf{Q}$. Then there must exist some irreducible polynomial $g(x) \in \mathbf{Q}[x]$ with $0 < \deg(g) = d < n$ which divides $\mathscr{K}_n^{(\lambda,\mu)}(x)$. Since $2n+2+\mu = q \equiv 0 \bmod q$ have that $n \equiv -1-\mu/2 \bmod q$ and thus that $n-k \equiv -k-1-\mu/2 \bmod q$. From Theorem 3.3.2(2), we therefore see that $\mathtt{NP}_q(\mathscr{K}_n^{(\lambda,\mu)}(x))$ has the shape shown in Figure 6.1.1.

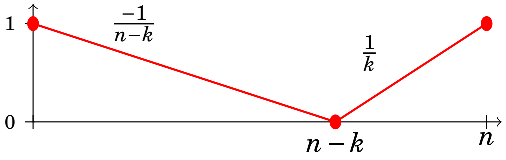


Figure 6.1.1

Furthermore, notice that $2n+2+\mu = 3n+\lambda-3k$ implies $k < n/3$. This means $k < n-2k < n-k \implies |\frac{-1}{n-k}| < 1/k$ and so $1/k = \max\{$ slopes of $\mathtt{NP}_q(\mathscr{K}_n^{(\lambda,\mu)}(x)\,\}$. Hence, from Theorem 6.1.1, we find that $d \not\in (0,k)$ and therefore (since $d \neq 0$) we have that $k \leq d < n$.

We furthermore note that Theorem 6.1.1 states that this inequality holds for any degree d_i factor of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ over $\mathbf{Q}$. In other words, if $g_i(x) \in \mathbf{Q}[x]$ is a polynomial of degree d_i which divides $\mathscr{K}_n^{(\lambda,\mu)}(x)$, assuming that $s < k$, we obtain

$$s < k \leq d_i < n. \tag{6.1.1}$$

Now consider that, by Theorem 3.3.2(1), we have the following shape for $\mathtt{NP}_p(\mathscr{K}_n^{(\lambda,\mu)}(x))$.

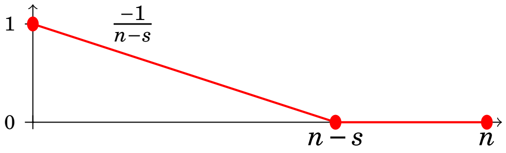


Figure 6.1.2

From Corollary 2.4.6, the Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ shown in Figure 6.1.2 allows us to conclude the following regarding the degree d of $g(x)$. One of the following holds

$$
\begin{aligned}
&(i) && d = a, \ \text{ for some } a \text{ in the interval } 0 < a \le s\\
&(ii) && d = n - s, \ \text{ or}\\
&(iii) && d = n - s + b, \ \text{ for some } b \text{ in the interval } 0 < b < s.
\end{aligned}
$$

We now show that items (i), (ii) and (iii) are false and therefore that $\deg(g) = 0$ or n, which implies the result. For item (i), observe that if $d = a \in (0,s]$ then $d \le s$ which contradicts the inequality (6.1.1) above. For item (ii), we see that if $d = n - s$ then there must exist an irreducible polynomial $g_1(x) \in \mathbf{Q}[x]$ with degree $d_1 \le s < k$ which divides $\mathscr{K}_n^{(\lambda,\mu)}(x)$, but this also contradicts inequality (6.1.1). If item (iii) were true then, similarly, there must exist some irreducible polynomial $g_2(x) \in \mathbf{Q}[x]$ with degree $d_2 \le s - b < k$ which also contradicts inequality (6.1.1). Therefore, assuming that $s < k$ is always the case, the above Newton Polygons at q and p (Figures 6.1.1 and 6.1.2, respectively) imply that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ is irreducible over $\mathbf{Q}$.

The number of degrees $n < N$ for which there exists at least one pair of primes p and q (i.e., there exists at least one desired pair of Newton Polygons) of the form described in Conjecture 6.1.2 are listed in Figure 6.1.3 for the specialization $(\lambda,\mu) = (1,1)$. We define

$$V_{(\lambda,\mu)}(N) = |\{n < N : \text{there exists primes } p = 3n + \lambda - 3s \text{ and } q = 3n + \lambda - 3k = 2n + 2 + \mu\}|.$$

N	$V_{(1,1)}(N)$
10	3
100	21
1000	148
10 000	1124
100 000	8 988

Figure 6.1.3: Number of degrees $n < N$ for which $\mathscr{K}_n^{(\lambda,\mu)}(x)$ exhibits both a V-shaped Newton Polygon of the type in Figure 6.1.1 and a Newton Polygon of the type in Figure 6.1.2.

6.2 Newton Polygons for $n = \frac{\ell^r - \lambda}{3}$

Recall from Sections 3.2 and 3.3 that we were able to find many nontrivial Newton Polygons for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ by considering primes of the form $p = a_k = 3n+\lambda-3k$ and $q = b_m = 6n+6+\epsilon+6m$ for some $k, m \in [0, n-1]$. In particular, when either $p = a_0$ or $q = b_0$ was prime, we obtained pure Newton Polygons and thus irreducibility (as stated in Corollaries 4.1.1 and 4.1.2). In this chapter, we formulate conjectures about the Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ when the first term in $\alpha_j = (3n+\lambda)(3n+\lambda-3\cdot 1)\cdots(3n+\lambda-3(n-j-1))$ is a prime power, rather than a prime. In other words, we let ℓ be a prime and consider the case where $\ell^r = a_0 = 3n+\lambda$, so that $\alpha_j = \ell^r \cdot (3n+\lambda-3\cdot 1)\cdots(3n+\lambda-3(n-j-1))$.

As with Corollaries 4.1.1 and 4.1.2, solving n in terms of ℓ^r in allows us to see that the degree

$$n = \frac{\ell^r - \lambda}{3} \tag{6.2.1}$$

of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ will give α_j this form.

We note that a similar question can be asked about the shape of $\mathtt{NP}_\ell(\mathscr{K}_n^{(\lambda,\mu)}(x))$ when $\ell^r = b_0$ in the product β_j. In other words, recall that $\beta_j = (6n+6+\epsilon)(6n+6+\epsilon+6\cdot 1)\cdots(6n+6+\epsilon+6(j-1)$ and so $b_0 = \ell^r$ whenever $n = \frac{\ell^r-6-2\lambda-3\mu}{6}$. It is our belief that considering this question with regard to β_j may allow one to recover the irreducibility results given by Mahlburg and Ono in [18] in their entirety (the results in Corollary 4.1.2 only recover some of their cases). Mahlburg and Ono have shown that $\mathtt{NP}_\ell(\mathscr{K}_n^{(\lambda,\mu)}(x))$ is irreducible at $n = \frac{\ell^r-6-2\lambda-3\mu}{6}$ (with some restrictions on ℓ and r); we believe that the degrees $n = \frac{\ell^r-\lambda}{3}$ of $\mathscr{K}_n^{(\lambda,\mu)}(x)$ may also be irreducible, though our results on this matter are only partial. In any case, we note that $\mathscr{K}_n^{(\lambda,\mu)}(x)$ seems to exhibit interesting ℓ-adic factorizations at these degrees. Our conjecture is as follows.

Conjecture 6.2.1. *Fix some prime ℓ and some $r \in \mathbf{N}$. Let $n = \frac{\ell^r - \lambda}{3}$, where*

$$\lambda = 1 \text{ } when \text{ } \ell \equiv 1 \mod 3, \text{ } and$$

$$\lambda = (-1)^r \text{ } when \text{ } \ell \equiv -1 \mod 3.$$

Let C^+ and C^- be defined by $C^{\pm} = \frac{\ell - \lambda}{3}$ (where + and − correspond to the value of λ) and let $D = \frac{\ell^2 - 1}{3}$. Define

$$S_k = \begin{cases} \sum_{j=0}^{k} \left(C^+ \ell^j \right), & \text{if } \ell \equiv 1 \text{ mod } 3, \\ \sum_{j=0}^{k} \left(D \ell^{2j} \right), & \text{if } \ell \equiv -1 \text{ mod } 3 \text{ and } r \text{ is even,} \\ C^- + \sum_{j=1}^{k} \left(D \ell^{2j-1} \right), & \text{if } \ell \equiv -1 \text{ mod } 3 \text{ and } r \text{ is odd.} \end{cases}$$

(1). If $\ell \equiv 1 \mod 3$, then the vertices of $\mathtt{NP}_\ell(\mathscr{K}_n^{(1,\mu)}(x))$ are

$$\left(0, r\right), \left(S_0, r-1\right), \left(S_1, r-2\right), \ldots, \left(S_{r-1}, 0\right).$$

In particular, $\mathtt{NP}_\ell(\mathscr{K}_n^{(1,\mu)}(x))$ consists of r segments of lengths $C^+, C^+\ell, C^+\ell^2, \ldots, C^+\ell^{r-1}$ with respective slopes $\frac{-1}{C^+}, \frac{-1}{C^+\ell}, \frac{-1}{C^+\ell^2}, \ldots, \frac{-1}{C^+\ell^{r-1}}$.

(2). If $\ell \equiv -1 \mod 3$ ($\ell > 5$) and r is even, then the vertices of $\mathtt{NP}_\ell(\mathscr{K}_n^{(1,\mu)}(x))$ are

$$\left(0, r\right), \left(S_0, r-1\right), \ldots, \left(S_{r/2-1}, \frac{r}{2}\right).$$

In particular, $\mathtt{NP}_\ell(\mathscr{K}_n^{(1,\mu)}(x))$ consists of $\frac{r}{2}$ segments of lengths $D, D\ell, D\ell^2, \ldots, D\ell^{r-2}$ with respective slopes $\frac{-1}{D}, \frac{-1}{D\ell^2}, \frac{-1}{D\ell^4}, \ldots, \frac{-1}{D\ell^{r-2}}$.

(3). If $\ell \equiv -1 \mod 3$ ($\ell > 5$) and r is odd, then the vertices of $\mathtt{NP}_\ell(\mathscr{K}_n^{(-1,\mu)}(x))$ are

$$\left(0, r\right), \left(S_0, r-1\right), \ldots, \left(S_{(r+1)/2-1}, \frac{r-1}{2}\right).$$

In particular, $\mathtt{NP}_\ell(\mathscr{K}_n^{(-1,\mu)}(x))$ consists of $\frac{r+1}{2}$ segments of lengths $C^-, D\ell, D\ell^2, \ldots, D\ell^{r-2}$ with respective slopes $\frac{-1}{C^-}, \frac{-1}{D\ell}, \frac{-1}{D\ell^3}, \ldots, \frac{-1}{D\ell^{r-2}}$.

Example 6.2.2. Let $r = 5$ and $\ell = 7$. We consider the Newton Polygon for $\mathscr{K}_n^{(1,1)}(x)$ at $n = (7^5 - 1)/3 = 5602$. Since $7 \equiv 1 \bmod 3$, Conjecture 6.2.1 (1) says $C^+ = (7-1)/3 = 2$ and so $S_k = \sum_{j=0}^{k} 2 \cdot 7^j$. The vertices of $\mathtt{NP}_7(\mathscr{K}_{5602}^{(1,1)}(x))$ are then seen to be $(0,5)$, $(2,4)$, $(2+2\cdot 7, 3)$, $(2+2\cdot 7+2\cdot 7^2, 2)$, $(2+2\cdot 7+2\cdot 7^2+2\cdot 7^3, 1)$, and $(2+2\cdot 7+2\cdot 7^2+2\cdot 7^3+2\cdot 7^4, 0)$.

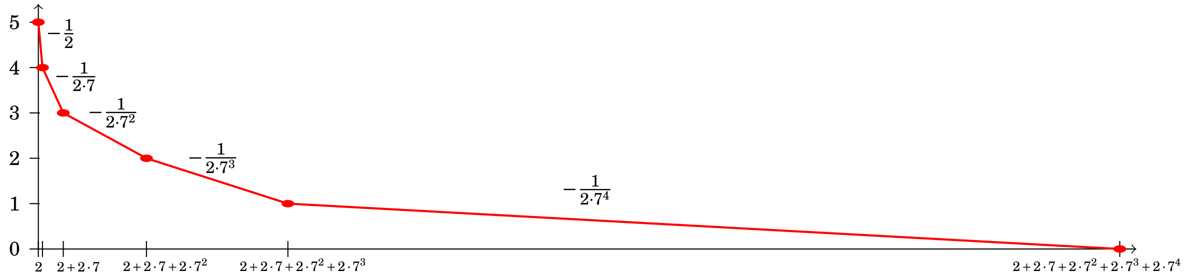


Figure 6.2.1: $\mathtt{NP}_7(\mathscr{K}_{5602}^{(1,1)}(x))$.

This Newton Polygon tells us that $\mathtt{NP}_7(\mathscr{K}_n^{(1,1)}(x)) = f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)$ over $\mathbf{Q}_p$, where the degree of each f_i is $\deg(f_i) = 2 \cdot 7^{i-1}$. Observe that the denominator of every slope of this Newton Polygon is divisible by 2. Therefore, by Coleman's Theorem 2.4.10 we can see that 2 divides the degree of every irreducible factor of $\mathtt{NP}_7(\mathscr{K}_n^{(1,1)}(x))$ over $\mathbf{Q}$. ◊

Attempting to prove Conjecture 6.2.1 has been decidedly difficult for several reasons. Namely, the prime ℓ is less than $\binom{n}{j}$, α_j and β_j, and therefore ℓ can divide each of these quantities nontrivially. Thus, determining the ℓ-adic valuation of the jth coefficient A_j requires more care than we have previously seen. Furthermore, the large magnitude of the degrees $n = \frac{\ell^r - \lambda}{3}$ means that it can take longer to compute Newton Polygons (over 8 hours were needed for Pari/GP to compute the Newton Polygon for the degree $39216 = (7^6-1)/3$ polynomial), and so generating examples for larger values of r or for bigger primes has been difficult.

Observe that Corollary 4.1.1 is a special case of Conjecture 6.2.1. If we let $r = 1$ and $\ell \equiv \lambda \bmod 3$, Conjecture 6.2.1 says that the vertices of $\mathtt{NP}_\ell(\mathcal{K}_n^{(\lambda,\mu)}(x))$ are $(0,1)$ and $(S_0,0) = ((\ell-\lambda)/3,0) = (n,0)$, which agrees precisely with the irreducibility results stated in Corollary 4.1.1.

Below are listed the necessary items for an inductive proof of Conjecture 6.2.1. We have managed to show the base case for some required steps, but a full proof has not yet been reached. The items in bold font indicate items which we have proven.

Steps to Prove Conjecture 6.2.1 *(1).*

(Base case: $r = 2$). Let $r = 2$ and let $\ell \equiv 1 \bmod 3$ (so that $n = (\ell^2-1)/3$ and we take $C = C^+ = \frac{\ell-1}{3}$). Show that

$$\textbf{(1a)}\quad \mathrm{ord}_\ell(A_0) = 2,$$

$$(1b)\quad \mathrm{ord}_\ell(A_C) = 1,$$

$$\textbf{(1c)}\quad \mathrm{ord}_\ell(A_{C+C\ell}) = 0,$$

$$(1d)\quad \mathrm{ord}_\ell(A_j) \geq 2, \text{ for all } j \in (0,C), \text{ and that}$$

$$(1e)\quad \mathrm{ord}_\ell(A_j) \geq 1, \text{ for all } j \in (C, C+C\ell).$$

Proceed using induction on r.

Steps to Prove Conjecture 6.2.1 *(2).*

(Base case: $r = 2$). Let $r = 2$ and let $\ell \equiv -1 \bmod 3$ (so that $n = (\ell^2-1)/3$ and $D = \frac{\ell^2-1}{3}$). Show that

$$\textbf{(2a)}\quad \mathrm{ord}_\ell(A_0) = 2,$$

$$\textbf{(2b)}\quad \mathrm{ord}_\ell(A_D) = 1, and$$

$$(2c)\quad \mathrm{ord}_\ell(A_j) \geq 2, \text{ for all } j \in (0,D).$$

Proceed using induction on r.

Steps to Prove Conjecture 6.2.1 *(3).*

(Base case: $r = 3$). Let $r = 3$ and let $\ell \equiv -1 \bmod 3$ (so that $n = (\ell^3+1)/3$ and $C^- = \frac{\ell+1}{3}$). Show that

(3a) $\mathrm{ord}_\ell(A_0) = 3$,

$(3b)$ $\mathrm{ord}_\ell(A_{C^-}) = 2$,

(3c) $\mathrm{ord}_\ell(A_{C^-+D\ell}) = 1$,

$(3d)$ $\mathrm{ord}_\ell(A_j) \geq 3$, for all $j \in (0, C^-)$, and that

$(3e)$ $\mathrm{ord}_\ell(A_j) \geq 1$, for all $j \in (C^-, C^- + C\ell)$.

Proceed using induction on r. □

Conjecture 6.2.1 has the following implications.

Corollary 6.2.3 (Assuming Conjecture 6.2.1)**.** *Let ℓ be a prime congruent to* 2 mod 3 *and let $n = \frac{\ell^2-1}{3}$. Then $\mathcal{K}_n^{(1,\mu)}(x)$ is irreducible over* $\mathbf{Q}$*.*

The above corollary would result from proving only the base case of Conjecture 6.2.1 (2) (i.e., a pure Newton Polygon results from setting $r = 2$). We believe that this result would be a new infinite class irreducible of degrees for $\mathcal{K}_n^{(\lambda,\mu)}(x)$.

Corollary 6.2.4 (Assuming Conjecture 6.2.1)**.** *Let ℓ be a prime and let $n = \frac{\ell^r-\lambda}{3}$, where λ is defined as in Conjecture* 6.2.1*. Suppose that $g(x) \in \mathbf{Q}[x]$ is an irreducible factor of $\mathcal{K}_n^{(\lambda,\mu)}(x)$ with degree* $\deg(g) = d$*.*

(i) If $\ell \equiv 1$ mod 3 *then $C^+|d$.*

(ii) If $\ell \equiv -1$ mod 3 *and r is even then $D|d$.*

(iii) If $\ell \equiv -1$ mod 3 *and r is odd then $gcd(C^-, D)|d$.*

Furthermore, in every case we have that d is divisible by 2^k, where

$$k = \begin{cases} \operatorname{ord}_2(C^+) & \text{if } \ell \equiv 1 \bmod 3, \\ \operatorname{ord}_2(D) & \text{if } \ell \equiv -1 \bmod 3 \text{ and } r \text{ is even}, \\ \operatorname{ord}_2(gcd(C^-,D)) & \text{if } \ell \equiv -1 \bmod 3 \text{ and } r \text{ is odd}. \end{cases}$$

Note that $k \geq 1$ in each of the cases listed in Corollary 6.2.4. Items (i), (ii) and (iii) follow easily from Coleman's Theorem 2.4.10. The second remark in this Corollary 6.2.4 is just the observation that 2 divides each C^+, C^-, D (and therefore $(gcd(C^-,D))$). Our next corollary uses a similar technique as was used in the proof we sketched for Conjecture 6.1.2.

Corollary 6.2.5 (Assuming Conjecture 6.2.1)**.** *Let $n = \frac{\ell^r - \lambda}{3}$ (where λ is chosen according to the criterion in Conjecture* 6.2.1*) and let s be a divisor of C^+ (if $\ell \equiv 1 \bmod 3$), of D (if $\ell \equiv -1 \bmod 3$ and r is even), or of $gcd(C^-,D)$ (if $\ell \equiv -1 \bmod 3$ and r is odd). If there exists a prime p such that $p = 6n + 6 + \epsilon + 6(s-1) = 2\ell^r + 3\mu + 6s$ then $\mathcal{K}_n^{(\lambda,\mu)}(x)$ is irreducible.*

Proof. We prove the case where $\ell \equiv 1 \mod 3$. Let $C = C^+$ and $g(x)$ be an irreducible factor of $\mathcal{K}_n^{(1,\mu)}(x)$ in $\mathbf{Q}[x]$ such that $0 < \deg\, g(x) = d < n$. We show by contradiction that $d = n$. From Conjecture 6.2.1 and Coleman's Theorem 2.4.10 we know that $C|d$ and thus that $s|d$. Now consider the Newton Polygon of $\mathcal{K}_n^{(1,\mu)}(x)$ at the prime p. By Theorem 3.2.2 we know that this Newton Polygon consists of two segments of lengths $s-1$ and $n-(s-1)$ with respective slopes 0 and $\frac{1}{n-(s-1)}$.

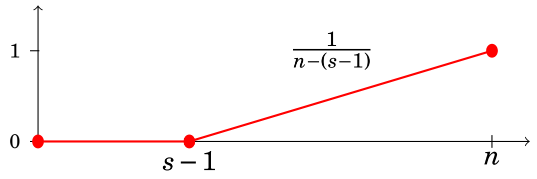


Figure 6.2.2: Newton Polygon for $\mathcal{K}_n^{(\lambda,\mu)}(x)$ at $p = 2\ell^r + 3\mu + 6s$.

Thus, we can conclude that one of the following must be true regarding the degree d of $g(x)$ over $\mathbf{Q}$.

$$\begin{aligned} &(i) && d = n-(s-1), \\ &(ii) && d = a, \text{ for some } a \text{ in the range } 1 \le a \le s-1, \\ &(iii) && d = n-(s-1)+b, \text{ for some } b \text{ in the range } 1 \le b < s-1. \end{aligned}$$

We first note that $d \equiv 0(\bmod s)$ since $s|d$. For the first case, we have that $d = n-(s-1) \equiv n+1 \bmod s$. Using Lemma 6.3.3 (i) below we know that $n = C + C\ell + C\ell^2 + \cdots + C\ell^{r-1}$ and thus that $d \equiv 1 \mod s$, which is a contradiction. For the second case, observe that $d \equiv a \mod s$, which also cannot be true since $s|d$. For the third case, we have that $d = n-(s-1)+b \equiv 1+b \bmod s$. But since, $b < s-1$, we also have a contradiction in this case. Hence $\mathscr{K}_n^{(1,\mu)}(x)$ has an irreducible factor $g(x)$ of degree n and therefore $\mathscr{K}_n^{(1,\mu)}(x)$ is irreducible over $\mathbf{Q}$. □

We expect that a similar proof can be constructed when $\ell \equiv -1 \bmod 3$ (where there would be two cases for r being even or odd), but we have not yet attempted this.

Note that Corollary 6.2.5 relies on the existence of primes of a rather complex form. Fixing r, we see that for every prime ℓ (which corresponds to a degree n) we need a prime p which can be written in terms of a *divisor* s of $C = (\ell-1)/3$. In other words, we need a pair (p,s) such that $s|(\ell-1)/3$ and

$$p - 6s = 2\ell^r + 3\mu.$$

Corollary 6.2.5 states that we only need to find one satisfactory pair for every prime ℓ in order to conclude irreducibility. To consider the number of such pairs, we define the set

$$U_{r,(\lambda,\mu)}(k) = |\{\ell \equiv \lambda \bmod 3 < k : \text{there exists } p \text{ and } s \text{ such that } s|(\ell-1)/3 \text{ and } p-6s = 2\ell^r + 3\mu\}|.$$

We record some values of $U_{2,(1,1)}(k)$ in Figure 6.2.3 below. We compare this order to the total number of primes less than k which are congruent to $1 \mod 3$, which we denote

$$\pi_{1 \bmod 3}(k) = |\{\text{primes } \ell < k : \ell \equiv 1 \bmod 3\}|.$$

k	$\pi_{1 \bmod 3}(k)$	$U_{2,(1,1)}(k)$
10	11	9
500	45	33
8 000	495	414
163 841	7 477	5 979
1 299 709	49 916	39 188

Figure 6.2.3

6.3 Base Case Proofs for the ℓ-adic Valuation of A_0 and A_n

One of the difficulties we have found while attempting to prove Conjecture 6.2.1 has been establishing that the vertices of $\mathtt{NP}_\ell \mathscr{K}_n^{(\lambda,\mu)}(x)$ are in the correct positions. This has been problematic due to the obvious reason that ℓ can divide each constituent product of $A_j = \binom{n}{j}\alpha_j\beta_j$.

A question which we only partially understand is why the reduction of ℓ modulo 3 should affect the shape of the Newton Polygon, as seen in the difference between Conjecture 6.2.1 (1) and (2). Namely, we hope to understand why the degree $n = \frac{\ell^r - \lambda}{3}$ at a prime $\ell \equiv -1 \bmod 3$ results in a Newton Polygon with half the number of segments as the Newton Polygon for $\mathscr{K}_n^{(\lambda,\mu)}(x)$ when $\ell \equiv 1 \bmod 3$.

In this section we focus primarily on the cases where $r = 2$ and $r = 3$, which are the base cases for an inductive proof of Conjecture 6.2.1. These cases offer some resolution regarding the affect that ℓ modulo 3 has on the Newton Polygon shape. From the steps listed in bold-font in Section 6.2, we will prove items: (1a), (2a) and (3a) for any value of r; (1c) and (2b) for $r = 2$; and (3c) for $r = 3$. The general propositions are as follows.

Proposition 6.3.1. *Fix some prime $\ell > 5$ and some $r \in \mathbf{N}$ and $n = \frac{\ell^r - \lambda}{3}$, where*

$$\lambda = 1 \text{ when } \ell \equiv 1 \mod 3, \text{ and}$$

$$\lambda = (-1)^r \text{ when } \ell \equiv -1 \mod 3.$$

Then

$$\mathrm{ord}_\ell(A_0) = r + \mathrm{ord}_\ell((n-1)!).$$

Proposition 6.3.2. *Fix ℓ, r and let $n = \frac{\ell^r-\lambda}{3}$ (with λ the same as in Proposition* 6.3.1.

(i). If $\ell \equiv 1 \bmod 3$ then $\mathrm{ord}_\ell(A_n) = \mathrm{ord}_\ell((n-1)!)$.

(ii). If $\ell \equiv -1 \bmod 3$ and r is even then $\mathrm{ord}_\ell(A_n) = r/2 + \mathrm{ord}_\ell((n-1)!)$.

(iii). If $\ell \equiv -1 \bmod 3$ ($\ell > 5$), r is odd then $\mathrm{ord}_\ell(A_n) = (r-1)/2 + \mathrm{ord}_\ell((n-1)!)$.

The $\mathrm{ord}_\ell((n-1)!)$ term arises since the $\mathscr{K}_n^{(\lambda,\mu)}(x)$ polynomials do not have 1 as their constant term which means their Newton Polygons can be vertically shifted. However, this shift does not affect the overall polygon shape since the vertices will have the same relative distances from one another (the lower convex hull does not change).

Before proceeding, we provide some general remarks regarding the degree $n = \frac{\ell^r-\lambda}{3}$ that we will use later on.

Lemma 6.3.3. *Fix some prime ℓ and some $r \in \mathbf{N}$. Recall the definitions $C^+ = \frac{\ell-1}{3}$, $C^- = \frac{\ell+1}{3}$ and $D = \frac{\ell^2-1}{3}$.*

(i). If $\ell \equiv 1 \mod 3$ then $\frac{\ell^r-1}{3} = \sum_{j=0}^{r-1} C^+\ell^j$.

(ii). If $\ell \equiv -1 \mod 3$ and r is even then $\frac{\ell^r-1}{3} = \sum_{j=0}^{r/2-1} D\ell^{2j}$.

(iii). If $\ell \equiv -1 \mod 3$ and r is odd then $\frac{\ell^r+1}{3} = C^- + \sum_{j=1}^{(r+1)/2-1} D\ell^{2j-1}$.

Proof. We proceed with induction on r.

Proof of (i). Let $\ell \equiv 1 \mod 3$ and let $C = C^+ = \frac{\ell-1}{3}$. The case where $r = 1$ is trivial since $\sum_{j=0}^{0} C\ell^j = C = (\ell-1)/3$. Let $r = 2$. Then

$$\begin{aligned} 3\sum_{j=0}^{2-1} C\ell^j &= 3C + 3C\ell \\ &= 3\Big(\frac{\ell-1}{3}\Big) + 3\Big(\frac{\ell-1}{3}\Big)\ell \\ &= (\ell-1) + (\ell-1)\ell \\ &= \ell^2 - 1. \end{aligned}$$

Dividing both sides of the above equation by 3 yields the result for $r = 2$. Now let $r = m$ and suppose that $\frac{\ell^m-1}{3} = \sum_{j=0}^{m-1} C\ell^j$. Then

$$\begin{aligned} 3\sum_{j=0}^{(m+1)-1} C\ell^j &= 3\sum_{j=0}^{m-1} C\ell^j + 3C\ell^m \\ &= (\ell^m - 1) + 3\Big(\frac{\ell-1}{3}\Big)\ell^m \\ &= (\ell^m - 1) + (\ell-1)\ell^m \\ &= \ell^{m+1} - 1. \end{aligned}$$

Thus $\frac{\ell^r-1}{3} = \sum_{j=0}^{r-1} C\ell^j$ for all r.

Proof of (ii). Let $\ell \equiv -1 \mod 3$ and let $r = 2m$ be an even integer. The case where $r = 2$ is trivial since $\sum_{j=0}^{0} D\ell^{2j} = D = (\ell^2-1)/3$. So we take our base case to be $r = 4$. Then

$$\begin{aligned} 3\sum_{j=0}^{4/2-1} D\ell^{2j} &= 3D + 3D\ell^2 \\ &= 3\Big(\frac{\ell^2-1}{3}\Big) + 3\Big(\frac{\ell^2-1}{3}\Big)\ell^2 \\ &= (\ell^2-1) + (\ell^2-1)\ell^2 \\ &= \ell^4 - 1. \end{aligned}$$

Dividing both sides of the above equation by 3 yields the result for $r = 4$. Now let $r = 2m$ and suppose that $\frac{\ell^r-1}{3} = \frac{\ell^{2m}-1}{3} = \sum_{j=0}^{m-1} D\ell^{2j}$. We show the result holds for $r = 2(m+1)$. Observe that

$$\begin{aligned}
3\sum_{j=0}^{r/2-1} D\ell^{2j} &= 3\sum_{j=0}^{\frac{2(m+1)}{2}-1} D\ell^{2j} \\
&= 3\sum_{j=0}^{m} D\ell^{2j} \\
&= 3\sum_{j=0}^{m-1} D\ell^{2j} + 3D\ell^{2m} \\
&= (\ell^{2m}-1) + 3\Big(\frac{\ell^2-1}{3}\Big)\ell^{2m} \\
&= \ell^{2(m+1)} - 1 \\
&= \ell^r - 1.
\end{aligned}$$

Thus $\sum_{j=0}^{r/2-1} D\ell^{2j} = \frac{\ell^r-1}{3}$ for every $r \in \mathbf{N}$.

Proof of (iii). Let $\ell \equiv -1 \mod 3$, let $r = 2m+1$ be an odd integer and let $C = C^- = (\ell+1)/3$. The case where $r = 1$ is trivial since $C + \sum_{j=1}^{(r+1)/2-1} D\ell^{2j-1} = C + \sum_{j=1}^{0} D\ell^{2j-1} = C$ under the usual convention that $\sum_{j=1}^{0} f(j) = 0$. So we take our base case to be $r = 3$. Then

$$\begin{aligned}
3\Big(C + \sum_{j=1}^{(3+1)/2-1} D\ell^{2j-1}\Big) &= 3C + 3D\ell \\
&= 3\Big(\frac{\ell+1}{3}\Big) + 3\Big(\frac{\ell^2-1}{3}\Big)\ell \\
&= (\ell+1) + (\ell^2-1)\ell \\
&= 1 + \ell^3.
\end{aligned}$$

Dividing both sides of the above equation by 3 yields the result for $r = 3$. Now let $r = 2m+1$ and suppose that

$$\frac{\ell^r+1}{3} = \frac{\ell^{(2m+1)}+1}{3} = C + \sum_{j=1}^{\frac{(2m+1)+1}{2}-1} D\ell^{2j-1}.$$

We now show that the result holds for $r = 2(m+1)+1$. Observe that

$$\begin{aligned} 3\Big(C + \sum_{j=1}^{(r+1)/2-1} D\ell^{2j-1}\Big) &= 3\Big(C + \sum_{j=1}^{m+1} D\ell^{2j-1}\Big) \\ &= 3C + 3\sum_{j=1}^{m} D\ell^{2j-1} + 3D\ell^{2(m+1)-1} \\ &= (\ell^{(2m+1)}+1) + (\ell^2-1)\ell^{2m+1} \\ &= 1 + \ell^{2(m+1)+1} \\ &= 1 + \ell^r. \end{aligned}$$

Thus $\frac{\ell^r+1}{3} = C + \sum_{j=1}^{\frac{r+1}{2}-1} D\ell^{2j-1}$ for all $r \in \mathbf{N}$. □

We are now able to prove Proposition 6.3.1.

Proof of Proposition 6.3.1. Fix some prime $\ell > 5$ and some $r \in \mathbf{N}$ and $n = \frac{\ell^r-\lambda}{3}$, where

$$\lambda = 1 \text{ when } \ell \equiv 1 \mod 3, \text{ and}$$

$$\lambda = (-1)^r \text{ when } \ell \equiv -1 \mod 3.$$

We show that

$$\mathrm{ord}_\ell(A_0) = r + \mathrm{ord}_\ell((n-1)!).$$

Since $n = \frac{\ell^r-\lambda}{3}$ we have that

$$\begin{aligned} \mathrm{ord}_\ell(A_0) &= \mathrm{ord}_\ell(\alpha_0) \\ &= \mathrm{ord}_\ell\Big(\prod_{k=0}^{n-1}(3\Big(\frac{\ell^r-\lambda}{3}\Big)+\lambda-3k)\Big) \\ &= \mathrm{ord}_\ell\Big(\prod_{k=0}^{n-1}(\ell^r-3k)\Big) \\ &= \mathrm{ord}_\ell(\ell^r) + \mathrm{ord}_\ell(\ell^r-3) + \mathrm{ord}_\ell(\ell^r-3\cdot 2)\cdots + \mathrm{ord}_\ell(\ell^r-3(n-1)) \\ &= r + \sum_{k=1}^{n-1} \mathrm{ord}_\ell(\ell^r-3k) \end{aligned}$$

Note that $\mathrm{ord}_\ell(\ell^r-3k) \le r$ for every $1 \le k \le n-1$. (If not, then there exists some $1 \le k \le n-1$ such that $\ell^r - 3k \equiv 0 \bmod \ell^{r+1}$ which implies that $3k = \ell^r$ which is clearly false since ℓ is prime).

Thus we see that every term in the sum $\sum_{k=1}^{n-1} \mathrm{ord}_\ell(\ell^r - 3k)$ is zero except when k is a multiple of ℓ^i for some $i \leq r$. But this means that the sum $\sum_{k=1}^{n-1} \mathrm{ord}_\ell(\ell^r - 3k)$ is equal to the sum of ℓ-adic valuations of every multiple of ℓ^i in the interval $[1, n-1]$. In other words, we find that

$$\sum_{k=1}^{n-1} \mathrm{ord}_\ell(\ell^r - 3k) = \mathrm{ord}_\ell(1) + \mathrm{ord}_\ell(2) + \mathrm{ord}_\ell(3) + \cdots + \mathrm{ord}_\ell(n-1)$$

since the sum on the right-hand side accounts for the ℓ-adic valuation of every possible value of k in the range $1 \leq k \leq n-1$, where each term in the right-handed sum is zero exactly when that term is not of the form $m\ell^i$ for some $m \in \mathbf{N}$ and $i \leq r$. We therefore have that

$$\begin{aligned} \sum_{k=1}^{n-1} \mathrm{ord}_\ell(\ell^r - 3k) &= \mathrm{ord}_\ell(1) + \mathrm{ord}_\ell(2) + \mathrm{ord}_\ell(3) + \cdots + \mathrm{ord}_\ell(n-1) \\ &= \mathrm{ord}_\ell((n-1)!), \end{aligned}$$

and so $\mathrm{ord}_\ell(A_0) = r + \mathrm{ord}_\ell((n-1)!)$.

In the case of $\ell \equiv 1 \bmod 3$, we can say even more. It is well-known (see [16]) that, if $n = n_0 + n_1 p + n_2 p + \cdots$ is the p-adic expansion of an integer $n \geq 1$ then

$$\mathrm{ord}(n!) = \frac{n - (n_0 + n_1 + n_2 + \cdots)}{p-1}.$$

From Lemma 6.3.3 (i) we know that the ℓ-adic expansion of $n = \frac{\ell^r - 1}{3}$ is $\sum_{j=0}^{r-1} C^+ \ell^j$, where $C^+ = (\ell - 1)/3$. Thus, letting $C^+ = C = (\ell-1)/3$, we have that

$$\begin{aligned} \mathrm{ord}_\ell((n-1)!) &= \frac{(n-1) - (rC - 1)}{\ell - 1} \\ &= \frac{(\ell^r - 1)/3 - r(\ell - 1)/3}{\ell - 1} \\ &= \frac{\ell^r - r\ell + r - 1}{3(\ell - 1)}. \end{aligned}$$

So, in the case of $\ell \equiv 1 \bmod 3$, we may conclude that $\mathrm{ord}_\ell(A_0) = r + \frac{\ell^r - r\ell + r - 1}{3(\ell - 1)}$. □

We now construct some framework in order to prove each base case of Proposition 6.3.2. The reliance of Proposition 6.3.2 on the reduction of ℓ modulo 3 is subtle and, though the following lemmas may seem unrelated at first, we have found them necessary in order to exhibit this relationship. In essence, the proof of Proposition 6.3.2 (i) will be done by constructing two sets, the first with order $\mathrm{ord}_\ell((n-1)!)$ and the second with order $\mathrm{ord}_\ell(A_n)$, and then producing a bijective function between them, allowing us to conclude that their orders are equal. The proofs of part (ii) and (iii) are done with similar sets but if $\ell \equiv -1 \bmod 3$ an element from the second set must be removed in order for our function to be bijective.

Before we proceed, consider the following preliminary observations. By definition, we can see that

$$\begin{aligned} A_n &= \binom{n}{n}\alpha_n\beta_n \\ &= \beta_n \\ &= \prod_{k=0}^{n-1}(6n+6+\epsilon+6k) \\ &= \prod_{k=0}^{n-1}(6\Big(\frac{\ell^r-\lambda}{3}\Big)+6+\epsilon+6k) \\ &= \prod_{k=0}^{n-1}(2\ell^r-2\lambda+6+2\lambda+3\mu+6k) \\ &= \prod_{k=0}^{n-1}(2\ell^r+6+3\mu+6k). \end{aligned}$$

Thus we obtain

$$\mathrm{ord}_\ell(A_n) = \sum_{k=0}^{n-1}\mathrm{ord}_\ell(2\ell^r+6+3\mu+6k). \tag{6.3.1}$$

Furthermore, when $k=0$ we have that $2\ell^r+6+3\mu \equiv 0(\bmod \ell)$ which implies $\mu \equiv -2(\bmod \ell)$, where this last congruence is only true when $\mu = 1$ and $\ell = 3 \not\equiv \pm 1 \mod 3$. We may therefore change the lower index on the sum for $\mathrm{ord}_\ell(A_n)$ in equation (6.3.1) (since the prime 3 does not fit our hypothesis) to read

$$\mathrm{ord}_\ell(A_n) = \sum_{k=1}^{n-1}\mathrm{ord}_\ell(2\ell^r+6+3\mu+6k) \tag{6.3.2}$$

Switching to the notation $b_k = 2\ell^r + 6 + 3\mu + 6k$, it is therefore seen that every term in the sum $\text{ord}_\ell(A_n) = \sum_{k=1}^{n-1} \text{ord}_\ell(b_k)$ is zero except at the values of k that satisfy

$$2\ell^r + 6 + 3\mu + 6k \equiv 0 \bmod \ell,$$

which implies that $2 + \mu + 2k \equiv 0 \bmod \ell$ and therefore $k \equiv -\mu/2 - 1 \bmod \ell$. These congruences imply that $\text{ord}_\ell(2\ell^r + 6 + 3\mu + 6k) \geq 1$ whenever $k \equiv (-\mu/2 - 1) \bmod \ell$.

When $\mu = 1$, since $(\ell-1)/2-1 \in \mathbf{Z}/\ell$ and $(\ell-1)/2-1 \equiv (\ell-1)\cdot 1/2-1 \bmod \ell \equiv (-1/2-1) \bmod \ell \equiv -\mu/2-1 \bmod \ell$, it follows that any k satisfying $2\ell^r+6+3\cdot 1+6k \equiv 0 \bmod \ell$ must reduce modulo ℓ to $(\ell-1)/2-1$. In other words, if $\mu = 1$ then every value k satisfying $b_k \equiv 0 \bmod \ell$ has the form $(\ell - 1)/2 - 1 + t\ell$ for some $t \in \mathbf{N}$.

When $\mu = -1$, we have that $(\ell + 1)/2 - 1 \in \mathbf{Z}/\ell$ and $(\ell + 1)/2 - 1 \equiv 1/2 - 1 \bmod \ell \equiv -\mu/2 - 1 \bmod \ell$. This means that, if $\mu = -1$ then every value k satisfying $b_k \equiv 0 \bmod \ell$ has the form $(\ell + 1)/2 - 1 + t\ell$ for some $t \in \mathbf{N}$. Thus we see that

$$b_k \equiv 0 \bmod \ell \ \text{ if and only if } \ k = \frac{\ell - \mu}{2} - 1 + t\ell.$$

Letting $X = \{1, \cdots, n-1\}$, we now define the sets

$$X_i \overset{\text{def}}{=} \{m \in X : m \equiv 0 \bmod \ell^i\} = \{m \in X : \text{ord}_\ell(m) \geq i\} \text{ and,} \tag{6.3.3}$$

$$X_{i_b} \overset{\text{def}}{=} \{k \in X : b_k \equiv 0 \bmod \ell^i\} = \{k \in X : \text{ord}_\ell(b_k) \geq i\}. \tag{6.3.4}$$

Note that $X_i \supseteq X_{i+1}$ and that $X_{i_b} \supseteq X_{(i+1)_b}$ for all i. Furthermore, for any given $m \in X_1$ or $k \in X_{1_b}$ it is obvious that ℓ can only divide m or b_k a finite number of times, which means that there must exist some N such that for all $i \geq N$ both X_i and X_{i_b} are empty.

Remark 6.3.4. Every $m \in X_1$ has the form $m = u\ell$ for some $u \in \mathbf{N} - \{0\}$ and, from our discussion above, we also know that every $k \in X_{1_b}$ has the form $k = \frac{\ell-\mu}{2} - 1 + t\ell$ for some $t \in \mathbf{N}$. ◊

Example 6.3.5. Let $\ell = 5$ and $r = 3$. Since $5 \equiv -1 \bmod 3$ we take $n = (5^3 - (-1))/3 = 42$ and therefore consider the polynomial $\mathscr{K}_{42}^{(-1,\mu)}(x)$. We easily find that $X_1 = \{5, 10, 15, 20, 25, 30, 35, 40\}$

and $X_2 = \{25\}$. If $\mu = 1$ then $\min\{k\} = (5-1)/2-1 = 1 \in X_{1_b}$ and so the elements of X_{1_b} are simply all the lifts of 1 mod 5 which are less than $n-1$ (i.e., $1, 1+5, 1+2\cdot5, \ldots, (1+t\cdot5) \le n-1 = 41$). Hence $X_{1_b} = \{1,6,11,16,21,26,31,36\}$ and $X_{2_b} = \{11,36\}$. If $\mu = -1$ then $\min\{k\} = (5+1)/2-1 = 2 \in X_{1_b}$ and thus $X_{1_b} = \{2,7,12,17,22,27,32,37\}$ and $X_{2_b} = \{12,37\}$. ♢

Lemma 6.3.6. *Let $k \in X_{b_1}$. Then*

$$\frac{\ell-\mu}{2} - 1 + t\ell = k \in X_{b_1} \text{ if and only if } t < \frac{2\ell^r - 3\ell - 2\lambda + 3\mu + 6}{6\ell}.$$

Proof. Since $k \in X_{b_1}$ we know that $k = \frac{\ell-\mu}{2} - 1 + t\ell < (\ell^r - \lambda)/3 = n$ by definition. This implies that $3(\ell - \mu - 2 + 2t\ell) < 2(\ell^r - \lambda)$ and so $6t\ell < 2\ell^r - 3\ell - 2\lambda + 3\mu + 6$. Hence

$$t < \frac{2\ell^r - 3\ell - 2\lambda + 3\mu + 6}{6\ell}.$$

The other implication is not difficult to see. □

We now summarize the properties of X_1 and X_{1_b} discussed above for future reference.

Remark 6.3.7. If $m \in X_1$ then:

- $m = u\ell$ for some $u \in \{1, \ldots, \lfloor \frac{n}{\ell} \rfloor\}$
- $\min\{m\} = \ell$
- $\max\{m\} = \lfloor \frac{n}{\ell} \rfloor \ell$

If $k \in X_{1_b}$ then:

- $k = (\ell - \mu)/2 - 1 + t\ell$ for some $t \in \{0, \ldots, \lfloor \frac{2\ell^r - 3\ell - 2\lambda + 3\mu + 6}{6\ell} \rfloor\}$.
- $\min\{k\} = (\ell - \mu)/2 - 1$
- $\max\{k\} = (\ell - \mu)/2 - 1 + \lfloor \frac{2\ell^r - 3\ell - 2\lambda + 3\mu + 6}{6\ell} \rfloor \ell$

♢

Furthermore, it is helpful to note the following regarding elements of X_i and X_{b_i}.

Remark 6.3.8. If $m \in X_i$ then:

- $m = u\ell^i$ for some $u \in \{1, \dots, \lfloor \frac{n}{\ell^i} \rfloor\}$

If $k \in X_{i_b}$ then:

- $k = (\ell^i - \mu)/2 - 1 + t\ell^i$ for some $t \in \{0, \dots, \lfloor \frac{2\ell^r - 3\ell^i - 2\lambda + 3\mu + 6}{6\ell^i} \rfloor\}$.

- $\max_i\{t\} \overset{\text{def}}{=} \max\{t \in \mathbf{Z} : t \in \{0, \dots, \lfloor \frac{2\ell^r - 3\ell^i - 2\lambda + 3\mu + 6}{6\ell^i} \rfloor\}$

◊

It was mentioned above that there must exist some N such that for all $i \geq N$ both X_i and X_{i_b} are empty. We claim that $N = r$.

Lemma 6.3.9. *If $k \in X_1$ then $\text{ord}_\ell(m) < r$, (which implies that $|X_i| = 0$ for all $i \geq r$).*

Proof. Suppose that there exists some $m \in X_1$ such that $\text{ord}_\ell(m) \geq r$. Then $m \equiv 0 \bmod \ell^r$. But $0 < m < n = (\ell^r - \lambda)/3 < \ell^r$ by definition, which implies that $m \not\equiv 0 \bmod \ell^r$, a contradiction. □

In the Lemma above, we were using the fact that $0 < m < \ell^r$ and thus the reduction of m modulo ℓ^r is simply m. This technique cannot be used to show that $k \in X_{1_b}$ implies $\text{ord}_\ell(b_k) = \text{ord}_\ell(2\ell^r + 6 + 3\mu + 6k) < r$ because $b_k > \ell^r$ and therefore b_k has a nontrivial reduction modulo ℓ^r. But since $k = (\ell - \mu)/2 - 1 + t\ell$ we know that

$$\begin{aligned} b_k &= 2\ell^r + 6 + 3\mu + 6k \\ &= 2\ell^r + 6 + 3\mu + 6((\ell - \mu)/2 - 1 + t\ell) \\ &= 2\ell^r + 3\ell + 6t\ell, \end{aligned}$$

and we may there construct an argument using the permitted values of t to show that $b_k \not\equiv 0 \bmod \ell^r$. In particular, we use the fact that $t < \ell^r$, a detail we now show.

Lemma 6.3.10. *Let* $t \in \{0,\dots,\lfloor\frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell}\rfloor\}$. *Then* $t < \ell^r$.

Proof. Since $t < \frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell}$ by definition, $t < \ell^r$ will be implied by showing that $\frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell} < \ell^r$. We can see this in the following way. If it were the case that $\ell^r < \frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell}$ then $6\ell^{r+1} < 2\ell^r - 3\ell - 2\lambda + 3\mu + 6$ which implies that $2\ell^r < \frac{6-3\ell-2\lambda+3\mu}{3\ell-1}$. Now observe that the numerator $6-3\ell-2\lambda+3\mu < 0$ whenever $\ell > \frac{6+3\mu-2\lambda}{3}$. But for every $\lambda,\mu \in \{\pm1\}$, we know that $\frac{6+3\mu-2\lambda}{3} \le 11/3 < 4 < \ell$ and so $6-3\ell-2\lambda+3\mu < 0$ for all primes $\ell > 4$. Since we are only concerned with primes $\ell \ge 5$ we see that $2\ell^r < \frac{6-3\ell-2\lambda+3\mu}{3\ell-1} < 0$, which is a contradiction. Thus we know that $t < \ell^r$ for any choice of λ, μ. □

Using Lemma 6.3.10 we can show the following.

Lemma 6.3.11. *If* $k \in X_{1_b}$ *then* $\text{ord}_\ell(b_k) = \text{ord}_\ell(2\ell^r + 6 + 3\mu + 6k) < r$, *(which implies that* $|X_{b_i}| = 0$ *for all* $i \ge r$*).*

Proof. Suppose that there exists some $k \in X_{1_b}$ such that $\text{ord}_\ell(2\ell^r + 6 + 3\mu + 6k) \ge r$. Then $2\ell^r + 6 + 3\mu + 6k \equiv 0 \bmod \ell^r$. Substituting $k = (\ell-\mu)/2 - 1 + t\ell$ and simplifying yields $\ell(3+6t) \equiv 0 \bmod \ell^r$ which implies that $t \equiv -1/2 \bmod \ell^r \equiv (\ell^r - 1)/2 \bmod \ell^r$. But since $0 < (\ell^r-1)/2 < \ell^r$ and $t < \ell^r$, we see that $t = (\ell^r-1)/2$. Thus, we have that $t = (\ell^r-1)/2 < \frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell}$. However, we also see that

$$\begin{aligned} t &= \frac{\ell^r-1}{2} \\ &= \frac{3\ell^r-3}{6} \\ &> \frac{3\ell^r-3}{6\ell} \\ &> \frac{2\ell^r-3}{6\ell}, \end{aligned}$$

and since $\ell \geq 5 = 15/3 > 14/3$ we have $3\ell > 14$ and so $2\ell^r - 3 > 2\ell^r - 3\ell + 11$ for all ℓ. This means that

$$\begin{aligned} t &= \frac{\ell^r - 1}{2} \\ &> \frac{2\ell^r - 3}{6\ell} \\ &> \frac{2\ell^r - 3\ell + 11}{6\ell} \\ &\geq \frac{2\ell^r - 3\ell - 2\lambda + 3\mu + 6}{6\ell}, \end{aligned}$$

which contradicts the fact that $t < \frac{2\ell^r - 3\ell - 2\lambda + 3\mu + 6}{6\ell}$. Thus $k \in X_{1_b}$ implies that $\mathrm{ord}_\ell(b_k) < r$. □

The collection of lemmas above allow us to see that

$$\sum_{i=1}^{r-1} |X_i| = \mathrm{ord}_\ell((n-1)!)$$

and

$$\sum_{i=1}^{r-1} |X_{i_b}| = \mathrm{ord}_\ell(\beta_n).$$

Recalling that $n = \frac{\ell^2 - \lambda}{3}$, we can now to illustrate the effect of $\ell \equiv \lambda \bmod 3$ in Proposition 6.3.2. Before doing so, we remind our reader of the following properties of the floor function.

Lemma 6.3.12. *Let $x \in \mathbf{R}$. Then*

(i). $\lfloor x \rfloor = m \in \mathbf{Z}$ if and only if $m - 1 \leq x < m$.

(ii). $x - 1 < \lfloor x \rfloor \leq x$.

(iii). If $m \in \mathbf{Z}$ then $\lfloor m + x \rfloor = m + \lfloor x \rfloor$.

Proof. See [17, Chapter 3] □

Lemma 6.3.13. *Let ℓ be a prime and let $r = 2$.*

(i). If $\ell \equiv 1 \bmod 3$ and $\ell > 7$ then

$$\ell(\max{}_1\{t\} + 1) < n$$

(ii). If $\ell \equiv -1 \bmod 3$ and $\ell > 2$ then

$$\ell(\max{}_1\{t\}+1) > n \textit{ and } \max{}_1\{t\}\ell < n.$$

Proof. Note that since $r = 2$ we have that $\lambda = 1$ for both cases (i) and (ii). We now proceed, remembering that $n = \frac{\ell^2-1}{3}$.

*Proof of (i).*We show that $\max_1\{t\} < n/\ell - 1$, which implies the result. Since $\ell \equiv 1 \bmod 3$ we know that $\ell = 3s+1$ for some $s \in \mathbf{N}$ such that $s > 2$. Thus

$$\begin{aligned} n &= \frac{\ell^2-1}{3} \\ &= \frac{(3s+1)^2-1}{3} \\ &= \frac{9s^2+6s}{3} \\ &= 3s^2+2s \end{aligned}$$

and so

$$\begin{aligned} \frac{n}{\ell} - 1 &= \frac{3s^2+2s}{3s+1} - 1 \\ &= \frac{3s^2-s-1}{3s+1}. \end{aligned}$$

Furthermore, recall from Remark 6.3.8 that $\max_1\{t\} = \lfloor\frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell}\rfloor$. Since $\lambda = 1$ we then obtain

$$\begin{aligned} \max{}_1\{t\} &= \left\lfloor\frac{2\ell^2-3\ell+3\mu+4}{6\ell}\right\rfloor \\ &= \left\lfloor\frac{2(3s+1)^2-3(3s+1)+3\mu+4}{6(3s+1)}\right\rfloor \\ &= \left\lfloor\frac{18s^2+3s+3\mu+3}{18s+6}\right\rfloor \\ &= \left\lfloor\frac{6s^2+s+\mu+1}{6s+2}\right\rfloor. \end{aligned}$$

We now show that

$$s-1 < \frac{6s^2+s+\mu+1}{6s+2} < s$$

in order to conclude that $\left\lfloor \frac{6s^2+s+\mu+1}{6s+2} \right\rfloor = \max_1\{t\} = s-1$ by Lemma 6.3.12. Observe that

$$\begin{aligned} (s-1)(6s+2) &= 6s^2-4s-2 \\ &< 6s^2+s \\ &\leq 6s^2+s+\mu+1 \end{aligned}$$

and thus we know that $s-1 < \frac{6s^2+s+\mu+1}{6s+2}$. Furthermore, since $s > 2$ we see that

$$\begin{aligned} 6s^2+s-\mu+1 &\leq 6s^2+s+2 \\ &< 6s^2+2s \\ &= s(6s+2), \end{aligned}$$

and so $\frac{6s^2+s+\mu+1}{6s+2} < s$. Hence $\left\lfloor \frac{6s^2+s+\mu+1}{6s+2} \right\rfloor = \max_1\{t\} = s-1$.

We now show that $\max_1\{t\} < n/\ell - 1 = \frac{3s^2-s-1}{3s+1}$. Observe that

$$\begin{aligned} \max_1\{t\}(3s+1) &= (s-1)(3s+1) \\ &= 3s^2-2s-1 \\ &< 3s^2-s-1. \end{aligned}$$

Hence $\max_1\{t\} < \frac{3s^2-s-1}{3s+1} = n/\ell - 1$ and therefore $\ell(\max_1\{t\}+1) < n$.

Proof of (ii). Since $\ell \equiv -1 \bmod 3$ we know that $\ell = 3s-1$ for some $s \in \mathbf{N}$ such that $s > 1$. We first show that $\ell(\max_1\{t\}+1) > n$ by proving that $\max_1\{t\} > n\ell - 1$. Observe that

$$\begin{aligned} n &= \frac{\ell^2-1}{3} \\ &= \frac{(3s-1)^2-1}{3} \\ &= \frac{9s^2-6s}{3} \\ &= 3s^2-2s \end{aligned}$$

and so

$$\begin{aligned}\frac{n}{\ell}-1 &= \frac{3s^2-2s}{3s-1}-1\\ &= \frac{3s^2-5s+1}{3s-1}.\end{aligned}$$

Since $\max_1\{t\} = \lfloor\frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell}\rfloor$ and because $\lambda = 1$ we have that

$$\begin{aligned}\max_1\{t\} &= \left\lfloor\frac{2\ell^2-3\ell+3\mu+4}{6\ell}\right\rfloor\\ &= \left\lfloor\frac{2(3s-1)^2-3(3s-1)+3\mu+4}{6(3s-1)}\right\rfloor\\ &= \left\lfloor\frac{18s^2-21s+3\mu+9}{18s-6}\right\rfloor\\ &= \left\lfloor\frac{6s^2-7s+\mu+3}{6s-2}\right\rfloor.\end{aligned}$$

We now show that

$$s-1 < \frac{6s^2-7s+\mu+3}{6s-2} < s$$

in order to conclude that $\max_1\{t\} = \left\lfloor\frac{6s^2-7s+\mu+3}{6s-2}\right\rfloor = s-1$ by Lemma 6.3.12. Observe that

$$\begin{aligned}(s-1)(6s-2) &= 6s^2-8s+2\\ &< 6s^2-7s+2\\ &\leq 6s^2-7s+\mu+3,\end{aligned}$$

and thus we know that $s-1 < \frac{6s^2-7s+\mu+3}{6s-2}$. Furthermore, since $s > 1$ we see that

$$\begin{aligned}6s^2-7s+\mu+3 &\leq 6s^2-7s+4\\ &< 6s^2-7s+4s\\ &= 6s^2-3s\\ &< 6s^2-2s\\ &= s(6s-2)\end{aligned}$$

and so $\frac{6s^2-7s+\mu+3}{6s-2} < s$. Hence, $\left\lfloor \frac{6s^2-7s+\mu+3}{6s-2} \right\rfloor = \max_1\{t\} = s-1$. We now show that $\max_1\{t\} > n/\ell - 1 = \frac{3s^2-5s+1}{3s-1}$. Observe that

$$\begin{aligned}
\max_1\{t\}(3s-1) &= (s-1)(3s-1) \\
&= 3s^2-4s+1 \\
&> 3s^2-5s+1.
\end{aligned}$$

Therefore $\max_1\{t\} > \frac{3s^2-5s+1}{3s-1} = n/\ell - 1$ and so $\ell(\max_1\{t\}+1) > n$. □

Lemma 6.3.14. *Let* $\ell \equiv -1 \bmod 3$ *be a prime and let* $r = 3$.

(i). If $\mu = 1$ *then* $\ell((\max_1\{t\})+1) < n$ *for all* $\ell > 11$ *and if* $\mu = -1$ *then* $\ell((\max_1\{t\})+1) < n$ *for all* $\ell > 5$

(ii). If $\ell > 5$ *then* $(\max\{t\}_2)\ell^2 < n$.

Proof. *Proof of (i).* We begin by showing that $\max_1\{t\} < n/\ell - 1$ which will imply that $\ell((\max_1\{t\})+1) < n$. Since $\ell \equiv -1 \bmod 3$ we know that $\ell = 3s-1$ for some $s \in \mathbf{N}$. Furthermore, because r is odd we have $\lambda = -1$ and so $n = (\ell^3+1)/3$. Observe that

$$\begin{aligned}
n &= \frac{\ell^3+1}{3} \\
&= \frac{(3s-1)^3+1}{3} \\
&= 9s^3-9s^2+3s
\end{aligned}$$

and so

$$\begin{aligned}
\frac{n}{\ell}-1 &= \frac{9s^3-9s^2+3s}{3s-1}-1 \\
&= \frac{9s^3-9s^2+1}{3s-1}.
\end{aligned}$$

Substituting $r = 3$, $\lambda = -1$, and $\ell = 3s - 1$ yields

$$\begin{aligned}\max{}_1\{t\} &= \left\lfloor \frac{2\ell^3 - 3\ell + 3\mu + 8}{6\ell} \right\rfloor \\ &= \left\lfloor \frac{2(3s-1)^3 - 3(3s-1) + 3\mu + 8}{6(3s-1)} \right\rfloor \\ &= \left\lfloor \frac{18s^3 - 18s^2 + 3s + \mu + 3}{6s-2} \right\rfloor.\end{aligned}$$

This expression may be simplified by observing that

$$\begin{aligned}\frac{18s^3 - 18s^2 + 3s + \mu + 3}{6s-2} &= \frac{18s^3 - 6s^2 - 12s^2 + 4s - s + \mu + 3}{6s-2} \\ &= \frac{3s^2(6s-2) - 2s(6s-2) - s + \mu + 3}{6s-2} \\ &= 3s^2 - 2s + \frac{\mu + 3 - s}{6s-2}.\end{aligned}$$

Thus

$$\max{}_1\{t\} = \left\lfloor \frac{18s^3 - 18s^2 + 3s + \mu + 3}{6s-2} \right\rfloor = 3s^2 - 2s + \left\lfloor \frac{\mu + 3 - s}{6s-2} \right\rfloor.$$

Now observe that $\frac{\mu+3-s}{6s-2} < 0$ whenever $s > \mu + 3 = 2$ or 4 (so if $\mu = 1$ we consider primes $\ell = 3s - 1 > 11$ and if $\mu = -1$ we consider primes $\ell > 5$, as stated in the hypothesis). Furthermore, because $\mu = \pm 1$ and s is positive, we see that

$$\begin{aligned}(-1)(6s-2) &= -6s + 2 \\ &< -s + 2 \\ &\leq -s + \mu + 3,\end{aligned}$$

and thus that $-1 < \frac{\mu+3-s}{6s-2}$. These two observations allow us to conclude using Lemma 6.3.12 that $\lfloor \frac{\mu+3-s}{6s-2} \rfloor = -1$ and so

$$\max{}_1\{t\} = 3s^2 - 2s - 1.$$

From this, we obtain

$$\begin{aligned}(3s-1)(3s^2 - 2s - 1) &= (3s-1)(3s^2 - 2s - 1) \\ &= 9s^3 - 9s^2 - s + 1 \\ &< 9s^3 - 9s^2 + 1\end{aligned}$$

and therefore

$$\max{}_1\{t\} = 3s^2 - 2s - 1 < \frac{9s^3 - 9s^2 + 1}{3s - 1} = \frac{n}{\ell} - 1$$

which gives the result.

Proof of (ii). We prove that $\max_2\{t\} < n/\ell^2$. As with part (i), letting $\ell = 3s - 1$ we find that $n = 9s^3 - 9s^2 + 3s$ and so

$$\begin{aligned} \frac{n}{\ell^2} &= \frac{9s^3 - 9s^2 + 3s}{(3s-1)^2} \\ &= \frac{9s^3 - 9s^2 + 3s}{9s^2 - 6s + 1} \\ &= \frac{s(9s^3 - 6s + 1) - 3s^2 + 2s}{9s^2 - 6s + 1} \\ &= s + \frac{2s - 3s^2}{9s^2 - 6s + 1} \end{aligned}$$

Recall from Remark 6.3.8 that $\max{}_2\{t\} = \lfloor \frac{2\ell^r - 3\ell^2 - 2\lambda + 3\mu + 6}{6\ell^2} \rfloor$. Substituting $r = 3, \lambda = -1$, and $\ell = 3s - 1$ yields

$$\begin{aligned} \max{}_2\{t\} &= \left\lfloor \frac{2\ell^3 - 3\ell^2 + 3\mu + 8}{6\ell^2} \right\rfloor \\ &= \left\lfloor \frac{2(3s-1)^3 - 3(3s-1)^2 + 3\mu + 8}{6(3s-1)^2} \right\rfloor \\ &= \left\lfloor \frac{54s^3 - 81s^2 + 36s + 3\mu + 3}{54s^2 - 36s + 6} \right\rfloor \\ &= \left\lfloor \frac{18s^3 - 27s^2 + 12s + \mu + 1}{18s^2 - 12s + 2} \right\rfloor \\ &= \left\lfloor \frac{(18s^3 - 12s^2 + 2s) - 15s^2 + 10s + \mu + 1}{18s^2 - 12s + 2} \right\rfloor \\ &= \left\lfloor \frac{s(18s^2 - 12s + 2) - 15s^2 + 10s + \mu + 1}{18s^2 - 12s + 2} \right\rfloor \\ &= \left\lfloor s + \frac{10s - 15s^2 + \mu + 1}{18s^2 - 12s + 2} \right\rfloor \\ &= s + \left\lfloor \frac{10s - 15s^2 + \mu + 1}{18s^2 - 12s + 2} \right\rfloor. \end{aligned}$$

We now show that $\lfloor\frac{10s-15s^2+\mu+1}{18s^2-12s+2}\rfloor = -1$. Since $\ell > 5$, we know that $s > 2$ and so $2-s < 0$. Also, consider that $11s < 15s^2$ and so $11s-15s^2 < 0$. Thus

$$\begin{aligned} 10s-15s^2+\mu+1 &= 11s-15s^2+\mu+1-s \\ &< 0+\mu+1-s \\ &\leq 2-s \\ &< 0. \end{aligned}$$

Thus $\frac{10s-15s^2+\mu+1}{18s^2-12s+2} < 0$ for all $s > 2$. Furthermore, since $-3s^2 < -2s$ we have that

$$\begin{aligned} (-1)(18s^2-12s+2) &= -18s^2+12s-2 \\ &= -3s^2-15s^2+12s-2 \\ &< -2s-15s^2+12s-2 \\ &= -15s^2+10s-2 \\ &< -15s^2+10s+\mu+1. \end{aligned}$$

Hence $\lfloor\frac{10s-15s^2+\mu+1}{18s^2-12s+2}\rfloor > -1$. This implies that

$$\left\lfloor\frac{10s-15s^2+\mu+1}{18s^2-12s+2}\right\rfloor = -1$$

and so $\max_2\{t\} = s-1$.

Finally, consider that because $-3s^2 < -2s$ we have

$$\begin{aligned} (-1)(9s^2-6s+1) &= -9s^2+6s-1 \\ &= -3s^2-6s^2+6s-1 \\ &< -2s-6s^2+6s-1 \\ &< 4s-6s^2 \\ &= 2(2s-3s^2). \end{aligned}$$

which implies that $-1/2 < \frac{2s-3s^2}{9s^2-6s+1}$. Therefore

$$\begin{aligned} \max_2\{t\} &= s-1 \\ &< s-1/2 \\ &< s+\frac{2s-3s^2}{9s^2-6s+1} \\ &= \frac{n}{\ell^2} \end{aligned}$$

and so $\max_2\{t\}\ell^2 < n$. □

We are now ready to prove the base case steps of Proposition 6.3.2.

Base Case Proof of Proposition 6.3.2. .

Proof of (i) (Base Case $r = 2$). Suppose that $\ell \equiv 1 \bmod 3$ and that $n = (\ell^2-1)/3$. We show that $\mathrm{ord}_\ell(A_n) = \mathrm{ord}_\ell((n-1)!)$. From Lemma 6.3.11, we know that $|X_i| = 0 = |X_{b_i}|$ for all $i \geq 2$. Thus we have that

$$|X_1| = |\{m \in [1, n-1] : m \equiv 0 \bmod \ell\}| = \mathrm{ord}_\ell((n-1)!)$$

and

$$|X_{1_b}| = |\{k \in [1, n-1] : b_k \equiv 0 \bmod \ell\}| = \mathrm{ord}_\ell(\beta_n).$$

This means that every integer $k \in [1, n-1]$ which contributes to the ℓ-adic valuation of b_k must be a member of the set X_{1_b}, and furthermore, that the elements of X_{1_b} are the only integers which contribute to this valuation.

We now define the function

$$\varphi : X_1 \to X_{1_b} \text{ by } \varphi(m) = \frac{\ell-\mu}{2} - 1 - \ell + m.$$

If we can show that φ is a bijection, it will follow that

$$\mathrm{ord}_\ell(\beta_n) = |X_{1_b}| = |X_1| = \mathrm{ord}_\ell((n-1)!),$$

since X_1 and X_{1_b} are both finite (see [1]).

It is clear that φ is injective. Letting $m_1, m_2 \in X_1$, we see that $\varphi(m_1) = \varphi(m_2)$ implies $m_1 - \ell - 1 + \frac{\ell-\mu}{2} = m_2 - \ell - 1 + \frac{\ell-\mu}{2}$ and so $m_1 = m_2$.

In order to show that φ is surjective, we let $k \in X_{1_b}$ and recall from Remark 6.3.8 that $k = \frac{\ell-\mu}{2} - 1 + t\ell$ for some $t \in \{0, \ldots, \lfloor \frac{2\ell^2-3\ell-2\lambda+3\mu+6}{6\ell} \rfloor\}$. Then

$$\varphi((t+1)\ell) = \frac{\ell-\mu}{2} - 1 - \ell + (t+1)\ell = \frac{\ell-\mu}{2} - 1 + t\ell = k.$$

Thus, if we can show that $(t+1)\ell \in X_1$ for all $t \in \{0, \ldots, \lfloor \frac{2\ell^2-3\ell-2\lambda+3\mu+6}{6\ell} \rfloor\}$ then will have shown that φ is surjective. Since the elements of X_1 are simply every multiple of ℓ which is less than n, it will be sufficient to show that $(t+1)\ell < n = \frac{\ell^2-\lambda}{3}$ for all $t \in \{0, \ldots, \lfloor \frac{2\ell^2-3\ell-2\lambda+3\mu+6}{6\ell} \rfloor\}$. But this follows directly from Lemma 6.3.13 (i) since

$$\begin{aligned} (t+1)\ell &\leq (\max{}_1\{t\}+1)\ell \\ &< n, \end{aligned}$$

and thus we have that φ is a bijection. Hence $\mathrm{ord}_\ell(\beta_n) = |X_{1_b}| = |X_1| = \mathrm{ord}_\ell((n-1)!)$ and we are done.

Proof of (ii) (Base Case $r = 2$). Let $\ell \equiv -1 \bmod 3$ ($\ell > 5$) suppose that $r = 2$. We show that

$$\mathrm{ord}_\ell(A_n) = r/2 + \mathrm{ord}_\ell((n-1)!) = 1 + \mathrm{ord}_\ell((n-1)!).$$

From Lemma 6.3.11, we know that $|X_i| = 0 = |X_{b_i}|$ for all $i \geq 2$. Similar to the base case in part (i), it then follows that

$$|X_1| = |\{m \in [1, n-1] : m \equiv 0 \bmod \ell\}| = \mathrm{ord}_\ell((n-1)!)$$

and

$$|X_{1_b}| = |\{k \in [1, n-1] : b_k \equiv 0 \bmod \ell\}| = \mathrm{ord}_\ell(\beta_n).$$

Recall from Remark 6.3.7 that $\max\{k\} = (\ell-\mu)/2 - 1 + \max{}_1\{t\}\ell$ where $\max{}_1\{t\} = \lfloor \frac{2\ell^r-3\ell-2\lambda+3\mu+6}{6\ell} \rfloor = s - 1$ and s is defined via the decomposition of $\ell = 3s - 1$.

We now define the function

$$\phi : X_1 \to X_{1_b} - \left\{\max\{k\}\right\}$$

by

$$\phi(m) = \frac{\ell - \mu}{2} - 1 - \ell + m.$$

If we can show that ϕ is a bijection, it will follow that

$$\mathrm{ord}_\ell((n-1)!) = |X_1| = |X_{1_b}| - 1 = \mathrm{ord}_\ell(\beta_n) - 1$$

and thus that

$$\mathrm{ord}_\ell(\beta_n) = \mathrm{ord}_\ell((n-1)!) + 1.$$

It is clear that ϕ is injective. In order to show that ϕ is surjective, we let $k \in X_{1_b} - \{\max\{k\}\}$ and observe that $k = \frac{\ell-\mu}{2} - 1 + t\ell$ for some $t \in \{0, \ldots, \lfloor \frac{2\ell^2 - 3\ell - 2\lambda + 3\mu + 6}{6\ell} \rfloor - 1\}$. Consider now that

$$\phi((t+1)\ell) = \frac{\ell - \mu}{2} - 1 - \ell + (t+1)\ell = \frac{\ell - \mu}{2} - 1 + t\ell = k.$$

Hence, we must show that $(t+1)\ell \in X_1$ for all $t \in \{0, \ldots, \lfloor \frac{2\ell^2 - 3\ell - 2\lambda + 3\mu + 6}{6\ell} \rfloor - 1\}$. We know that the elements of X_1 are just every multiple of ℓ which is less than n and thus it will be sufficient to show that $(t+1)\ell < n = \frac{\ell^2 - \lambda}{3}$ for all $t \in \{0, \ldots, \lfloor \frac{2\ell^2 - 3\ell - 2\lambda + 3\mu + 6}{6\ell} \rfloor - 1\}$. By Lemma 6.3.13 (ii), we see that

$$\begin{aligned} (t+1)\ell &\leq ((\max{}_1\{t\} - 1) + 1)\ell \\ &= \max{}_1\{t\}\ell, \\ &< n \end{aligned}$$

and thus we have that ϕ is a bijection. Hence $\mathrm{ord}_\ell(\beta_n) = |X_{1_b}| = |X_1| + 1 = \mathrm{ord}_\ell((n-1)!) + 1$ and we are done.

Proof of (iii) (Base Case $r = 3$). Let $\ell \equiv -1 \bmod 3$ ($\ell > 5$) and suppose that $r = 3$. We show that $\mathrm{ord}_\ell(A_n) = (r-1)/2 + \mathrm{ord}_\ell((n-1)!)$. As before, we know that $|X_i| = 0 = |X_{b_i}|$ for all

$i \geq 3$ and thus that $\mathrm{ord}_\ell(b_k) \leq 2$ for all k. We can therefore conclude that every element $k \in [1, n-1]$ which yields $\mathrm{ord}_\ell(b_k) \geq 1$ must be an element of X_{b_1}. Furthermore, every element $k \in [1, n-1]$ which yields $\mathrm{ord}_\ell(b_k) = 2$ must be an element of the set $X_{b_2} \subset X_{b_1}$.

We now define two functions:

$$\Phi_1 : X_1 \to X_{1_b} \text{ by } \Phi_1(m) = \frac{\ell - \mu}{2} - 1 - \ell + m,$$

and

$$\Phi_2 : X_2 \to X_{2_b} - \Big\{\max\{k\}\Big\} \text{ by } \Phi_2(m') = \frac{\ell^2 - \mu}{2} - 1 - \ell^2 + m'.$$

Note that elements $m \in X_1$ have the form $m = u\ell < n$ and $m \in X_2$ have the form $m' = u'\ell^2 < n$. If we can show that Φ_1 and Φ_2 are bijections, it will follow that

$$\mathrm{ord}_\ell((n-1)!) = |X_1| + |X_2| = |X_{1_b}| + |X_{2_b}| - 1 = \mathrm{ord}_\ell(\beta_n) - 1$$

and thus that

$$\mathrm{ord}_\ell(\beta_n) = \mathrm{ord}_\ell((n-1)!) + 1.$$

It is routine to check that both Φ_1 and Φ_2 are injections. We now show that Φ_1 is surjective. Let $k \in X_{1_b}$ and recall that $k = \frac{\ell-\mu}{2} - 1 + t\ell$ for some $t \in \{0, \ldots, \max_1\{t\}\}$.

Consider that

$$\Phi_1((t+1)\ell) = \frac{\ell - \mu}{2} - 1 - \ell + (t+1)\ell = \frac{\ell - \mu}{2} - 1 + t\ell = k.$$

As in the other cases, we must show that $(t+1)\ell \in X_1$ for all $t \in \{0, \ldots, \max_1\{t\}\}$ in order to show that Φ_1 is surjective. It will suffice to show that $(t+1)\ell < n = \frac{\ell^3+1}{3}$ for all $t \in \{0, \ldots, \max_1\{t\}\}$. By Lemma 6.3.14 (i), we see that

$$\begin{aligned} (t+1)\ell &\leq (\max{}_1\{t\} + 1)\ell \\ &< n, \end{aligned}$$

and thus we have that Φ_1 is a bijection.

We now show that Φ_2 is surjective. Let $k' \in X_{2_b}$ and recall that $k' = \frac{\ell^2-\mu}{2} - 1 - t\ell^2$ for some $t \in \{0,\ldots,\max_2\{t\}-1\}$ (where $\max_2\{t\} = \lfloor \frac{2\ell^3-3\ell^2-2\lambda+3\mu+6}{6\ell^2} \rfloor$}by Remark 6.3.8). Consider that

$$\Phi_2((t+1)\ell^2) = \frac{\ell^2-\mu}{2} - 1 - \ell^2 + (t+1)\ell^2 = \frac{\ell^2-\mu}{2} - 1 + t\ell^2 = k'.$$

Thus, we must show that $(t+1)\ell^2 \in X_2$ for all $t \in \{0,\ldots,\max_2\{t\}-1\}$ to obtain that Φ_2 is surjective. Recall that the elements of X_2 are just every multiple of ℓ^2 which is less than n and it will therefore be sufficient to show that $(t+1)\ell^2 < n = \frac{\ell^3+1}{3}$ for all $t \in \{0,\ldots,\max_2\{t\}-1\}$. By Lemma 6.3.14 (ii), we see that

$$\begin{aligned}(t+1)\ell^2 &\leq ((\max_2\{t\}-1)+1)\ell^2 \\ &= \max_2\{t\}\ell^2, \\ &< n\end{aligned}$$

Therefore Φ_2 is also a bijection. Thus we know that $\text{ord}_\ell((n-1)!) = |X_1|+|X_2| = |X_{1_b}|+|X_{2_b}|-1 = \text{ord}_\ell(\beta_n)-1$ and the result for $r=3$ follows. □

Propositions 6.3.1 and 6.3.2 lead to the following corollary, which we have shown to be true when $r=2$ (for items (i) and (ii)) and $r=3$ (item (iii)) below.

Corollary 6.3.15. *Let* $n = \frac{\ell^r-\lambda}{3}$*, where* r *and* λ *are defined as in Theorem* 4.2.1.

(i). If $\ell \equiv 1 \bmod 3$ *then* $\text{ord}_\ell(A_0) - \text{ord}_\ell(A_n) = r$.

(ii). If $\ell \equiv -1 \bmod 3$ *and* r *is even then* $\text{ord}_\ell(A_0) - \text{ord}_\ell(A_n) = r/2$.

(iii). If $\ell \equiv -1 \bmod 3$ *and* r *is odd then* $\text{ord}_\ell(A_0) - \text{ord}_\ell(A_n) = (r+1)/2$.

Computational evidence gathered in Pari/GP suggests the following relationship between the family of functions $\phi_i : X_i \to X_{i_b}$ and $\Phi_i : X_i \to X_{i_b}$, depending on whether r is even or odd ($\ell \equiv -1 \bmod 3$ in both these cases).

Conjecture 6.3.16. *Let* $r \in \mathbf{N}$ *and let* $\ell \equiv -1 \bmod 3$.

(i) Suppose that r is even. If $i \in \mathbf{N}$ is even then $\phi_i : X_i \to X_{i_b}$ is a bijection and if i is odd then $\phi_i : X_i \to X_{i_b} - \{\max_i\{k\}\}$ is a bijection.

(ii) Suppose that r is odd. If $i \in \mathbf{N}$ is odd then $\Phi_i : X_i \to X_{i_b}$ is a bijection and if i is even then $\Phi_i : X_i \to X_{i_b} - \{\max_i\{k\}\}$ is a bijection.

We furthermore believe the following to hold.

Conjecture 6.3.17. *Fix some prime $\ell > 5$ and some $r \in \mathbf{N}$. Let $n = \frac{\ell^r - \lambda}{3}$, where*

$$\lambda = 1 \text{ when } \ell \equiv 1 \mod 3, \text{ and}$$

$$\lambda = (-1)^r \text{ when } \ell \equiv -1 \mod 3.$$

Then

$$\mathrm{ord}_\ell(\alpha_j) = r + \mathrm{ord}_\ell((n-j-1)!)$$

for all $j \in [0, n-1]$.

6.4 Newton Polygons for Shifts of $\mathcal{K}_n^{(\lambda,\mu)}(x)$ and Other Conjectures

Conjecture 6.4.1. *Let $r \in \mathbf{N}$ and let $n = 3^r$. Then $\mathtt{NP}_3(\mathcal{K}_n^{(\lambda,\mu)}(x+4))$ is pure with slope $(1-3n)/2n$.*

Conjecture 6.4.2. *Let $k \in \mathbf{N}$ and let $n = 5^{2k}$. Then $\mathtt{NP}_5(\mathcal{K}_n^{(-1,-1)}(x+4))$ is pure.*

Conjecture 6.4.3. *Let $k \in \mathbf{N}$ and let $n = 7^k$. Then $\mathtt{NP}_7(\mathcal{K}_n^{(-1,-1)}(x+8))$ is pure.*

Conjecture 6.4.4. *For every $n \in \mathbf{N}$ and $\lambda, \mu \in \{-1, 1\}$ we have the following congruence:*

$$\mathcal{K}_n^{(\lambda,\mu)}(x) \equiv (x+2)^n \mod 3.$$

Conjecture 6.4.5. *Let $C = \frac{\ell-1}{3}$, $\ell \equiv 1 \mod 3$ and $n = \frac{3\ell^r - \ell - 2}{6}$. Then the Newton Polygon for $\mathcal{K}_n^{(1,\mu)}(x)$ at ℓ consists of $2r-1$ segments of lengths $C, C\ell, \dots, C\ell^{r-1}, \frac{C\ell^{r-1}}{2}, \frac{C\ell^{r-2}}{2}, \dots, \frac{C\ell}{2}$ with respective slopes $\frac{-1}{C}, \frac{-1}{C+\ell}, \dots, \frac{-1}{C+\ell^{r-1}}, \frac{-2}{C\ell^{r-1}}, \frac{-2}{C\ell^{r-2}}, \dots, \frac{-2}{C\ell}$.*

Conjecture 6.4.6. *Let* $C^- = \frac{\ell+1}{3}$*,* $D = \frac{\ell^2-1}{3}$*,* $\ell \equiv -1 \mod 3$*,* $n = \frac{3\ell^r - \ell + 2}{6}$ *and* r *an odd integer. Then the Newton Polygon for* $\mathscr{K}_n^{(-1,\mu)}(x)$ *at* ℓ *consists of* r *segments of lengths* $C^-, D\ell, \ldots, D\ell^{r-1}, \frac{D\ell^{r-1}}{2}, \frac{D\ell^{r-2}}{2}, \ldots, \frac{D\ell}{2}$ *with respective slopes* $\frac{-1}{C^-}, \frac{-1}{D\ell}, \ldots, \frac{-1}{D\ell^{r-1}}, \frac{-2}{D\ell^{r-1}}, \frac{-2}{D\ell^{r-2}}, \ldots, \frac{-2}{D\ell}$*.*

Bibliography

[1] Ethan Bloch, *Proofs and Fundamentals, Second Edition*, Springer (2011).

[2] John Brillhart and Patrick Morton, *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial*, Journal of Number Theory (2004).

[3] Michael R. Bush and Farshid Hajir, *An Irreducibility Lemma*, J. Ramanujan Math. Soc. 23 (2008).

[4] Robert F. Coleman, *On the Galois Groups of the Exponential Polynomials*, L'Enseignement MathŐmatique (1987).

[5] Keith Conrad, *The Galois Correspondence*, Expository paper on the author's website (http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/galoiscorr.pdf).

[6] ———, *Galois Groups as Permutation Groups*, Expository paper on the author's website (http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/galoisaspermgp.pdf).

[7] J. Cullinan and F. Hajir, *Primes of Prescribed Congruence Class in Short Intervals*, INTEGERS (2012).

[8] ———, *Ramification in iterated towers for rational functions*, manuscripta math (2011).

[9] ———, *Algebraic Properties of Certain Lifts of Supersingular Polynomials*, Preprint.

[10] John Dixon and Brian Mortimer, *Permutation Groups* (1996).

[11] Joseph Gallian, *Contemporary Abstract Algebra, Sixth Edition*, Houghton Mifflin Company, New York, 2006.

[12] Fernando Q. Gouvêa, *p-adic Numbers, An Introduction*, Springer, 1997.

[13] F. Hajir, *Algebraic properties of a family of generalized Laguerre polynomials*, Canad. J. Math. 61 (3) (2009).

[14] Marshall Hall Jr., *The Theory of Groups*, The Macmillan Company, New York, 1959.

[15] G.H. Hardy and J.E. Littlewood, *Some problems of* Partitio Numerorum *III: On the expression of a number as a sum of primes*, Acta Mathematatica, 1922.

[16] Helmut Hasse, *Number Theory*, Springer (1980).

[17] Donald Knuth, Ronald Graham, and Oren Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley Professional (1994).

[18] K. Mahlburg and K. Ono, *Arithmetic of certain hypergeometric modular forms*, Acta Arithmetica (2004).

[19] Daniel A. Marcus, *Number Fields*, Springer (1995).

[20] Pari/GP, version 2.5.0 (Bordeaux, 2013), `http://Pari/GP.math.u-bordeaux.fr/`.

[21] Joseph Rotman, *Galois Theory, Second Edition*, Springer (1998).

[22] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (1985).

[23] G. Szegö, *Orthogonal Polynomials, 4th ed.*, American mathematical society (1939).