Factorization of Ideals in Algebraic Number Theory and the Montes Algorithm

Ryan Ibarra

University of Colorado Boulder
Department of Mathematics

April 4, 2019

Thesis Advisor:
Dr. Katherine Stange, Department of Mathematics

Honors Council Representative:
Dr. Nathaniel Thiem, Department of Mathematics

Outside Reader:
Dr. Steven Pollock, Department of Physics

Factorization of Ideals in Algebraic Number Theory and the Montes Algorithm

RYAN IBARRA

ABSTRACT. Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial and θ a root of f. Further, we define the field extension $K := \mathbb{Q}(\theta)$ and denote its ring of integers by $\mathcal{O}_K$; an essential task in Algebraic Number Theory is to compute the factorization of ideals of $\mathcal{O}_K$ into prime ideals. We begin this thesis by reviewing some basic properties of number fields. Then, we describe a classical result by Dedekind which gives the factorization of the ideal $p\mathcal{O}_K$ for all primes p not dividing the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. Finally, we discuss the Montes algorithm which builds off the previous work of Ore in exploiting certain Newton polygons to encode the data needed to create a general factorization algorithm.

CONTENTS

1. Introduction

In a paper published in 1844, Ernst Kummer discovered the failure of unique factorization of elements in the rings of integers of cyclotomic extensions. Suppose θ is a root of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}$ be prime; further take $\mathcal{O}_K$ to be the ring of integers of $\mathbb{Q}(\theta)$. Kummer realized that unique factorization persisted in $\mathcal{O}_K$ in the form of "ideal numbers" which he constructed as formal symbols containing the data of a lift of an irreducible factor of $f(x) \mod p$. However, Dedekind proved that Kummer's construction was only consistent when $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. This led him to the introduce new arithmetic in $\mathcal{O}_K$ through the use of ideals for which unique factorization held in general.

This thesis gives an exposition to the problem of factoring ideals in $\mathcal{O}_K$ and specifically to the Montes algorithm—developed in Montes' 1999 thesis [12] and explored in [7], [8], and [6]—which solves the problem in general.

Acknowledgements

Thank you to my advisor, Dr. Katherine Stange, who's feedback was invaluable and always encouraging.

2. Background

We begin by defining the main structure of study for this thesis: the ring of integers $\mathcal{O}_K$ of a number field K. Thus, first we define the idea of a number field:

Definition 1. A *number field* K is the extension of the field $\mathbb{Q}$ by a root θ of an irreducible polynomial $f(x)$ with coefficients in $\mathbb{Z}$ denoted by $f \in \mathbb{Z}[x]$. We say K equals $\mathbb{Q}$ *adjoined* θ or symbolically $K = \mathbb{Q}(\theta)$.

The field K is also often referred to as an *algebraic* number field since, by definition, K is an extension of $\mathbb{Q}$ by an algebraic number. In this context, the verbs "extend" and "adjoin" can be thought of as the process of beginning with the field $\mathbb{Q}$, adding the element θ to the set $\mathbb{Q}$ (ie. taking $\mathbb{Q} \cup \{\theta\}$), and closing this new set under the field operations $\cdot$ and $+$. Thus we always have

$$\mathbb{Q} \subseteq K \subseteq \mathbb{C}.$$

An example of a number field is $K = \mathbb{Q}(\sqrt{2})$ given by $\theta = \sqrt{2}$ a root of the irreducible polynomial $f(x) = x^2 - 2$; the underlying set of this number field is characterized as

$$K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

(since the claim is that this forms a field, you must convince yourself that this set obeys the field axioms; namely, it is non-obvious that for non-zero $\alpha \in K$, there is some $\beta \in K$ such that $\alpha \cdot \beta = 1$). This field extension may also be thought of as a

vector space over $\mathbb{Q}$. Specifically, since for $a, b, c, d \in \mathbb{Q}$ we have that

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2},\\ c(a + b\sqrt{2}) &= ca + cb\sqrt{2},\\ (c + d)(a + b\sqrt{2}) &= c(a + b\sqrt{2}) + d(a + b\sqrt{2}),\end{aligned}$$

then naturally this characterizes a vector space with entries in $\mathbb{Q}$ obeying addition and scalar multiplication laws

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d),\\ c(a, b) &= (ca, cb),\\ (c + d)(a, b) &= c(a, b) + d(a, b),\end{aligned}$$

with extra multiplication structure given by

$$(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$$

since

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd.$$

Thus, $\mathbb{Q}(\sqrt{2})$ as a vector space has dimension 2. In this case, we say that the *degree* of the extension is 2.

We can readily generalize this idea to the general irreducible polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

by noting that if θ is a root of f, then $f(\theta) = 0$, so any $\alpha \in K$ can be written as

$$\alpha = b_{n-1}\theta^{n-1} + b_{n-2}\theta^{n-2} + \ldots + b_1\theta + b_0$$

for some $b_i \in \mathbb{Q}$. Therefore, we must have that the degree of the extension must agree with the degree of the polynomial whose root gives the extension.

Now that we have defined what a number field is, we may define the analogue of the ring $\mathbb{Z}$ in K called the ring of integers.

Definition 2. The *ring of integers* $\mathcal{O}_K$ of a number field K is the set of all elements satisfying *monic* polynomials in K—that is, polynomials with integer coefficients and leading coefficient 1.

So, as alluded to, this can be seen as a generalization of the idea that $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ is the set of solutions to monic polynomials in $\mathbb{Z}[x]$. As suggested in the name, $\mathcal{O}_K$ has the structure of a commutative ring. More precisely, it is a $\mathbb{Z}-$*module* which is the generalization of a vector space over a field to the analogous structure over the ring $\mathbb{Z}$. So, akin to vector spaces, $\mathcal{O}_K$ admits a basis whose $\mathbb{Z}-$linear combinations generate all of $\mathcal{O}_K$. It is simple to see that $\mathbb{Z}$ is always a $\mathbb{Z}-$*submodule* (subset with $\mathbb{Z}-$module structure) of $\mathcal{O}_K$ and thus for any basis $\mathcal{B}$ of $\mathcal{O}_K$, we must have $1 \in \mathcal{B}$. Returning to our example of $K = \mathbb{Q}(\sqrt{2})$ we consider the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$. Then, for $a, b \in \mathbb{Z}$ we have

$$\Big(x + (a + b\sqrt{2})\Big)\Big(x - (a + b\sqrt{2})\Big) = x^2 - 2ax + a^2 - 2b^2$$

so that $a+b\sqrt{2}$ obeys a monic polynomial in $\mathbb{Q}(\sqrt{2})$ which implies $a+b\sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ and $\mathbb{Z}+\mathbb{Z}\sqrt{2} = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ is a subring of $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$. In fact, it is true that for a general field extension $\mathbb{Q}(\theta)$ for θ a root of a general irreducible n-th degree polynomial that

$$\mathbb{Z}[\theta] \subseteq \mathcal{O}_{\mathbb{Q}(\theta)}.$$

In our current example, one can show the reverse containment so that

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}+\mathbb{Z}\sqrt{2} = \mathbb{Z}[\sqrt{2}]$$

by the following argument: suppose that $q,r,s,t \in \mathbb{Z}$ are such that $\frac{q}{r}+\frac{s}{t}\sqrt{2}$ satisfies a monic polynomial in $\mathbb{Q}(\sqrt{2})$. Further, let $\frac{q}{r}$ and $\frac{s}{t}$ be reduced to lowest terms so that $\gcd(q,r) = 1 = \gcd(s,t)$. Then

$$\begin{aligned}\left(x+\left(\frac{q}{r}+\frac{s}{t}\sqrt{2}\right)\right)\left(x-\left(\frac{q}{r}+\frac{qs}{t}\sqrt{2}\right)\right) &= x^2 - \frac{2q}{r}x + \frac{q^2}{r^2} - \frac{2s^2}{t^2} \\ &= x^2 - \frac{2q}{r}x + \frac{t^2q^2-2s^2r^2}{t^2r^2},\end{aligned}$$

so first we check the cases if $q=0$ or $s=0$: if $q=0$ we see that $\frac{2s^2}{t^2}$ must be an integer so $\frac{q}{r}=0$ and $\frac{s}{t}$ is an integer. Similarly, if $s=0$ we get $\frac{q^2}{r^2}$ is an integer so $\frac{s}{t}=0$ and $\frac{q}{r}$ is an integer; thus, q and s must be non-zero. With this, we can see that either $r=1$ or $r=2$ for the coefficient of x to be an integer. If $r=1$, then again we must have that $\frac{2s^2}{t^2}$ is an integer, so $\frac{q}{r}=q$ and $\frac{s}{t}$ are both integers. If $r=2$ our polynomial becomes

$$x^2 - qx + \frac{t^2q^2-8s^2}{4t^2}$$

so that necessarily $4 \mid q^2$ so $2 \mid q$. But this contradicts our assumption since we assumed $\frac{q}{r}$ was reduced and $r=2$. Therefore, in all cases $\frac{q}{r}$ and $\frac{s}{t}$ are integers so we conclude $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}+\mathbb{Z}\sqrt{2}$.

Thus, we say that a basis for the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ is $\{1,\sqrt{2}\}$ and denote this by $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$. So in this case we say that $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ admits a *power integral basis*; more generally, $\mathcal{O}_K$ admits a power integral basis if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$ so that a basis for $\mathcal{O}_K$ is 1 and powers of α:

$$\mathcal{B}_K = \{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$$

for K a degree n extension.

However, the ring of integers is not always this simple; for θ a root of the polynomial x^3-x^2-2x-8, Dedkind showed that the $\mathcal{O}_{\mathbb{Q}(\theta)}$ does not admit a power integral basis and showed that $\mathcal{B}_{\mathbb{Q}(\theta)} = \{1,\theta,\frac{1}{2}(\theta+\theta^2)\}$ forms a basis. The classification of rings of integers with a power integral basis consisting of 1 and powers of θ is known as Hasse's problem.

A concept related to this that we now define is called the *index* denoted $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. This idea gives a measure of "how far" the ring $\mathcal{O}_K$ is from the ring $\mathbb{Z}[\theta]$. It is formally given by the index of two rings:

Definition 3. Let R be a ring with subring S: the *index* $[R : S]$ is the size of the quotient R/S as additive groups.

Example 4.

- $[\mathbb{Z} : n\mathbb{Z}] = n$ for $n \in \mathbb{Z}$.

There are many other interesting properties of $\mathcal{O}_K$ that motivate study. One that draws much attention is the question if unique factorization into primes persists from $\mathbb{Z}$. These are called *unique factorization domains* (UFDs). Related to this idea is *ramification* of prime ideals in $\mathcal{O}_K$ which we will discuss later.

Now that we have defined the ring of integers, we can begin to reveal the properties that we will study. Let R be a commutative ring; we recall the definition of an ideal in R.

Definition 5. An *ideal* I of R is an additive subgroup such that if $k \in I$ and $r \in R$, then $kr = rk$ is in I.

The following are some basic examples of ideals:

Example 6 (ideals).

- $\{0\}$ and R are trivially ideals in R.
- The even integers $2\mathbb{Z}$ form an ideal in $\mathbb{Z}$.
- Multiples of fixed $n \in \mathbb{Z}$: $n\mathbb{Z}$ in $\mathbb{Z}$ is an ideal.
- For a ring R, we denote

$$R[x] = \{\text{The set of polynomials in the indeterminate } x \text{ with coefficients in } R\}$$

  (like $\mathbb{Z}[x]$ denotes polynomials in x with coefficients in $\mathbb{Z}$) which forms a ring. If $I \subseteq R$ is an ideal, then $I[x] \subseteq R[x]$ is an ideal.
- $2\mathbb{Z} + 2\sqrt{2}\mathbb{Z} = 2\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$.
- For a ring R and elements $r_1, \ldots, r_n \in R$, the ideal *generated* by $r_1, \ldots, r_n$ is
$$(r_1, \ldots, r_n) = \{r_1x_1 + \ldots + r_nx_n \mid x_i \in R\}.$$
  From this viewpoint, the last example could be given by $(2, 2\sqrt{2})$.
- $p\mathcal{O}_K = \{pk \mid p \text{ prime}, k \in \mathcal{O}_K\}$ in $\mathcal{O}_K$.

The last example is particularly relevant because it is the concern of the Montes algorithm which we will explore in detail. Now we define the notion of prime ideals– one of the major structures with which this thesis is concerned.

Definition 7. A non-trivial ideal I is called *prime* if, for $k, r \in R$, then $kr \in I$ implies k or r is in I.

At first, this definition might seem to be a unintuitive notion of primeness given the definition of primes in the integers. However, the relation becomes clear when one notes that this is a generalization of the idea that for $a, b \in \mathbb{Z}$, a prime p divides ab if and only if $p \mid a$ or $p \mid b$.

Example 8 (prime ideals).

- As one might expect the ideals $p\mathbb{Z}$ for p prime are the prime ideals in $\mathbb{Z}$.

- A proper ideal M of a ring R is said to be *maximal* if I is an ideal such that $M \subseteq I$ implies $I = R$. Thus, this definition implies that every proper ideal of R is contained in some maximal ideal. Note that existence of maximal ideals can be proved by considering a partial ordering on the set of ideals of R given by inclusion and applying Zorn's Lemma. Thus, we can see that there is not necessarily a unique maximal ideal. Furthermore, it can be shown that if R is a commutative ring, every maximal ideal is a prime ideal.

The suggestive name prime ideal should inform the reader that we aim to express an ideal of R as a unique factorization of prime ideals. Thus we need define the product of ideals.

Definition 9. The *product* of two ideals I_1 and I_2 is the ideal

$$I_1 I_2 = \{a_1 b_1 + \ldots + a_n b_n \mid a_i \in I_1, b_i \in I_2, n \in \mathbb{Z}_{>0}\}.$$

It is not hard to show that this defines a new ideal. Now, we are able to state the following theorem we have been working towards which provides motivation for our study of the ideals of $\mathcal{O}_K$.

Theorem 10. *Every non-trivial ideal of $\mathcal{O}_K$ is a product of prime ideals in $\mathcal{O}_K$ which is unique up to reordering.*

We choose to omit the proof of this theorem as it is in a different scope than this thesis, but nevertheless, it motivates all of the ideas which will be discussed. For a full treatment of this topic with proofs, the reader is directed to consult [1]. The foundations of algebraic number theory were based in ideal theory because of this theorem. This is because not all field extensions are UFDs as one might first hope, but rather unique factorization persists in the ideals as the theorem states.

Now, we are able to move to the discussion of exactly how we find the factorization of ideals in $\mathcal{O}_K$.

3. A theorem of Dedekind

It turns out that there's a known method for finding the factorization the ideal $p\mathcal{O}_K$ for all but finitely many primes p. First, we need a quick definition:

Definition 11. A *rational prime* p is a prime element of $\mathbb{Z}$.

This definition gives us a nice way to distinguish the prime numbers of $\mathbb{Z}$ from say elements of a different domain we wish to call prime such as in a UFD. We also recall the Chinese remainder theorem for rings.

Theorem 12 (Chinese Remainder Theorem)**.** *Let $I_1, I_2, \ldots, I_k$ be ideals of a ring R. Then, the map*

$$R \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$
$$r \mapsto (r + I_1, r + I_2, \ldots, r + I_k)$$

is a ring homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_k$. Further, if $I_1, I_2, \ldots, I_k$ are pairwise comaximal, this map is surjective and

$$R/(I_1 I_2 \ldots I_k) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

Finally, we need the following lemma before we present the main theorem.

Lemma 13. *Let I and J be ideals of a commutative ring R; if I and J are comaximal, then I^k and J^ℓ are comaximal for $k, \ell \in \mathbb{Z}_{>0}$.*

Proof. Suppose that $I + J = R$, but $I^k + J^\ell \neq R$ for some $k, \ell \in \mathbb{Z}_{>0}$. Then $I^k + J^\ell$ is contained in some maximal ideal M of R and thus

$$I^k, J^\ell \subseteq I^k + J^\ell \subseteq M.$$

Since M is maximal and therefore prime, $I^k, J^\ell \subseteq M$ implies $I \subseteq M$ and $J \subseteq M$ which implies $I + J \subseteq M$—a contradiction. Thus, we must have $I^k + J^\ell = R$. □

Now, we have the following theorem as a result of Dedekind from 1878 [2]:

Theorem 14. *Take $K = \mathbb{Q}(\theta)$ to be a number field with θ a root of a irreducible polynomial $f(x) \in \mathbb{Z}[x]$. Let $\mathcal{O}_K$ be the ring of integers and p a rational prime such that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Then the prime ideal factorization of $p\mathcal{O}_K$ is completely determined by the factorization of f modulo p. That is, if*

$$f(x) \equiv \phi_1(x)^{e_1}\phi_2(x)^{e_2} \dots \phi_k(x)^{e_k} \mod p$$

where the ϕ_i are irreducibles, $e_i \in \mathbb{Z}_{>0}$, then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \dots \mathfrak{p}_k^{e_k}$$

where $\mathfrak{p}_i$ is the ideal $(p, \phi_i(\theta))$.

Proof. We will prove this theorem for the case when $\mathcal{O}_K = \mathbb{Z}[\theta]$; for a proof of the general case, one may consult [1]. We will show that the rings $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\theta]/p\mathbb{Z}[\theta]$ and $\mathbb{F}_p[x]/(\overline{f}(x))$ are isomorphic, where $\mathbb{F}_p$ is the finite field of p elements and $\overline{f}(x)$ is the reduction of f modulo p.

First, we wish to prove that $\mathbb{Z}[x]/(p, \phi_j(x)) \cong \mathbb{Z}[\theta]/(p, \phi_j(\theta))$ for $\phi_j(x)$ an irreducible factor of $\overline{f}(x)$. Consider the homomorphism $\psi : \mathbb{Z}[x] \to \mathbb{Z}[\theta]/(p, \phi_j(\theta))$ which maps x to θ; then, clearly $(p, \phi_j(x)) \subseteq \ker\psi$, and ψ is surjective because $\mathbb{Z}[\theta]/(p, \phi_j(\theta))$ is a field . Thus, it is sufficient to show $\ker\psi \subseteq (p, \phi_j(x))$ to obtain our desired isomorphism. Let $k(x) \in \mathbb{Z}[x]$ be in the kernel of ψ. Then, $k(\theta) \in (p, \phi_j(\theta))$ so, by definition, $k(\theta) = a(\theta) \cdot p + b(\theta) \cdot \phi_j(\theta)$ for some $a(\theta), b(\theta) \in \mathbb{Z}[\theta]$. Now, define

$$i(x) := a(x) \cdot p + b(x) \cdot \phi_j(x) - k(x) \in \mathbb{Z}[x]$$

so that $i(\theta) = 0$. Now, since $f(x)$ is the minimal polynomial of θ, we must have that $i(x) \mid f(x)$, and thus $i(x) = f(x) \cdot c(x)$ for some $c(x) \in \mathbb{Z}[x]$. Thus, since $f(x) \in (p, \phi_j(x))$ we must have $i(x) \in (p, \phi_j(x)) \implies k(x) \in (p, \phi_j(x))$. Thus, $\ker\psi = (p, \phi_j(x))$ and we get the isomorphism

$$\mathbb{Z}[x]/(p, \phi_j(x)) \cong \mathbb{Z}[\theta]/(p, \phi_j(\theta)).$$

Now, we have that

$$\begin{aligned}\mathcal{O}_K/\mathfrak{p}_i &= \mathbb{Z}[\theta]/(p,\phi_i(\theta))\\ &\cong \mathbb{Z}[x]/(p,\phi_i(x))\\ &\cong (\mathbb{Z}[x]/p\mathbb{Z})/(\phi_i(x))\\ &\cong \mathbb{F}_p[x]/(\overline{\phi_i}(x)).\end{aligned}$$

Thus, since $\overline{\phi_i}(x)$ is irreducible over $\mathbb{F}_p[x]$, $\mathbb{F}_p[x]/(\overline{\phi_i}(x)) \cong \mathcal{O}_K/\mathfrak{p}_i$ is a field which implies $\mathfrak{p}_i$ is maximal and therefore a prime ideal.

Now, for $i \neq j$, $\overline{\phi_i}(x)$ and $\overline{\phi_j}(x)$ are relatively prime in $\mathbb{F}_p[x]$. Thus, there exists $e(x), g(x) \in \mathbb{Z}[x]$ such that $\overline{e}(x)\cdot\overline{\phi_i}(x) + \overline{g}(x)\cdot\overline{\phi_j}(x) = 1$ which implies $1 \in (p,\phi_i(x),\phi_j(x))$. Thus, $1 \in \mathfrak{p}_i + \mathfrak{p}_j$ which implies $\mathfrak{p}_i \neq \mathfrak{p}_j$ and $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are comaximal for $i \neq j$. Thus, by Lemma 13, this implies that $\mathfrak{p}_i^{e_i}$ and $\mathfrak{p}_j^{e_j}$ are comaximal. Applying the Chinese Remainder Theorem (12), we get

$$\begin{aligned}\mathbb{F}_p[x]/(\overline{f}(x)) &\cong \mathbb{F}_p[x]/(\overline{\phi_1}(x))^{e_1} \times \mathbb{F}_p[x]/(\overline{\phi_2}(x))^{e_2} \times \cdots \times \mathbb{F}_p[x]/(\overline{\phi_k}(x))^{e_k}\\ &\cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \mathcal{O}_K/\mathfrak{p}_2^{e_2} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_k^{e_k}\\ &\cong \mathcal{O}_K/\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_k^{e_k}.\end{aligned}$$

□

Example 15. Consider $\mathbb{Q}(\sqrt{5})$ with ring of integers $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. $\sqrt{5}$ is a root of

$$f(x) = x^2 - 5$$

and

$$\begin{aligned}f(x) &\equiv x^2 - 2 \mod 3,\\ \implies (3) &= (3, \sqrt{5}^2 - 2 \mod 3) = (3).\end{aligned}$$

$$\begin{aligned}f(x) &\equiv x^2 \mod 5,\\ \implies (5) &= (5, \sqrt{5} \mod 5)(5, \sqrt{5} \mod 5) = (5)^2.\end{aligned}$$

$$\begin{aligned}f(x) &\equiv x^2 - 5 \mod 7\\ \implies (7) &= (7, \sqrt{5}^2 - 5 \mod 7) = (7).\end{aligned}$$

$$\begin{aligned}f(x) &\equiv (x-4)(x-7) \mod 11\\ \implies (11) &= (11, \sqrt{5} - 4 \mod 11)(11, \sqrt{5} - 7 \mod 11)\\ &= (11, \sqrt{5} - 4)(11, \sqrt{5} - 7).\end{aligned}$$

Note, we are unable to factor (2) using this method since 2 divides $\left[\mathbb{Z}[\frac{1+\sqrt{5}}{2}] : \mathbb{Z}[\sqrt{5}]\right]$.

Thus, through Theorem 14 we have shown that the factorization of $p\mathcal{O}_K$ behaves nicely for almost all primes p. It is the primes dividing the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ which elude this criteria for factorization. These primes have been the subject of much study, and the work of Montes gives an algorithm to find these factorizations in finite time.

4. Classical results from Ore

In the work of Ore from the 1920's, he constructed Newton Polygons for each irreducible factor of f to encode the data needed to factor $p\mathcal{O}_K$ in some cases where Dedekind's criterion failed. He defined the polynomials for which this method worked to be *p-regular*. In this section, we develop the theory of abstract Newton polygons and present the *three classical dissections* given by Ore. We center the discussion around definitions and examples; one can consult a full treatment in [7].

4.1. Constructing polygons.

First we give a simple definition needed for the rest of the paper.

Definition 16. A *semigroup* is a set S with

$$* : S \times S \to S$$

such that $(s*t)*r = s*(t*r)$ for all $s, t, r \in S$. Thus, a semigroup can be seen as the algebraic structure obtained by eliminating the requirement that a group have an identity and inverses leaving associativity as the only structure left. If a semigroup contains an identity element it is said to be a *monoid*.

Example 17 (Semigroups).

- $\mathbb{Z}_{\geq 0}$ forms a monoid with $*$ the usual multiplication or addition and identities 1 or 0 respectively.
- A ring R is a semigroup under the ring multiplication.
- $M_n(R)$—the set of $n \times n$ matrices with entries in a ring R—is a semigroup with matrix multiplication. If R has identity, then $M_n(R)$ is a monoid with identity given by the diagonal matrix of all entries equal to the identity in R.
- From the same terminology as in groups, a semigroup S is said to be *abelian* if
$$a * b = b * a$$
for all $a, b \in S$.

Definition 18. Let $(S, *)$ and $(T, \cdot)$ be semigroups; A *semigroup homomorphism* is a function

$$\phi : S \to T$$

such that

$$\phi(a * b) = \phi(a) \cdot \phi(b)$$

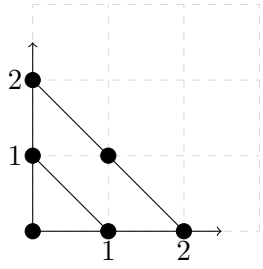
for all $a, b \in S$. If S and T are monoids with identities 1_S and 1_T respectively, then ϕ is a *monoid homomorphism* if additionally

$$\phi(1_S) = 1_T.$$

Now, denote $\mathbb{Q}^- = \{q \in \mathbb{Q} \mid q < 0\}$ and let $\lambda \in \mathbb{Q}^-$; we define $\mathcal{S}(\lambda)$ to be the set of line segments with slope λ in the positive quadrant of the plane $(\mathbb{R}_{\geq 0})^2 := \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0}$ having endpoints with integer coordinates. We call the elements of $\mathcal{S}(\lambda)$ *sides*. Let $\lambda = -h/w$ for h, w positive coprime integers; then, for $S \in \mathcal{S}(\lambda)$ we define the *length* of S, $\ell(S)$, and the *height* of S, $H(S)$, to be the length of the projections onto the horizontal and vertical axis respectively. Further, we define the *degree* of S to be $d(S) := \ell(S)/w = H(S)/h$ and denote $d = d(S)$, $\ell = \ell(S)$, $H = H(S)$ when S is clear from context. Thus, a side of $\mathcal{S}(\lambda)$ is completely determined by its *initial point* in $(\mathbb{Z}_{\geq 0})^2 := \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ and degree. In this context, the initial point of a side in $S(\lambda)$ is the top-left point, and the side is constructed by tracing a line of slope λ until it reaches the $d(S)$-th integer coordinate.

We also let a point $x \in (\mathbb{Z}_{\geq 0})^2$ be in $\mathcal{S}(\lambda)$ and define $\ell(x) = H(x) = d(x) = 0$.

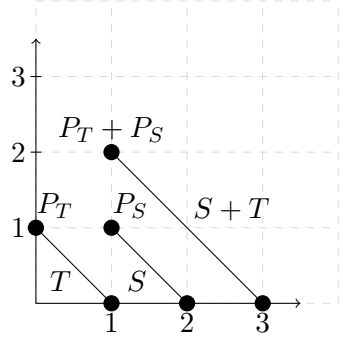
FIGURE 1. The sides of $\mathcal{S}(-1)$ with initial points near the origin



Shown are ten distinct sides of $\mathcal{S}(-1)$: six of degree 0, three of degree 1, and one of degree 2.

Let $S, T \in \mathcal{S}(\lambda)$ with initial points (s_x, s_y) and (t_x, t_y) respectively. Then, we define $S+T$ to be the side of degree $d(S)+d(T)$ with initial point (s_x+t_x, s_y+t_y) (see Figure 2 for geometric representation). We note that this gives $\mathcal{S}(\lambda)$ the structure of an abelian monoid with identity $(0, 0)$.

FIGURE 2. A visual representation of the sum of $S, T \in \mathcal{S}(-1)$ with initial points $P_T = (0, 1)$, $P_S = (1, 1)$ respectively



As we will see, it is necessary that we also allow $\lambda = -\infty$. The geometric representation of such a side is with initial point $(0, \infty)$ and endpoint somewhere in $(\mathbb{Z}_{\geq 0})^2$. The sum of sides of slope $-\infty$ is defined to be the sum of the integer representatives. In this case, we define the set

$$\mathcal{S}(-\infty) := \mathbb{Z}_{>0}$$

so that a side $S = l \in \mathcal{S}(-\infty)$ is given by the data $\ell(S) := l$, $H(S) := \infty$, and $d(S) := 1$. With this definition, we define *the sets of sides of negative slope* as

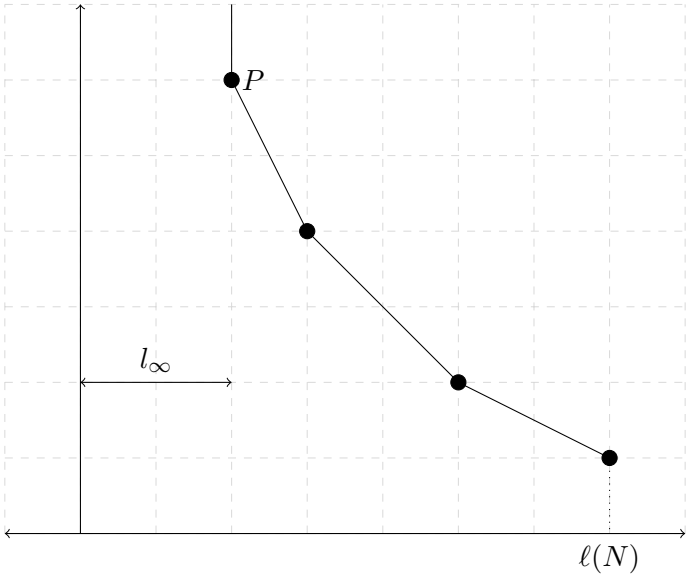
$$\mathcal{S} := \mathcal{S}(-\infty) \sqcup \left(\bigcup_{\lambda \in \mathbb{Q}} \mathcal{S}(\lambda) \right).$$

Now, using the notion of the sets of sides of negative slope, we wish to construct an open convex polygon from a sum of sides. Let

$$N = S_1 + S_2 + \cdots + S_k$$

be a finite sum of sides in $\mathcal{S}$. Further, let l' be the sum of the S_i's with slope $-\infty$ and $P_0 = (P_x, P_y)$ the sum of the initial points of the sides of finite slope (define $l' = 0$ and $P_0 = (0, 0)$ when the respective sums are empty). Then, N is the *principle polygon* with initial finite point $P := (l_\infty, P_y) := (l' + P_x, P_y)$, constructed by connecting the sides by increasing order of slope (see Figure 3).

FIGURE 3. Geometric representation of a principle polygon.



Definition 19. The monoid $\mathcal{P}$ is defined to be the set of all principle polygons with addition of polygons defined by the addition of their sides. That is, for $N, N' \in \mathcal{P}$ with

$$N = S_1 + \cdots + S_t,$$

$$N' = S_1' + \cdots + S_r'$$

then

$$N + N' = S_1 + \cdots + S_t + S_1' + \cdots + S_r'.$$

We may also extend the definition of length to principle polygons by defining

$$\ell(N) := \ell(S_1) + \cdots + \ell(S_t).$$

4.2. **Polygons from polynomials.** We give a series of definitions which gives the following association:

$f(x) \in \mathbb{Z}[x]$ and a lift of one of its irreducible factors modulo a rational prime p

$$\downarrow$$

a polygon of $\mathcal{P}$.

Definition 20. Let p be a rational prime; the *p-adic valuation* on $\mathbb{Z}$ is the function $v_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ given by

$$v_p(z) := \begin{cases} \max\{x \in \mathbb{Z}_{\geq 0} \big| p^x \text{ divides } z\} & z \neq 0 \\ \infty & z = 0. \end{cases}$$

We extend this definition to

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$$

by defining $v_p : \mathbb{Z}[x] \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ as

$$v_p(f(x)) = \min_{0 \leq i \leq n} \{v_p(a_i)\}.$$

Definition 21. Let $f(x), \phi(x)$ be irreducible polynomials in $\mathbb{Z}[x]$ with $\deg(f(x)) \geq \deg(\phi(x))$. Then, the *$\phi$-adic development of f* is

$$f(x) = b_0(x) + b_1(x)\phi(x) + \cdots + b_k(x)\phi(x)^k \tag{4.1}$$

with $b_i(x) \in \mathbb{Z}[x]$ such that $\deg(b_i(x)) < \deg(\phi(x))$. We are particularly interested in the case where f has irreducible factor $\overline{\phi}(x)$ modulo p and $\phi(x)$ is a lift of $\overline{\phi}(x)$ to $\mathbb{Z}[x]$.

The assertion of the word "the" in Definition 21 depends upon the following theorem:

Theorem 22. *The ϕ-adic development in Definition 21 is unique.*

Proof. Since $\mathbb{Z}[x]$ is a Euclidean domain, the division algorithm guarantees that

$$f(x) = \phi(x) \cdot q(x) + r(x)$$

for unique $q(x), r(x) \in \mathbb{Z}[x]$ with $\deg(r(x)) < \deg(\phi(x))$. With notation as in Definition 21, set $b_0(x) = r(x)$; now we may apply the division algorithm again to $q(x)$ to get

$$q(x) = \phi(x) \cdot c(x) + b_1(x)$$

with again $c(x), b_1(x) \in \mathbb{Z}[x]$ unique and $\deg(b_1(x)) < \deg(\phi(x))$. Thus, substitution gives

$$f(x) = \phi(x) \cdot (\phi(x) \cdot c(x) + b_1(x)) + b_0(x).$$

Now, note that in repeated application of this process, since $\deg(\phi(x)) > 0$ we must have

$$\deg(f(x)) > \deg(q(x)) > \deg(c(x)) > \dots$$

so that this process must terminate since the degree of $f(x)$ is finite. Thus, since in each level the coefficients determined are unique, we must have that the ϕ-adic development is unique. □

Example 23. We obtain the $(x^2 + x + 1)$-adic development of

$$g(x) = x^6 - 3x^3 + 10x^2 - 16$$

from the following computations:

$$\begin{aligned} x^6 - 3x^3 + 10x^2 - 16 &= (x^2 + x + 1)(x^4 - x^3 - 2x + 12) + (-10x - 28) \\ x^4 - x^3 - 2x + 12 &= (x^2 + x + 1)(x^2 - 2x + 1) + (11 - x) \\ x^2 - 2x + 1 &= (x^2 + x + 1) + (-3x) \end{aligned}$$

which implies

$$\begin{aligned} &x^6 - 3x^3 + 10x^2 - 16 = \\ &(x^2 + x + 1)((x^2 + x + 1)((x^2 + x + 1) - 3x) + (11 - x)) + (-10x - 28) \\ &= (x^2 + x + 1)^3 - 3x(x^2 + x + 1)^2 + (11 - x)(x^2 + x + 1) + (-10x - 28) \end{aligned}$$

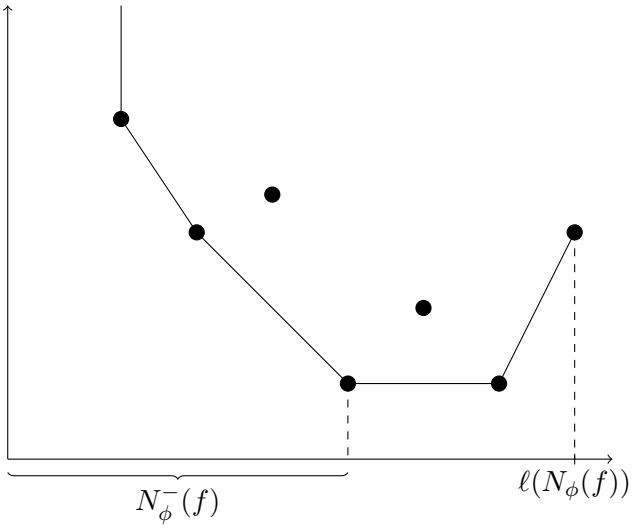
is the $(x^2 + x + 1)$-adic development of $g(x)$.

Definition 24. Let f be as in (4.1); then the ϕ-Newton polygon of f, denoted $N_\phi(f)$, is the lower convex hull in $(\mathbb{R}_{\geq 0})^2$ of the points $P_i = (i, v_p(b_i(x)))$ for $i \in \{0, 1, \dots, k\}$ such that $v_p(b_i(x)) < \infty$.

Definition 25. The *principle ϕ-polygon of* $f(x)$ is $N_\phi^-(f) \in \mathcal{P}$ constructed from the sides of negative slope of $N_\phi(f)$.

Example 26. The shape of a generic ϕ-Newton polygon is given by Figure 4.

FIGURE 4



Example 27. Let $p = 5$ and

$$f(x) = 3x^7 + 10x^6 + x^4 - 5x^3 + 15x - 25;$$

then

$$f(x) \equiv 3x^4(x+3)(x^2+2x+4) \mod 5,$$

so choosing $\overline{\phi}(x) = x + 3$ as our irreducible factor, then $\phi(x) = x + 3$ is the lift of $\overline{\phi}$. So, the $(x+3)$-adic development of f is

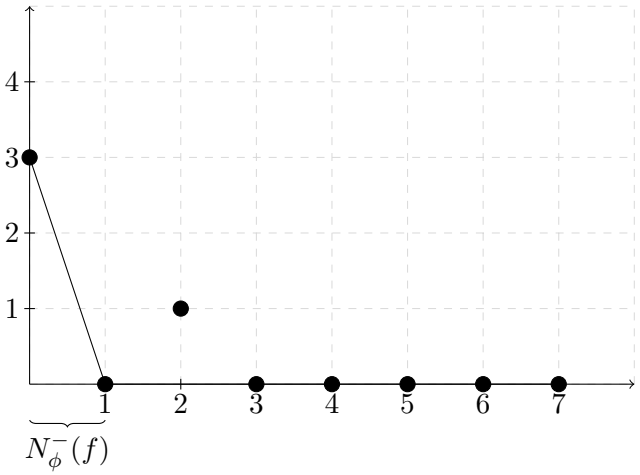
$$\begin{aligned} f(x) = {} & 3(x+3)^7 - 53(x+3)^6 + 387(x+3)^5 - 1484(x+3)^4 \\ & + 3088(x+3)^3 - 3060(x+3)^2 + 501(x+3) + 875. \end{aligned}$$

Thus, the points of the $x+3$-Newton polygon of f are

$$\begin{array}{lll} (0, v_5(875)) = (0,3), & (1, v_5(501)) = (1,0), & (2, v_5(3060)) = (2,1), \\ (3, v_5(3088)) = (3,0), & (4, v_5(1484)) = (4,0), & (5, v_5(387)) = (5,0), \\ (6, v_5(53)) = (6,0), & (7, v_5(3)) = (7,0), & \end{array}$$

so we obtain the Newton polygon in Figure 5.

FIGURE 5. $(x+3)$-Newton polygon of $f(x) = 3x^7+10x^6+x^4-5x^3+15x-25$ for $p=5$



Example 28. Consider $p = 2$ and

$$f(x) = x^5 + 4x^4 + 2x^3 + 11x^2 + 2x + 16;$$

then

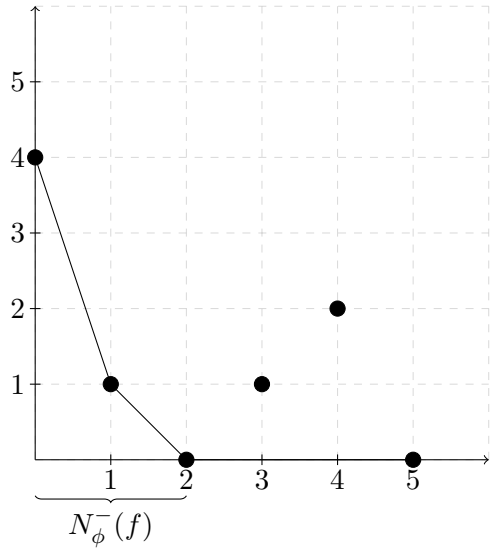
$$f(x) \equiv x^2(x^4+1) \mod 2,$$

so choosing irreducible factor $\overline{\phi}(x) = x$, then the lift is $\phi(x) = x$ and the x-adic development of f is simply f. Thus, the points of the x-Newton polygon of f are

$$\begin{array}{lll} (0, v_2(16)) = (0,4), & (1, v_2(2)) = (1,1), & (2, v_2(11)) = (2,0), \\ (3, v_2(2)) = (3,1), & (4, v_2(4)) = (4,2), & (5, v_2(1)) = (5,0). \end{array}$$

This gives the polygon in Figure 6:

FIGURE 6. x-Newton polygon of $f(x) = x^5+4x^4+2x^3+11x^2+2x+16$ for $p = 2$



Remark 29. We note the a Newton polygon $N_\phi(f)$ contains a side of slope $-\infty$ if and only if $v_p(b_m(x)) = \infty$ for some m in which case $v_p(b_i(x)) = \infty$ for all $0 \leq i \leq m$ and $\phi(x)^m \mid f(x)$. If such m is maximal for the $i \in \mathbb{Z}_{>0}$ such that $\phi(x)^i \mid f(x)$, then the finite part of $N_\phi(f)$ begins at $(m+1, v_p(b_{m+1}(x)))$ which is the endpoint of the side of slope $-\infty$.

Now that we have constructed the principle ϕ-polygon, we will show how to extract the data we need to a certain *residual polynomial*.

Definition 30. First, we define the *residual coefficients* encoded by $N_\phi^-(f) = N$. For $0 \leq i \leq \ell(N)$ we define $c_i \in \mathbb{F}_p[x]/\phi(x)$ to be

$$c_i := \begin{cases} 0 & \text{if } (i, v_p(b_i(x))) \text{ lies strictly above } N \\ \frac{b_i(x)}{p^{v_p(b_i(x))}} & \text{if } (i, v_p(b_i(x))) \text{ lies on } N. \end{cases}$$

It is clear the from the definition of N that these coefficients are well-defined. Also, c_i is always non-zero in the latter case because the $\deg(b_i(x)) < \deg(\phi(x))$.

Now, let S be a side of N of slope $\lambda = -h/w \in \mathbb{Q}^-$, h and w coprime, with initial point (u, s). We define the *residual polynomial attached to* S to be

$$R_\lambda(f)(y) := c_s + c_{s+w}y + \cdots + c_{s+(d(S)-1)w}y^{d(S)-1} + c_{s+d(S)w}y^{d(S)} \in (\mathbb{F}_p[x]/\phi(x))[y].$$

Thus, we can see by our definition of the c_i's that the only non-zero terms of $R_\lambda(f)(y)$ come from points $(i, v_p(b_i(x))$ that lie on S. By construction, c_s and $c_{s+d(S)}$ lie on the ends of S, so they are always non-zero. In particular, this implies that $y \nmid R_\lambda(f)(y)$ since $b_s(x)$ is irreducible and therefore has a non-zero constant term, and $R_\lambda(f)(y)$

is always a polynomial of degree $d(S)$—showing the relevance of our definition for the degree $d(S)$.

Example 31 (residual polynomials).

- Although long, Definition 30 simply states that we need only read off the coefficients of the residual polynomial from the points on the principle ϕ-polygon, and divide by the greatest power of p that we can. From Example 27, using Figure 5 we see that the principle $(x+3)$-polygon is one-sided with slope -3 and degree equal to 1. Then, the residual polynomial has degree one:
$$\begin{aligned} R_{-3}(f)(y) &= \frac{875}{5^3} + \frac{501}{5^0}y \\ &= 7 + 501y \in (\mathbb{F}_5[x]/(x+3))\,[y] \cong \mathbb{F}_5[y] \\ &\equiv 2 + y \end{aligned}$$
- From Example 28, in Figure 6 we see that the two residual polynomials attached to the principle x-polygon are
$$\begin{aligned} R_{-4}(f)(y) &= \frac{16}{2^4} + \frac{2}{2^1}y \\ &= 1 + y \\ R_{-1}(f)(y) &= \frac{2}{2^1} + \frac{11}{2^0}y \\ &= 1 + 11y \equiv 1 + y \end{aligned}$$
lying in $(\mathbb{F}_2[x]/x)\,[y] \cong \mathbb{F}_2[y]$.

4.3. **The results of Ore.** We showcase the results of Ore regarding the three classical dissections without proof. For a full treatment, one may consult [7]. We begin by noting that the construction of the ϕ-Newton polygon can be interpreted as a map
$$\begin{aligned} N_\phi^- : \mathbb{Z}[x] \setminus \{0\} &\to \mathcal{P} \\ f(x) &\mapsto N_\phi^-(f) \end{aligned}$$
and likewise the construction of the residual polynomial for $\lambda \in \mathbb{Q}^-$ is the map
$$\begin{aligned} R_\lambda : \mathbb{Z}[x] \setminus \{0\} &\to (\mathbb{F}_p[x]/\phi(x))\,[y] \\ f(x) &\mapsto R_\lambda(f)(y). \end{aligned}$$
Now, we can state the Theorem of the product.

Theorem 32 (Theorem of the product)**.** *For any non-zero $f(x), g(x) \in \mathbb{Z}[x]$ and $\lambda \in \mathbb{Q}^-$*
$$\begin{aligned} N_\phi^-(fg) &= N_\phi^-(f) + N_\phi^-(g) \\ R_\lambda(fg)(y) &= R_\lambda(f)(y) R_\lambda(g)(y). \end{aligned}$$
In particular, N_ϕ^- and R_λ are semigroup homomorphisms.

Notation 1. *Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$; then we denote*

$$f(x) \sim g(x)$$

if there exists $c \in \mathbb{F}^*$—the group of units of $\mathbb{F}$—such that

$$f(x) = cg(x).$$

Corollary 33. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that*

$$f(x) \equiv \phi_1(x)^{n_1}\phi_2(x)^{n_2}\cdots\phi_r(x)^{n_r} \mod p$$

is a factorization into distinct monic irreducibles $\phi_1(x), \ldots, \phi_r(x) \in \mathbb{Z}[x]$. Then, we define the first dissection of f using Hensel's Lemma to be

$$f(x) = F_1(x)\cdots F_r(x) \in \mathbb{Z}_p[x]$$

for the $F_i(x)$'s monic polynomials satisfying $F_i(x) \equiv \phi_i(x)^{n_i} \mod p$. $\mathbb{Z}_p$ denotes the p-adic integers which is the commutative ring with the underlying set

$$\left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \text{'s are in } \{0, 1, \ldots, p-1\} \right\}.$$

The field of fractions of $\mathbb{Z}_p$ called the field of p-adic numbers is $\mathbb{Q}_p$ which is a completion of $\mathbb{Q}$ with respect to the metric

$$d_p(x, y) = |x - y|_p$$

where for $a, b \in \mathbb{Z}$ coprime with p^n dividing $\frac{a}{b}$ for some maximal $|n|$, $n \in \mathbb{Z}$, has $|\frac{a}{b}|_p = p^{-n}$.

We also have

$$N^-_{\phi_i}(f) = N^-_{\phi_i}(F_i) = N_{\phi_i}(F_i)$$
$$R_\lambda(F_i)(y) \sim R_\lambda(f)(y)$$

for all $i \in \{1, 2, \ldots, r\}$ and $\lambda \in \mathbb{Q}^-$.

Now, with Corollary 33 and our theory of Newton polygons, we aim to further factorize each factor found from Hensel's lemma. Thanks to the previous lemma, we may read this information directly off of the principle polygon asssociated to f since $N^-_{\phi_i}(f) = N^-_{\phi_i}(F_i)$ and $R_\lambda(F_i)(y) \sim R_\lambda(f)(y)$; we call this the *second dissection of* f which is given by the following theorem.

Theorem 34 (Theorem of the polygon)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with irreducible factor $\overline{\phi}(x)$ modulo a prime p. Further let $f(x) = f_\phi(x)g(x)$ with $f_\phi(x) \equiv \overline{\phi}(x)^n \mod p$ the factorization of f given by Hensel lifting. Suppose that $N^-_\phi(f) = S_1 + \cdots + S_k$ has k sides with pairwise different slopes $\lambda_1, \ldots, \lambda_k$; then $f_\phi(x)$ admits a factorization in $\mathbb{Z}[x]$ into k monic polynomials*

$$f_\phi(x) = F_1(x)\cdots F_k(x)$$

such that for all $1 \le i \le k$

(1) $N_\phi(F_i) = S_i$ up to translation.
(2) λ_i finite implies $R_{\lambda_i}(F_i)(y) \sim R_{\lambda_i}(f)(y)$.

(3) *any root* α *in* $\overline{\mathbb{Q}}_p$*—the algebraic closure of* $\mathbb{Q}_p$*—of* $F_i(x)$*, we have* $v_p(\alpha) = |\lambda_i|$.

Theorem 35 (Theorem of the residual polynomial)**.** *Let* f *and* ϕ *be as in the theorem of the polygon and let* S *be a side of* $N_\phi^-(f)$ *of slope* $\lambda \in \mathbb{Q}^-$*. Further let*

$$R_\lambda(f)(y) \sim \psi_1(y)^{e_1} \cdots \psi_t(y)^{e_t}$$

be the factorization of the residual polynomial into pairwise different monic irreducibles of $(\mathbb{F}_p[x]/\phi(x))[y]$*. Then, the third dissection for each factor* $F_k(x)$ *of* $f(x)$*, attatched to* ϕ*,* λ *by the theorem of the polygon, is given by the factorization*

$$F_k(x) = G_1(x) \cdots G_t(x)$$

into a product of monic polynomials such that $N_\phi(G_i)$ *is one sided with slope* λ *and*

$$R_\lambda(G_i)(y) \sim \psi_i(y)^{e_i}$$

for all $1 \leq i \leq t$*.*

Unfortunately, the three dissections of f given by Hensel's Lemma, the theorem of the polygon, and the theorem of the residual polynomial are not enough to guarantee that the final set of factors obtained are irreducible. Ore defined a polynomial to be *p-regular* if these three dissections gave a factorization into irreducibles. He also gave a non-constructive proof of the existence of a p-regular defining equation for every number field. He also suggested that higher Newton polygons could be introduced to continue the factorization into irreducibles. The next section does just this.

5. The Montes Algorithm

From the viewpoint of the Montes algorithm, the work of Ore represents level 1 of the algorithm. We proceed by induction as if the algorithm is true in levels $1, \ldots, n-1$ and develop the theorem of the product, the theorem of the polygon, and the theorem of the residual polynomial in level n. We introduce an invariant in the form of *higher order indices* which indicate when the algorithm terminates.

5.1. Types and representatives.

First, we introduce a data structure that parametrizes the list of factors found in the three dissections of the previous section.

Definition 36. A *type of order zero*, $\mathbf{t}$, is a monic irreducible polynomial

$$\mathbf{t} = \psi_0(y) \in \mathbb{F}[y]$$

with attached semigroup homomorphism

$$\omega_0 : \mathbb{Z}[x] \to \mathbb{Z}_{\geq 0}$$
$$P(x) \mapsto \ell(N_{\psi_0}^-(P)).$$

The intuition behind this definition is that we think of the factors of our original polynomial provided by Hensel's Lemma as the residual polynomials in the zero-th order. As we have seen, if this factorization of f is not irreducible, each of the factors splits according to the Theorem of the polygon.

Definition 37. A *type of order one* is a triplet $\mathbf{t} = (\phi(x); \lambda, \psi(y))$ where

(1) $\phi(x) \in \mathbb{Z}[x]$ is irreducible modulo p.
(2) $\lambda \in \mathbb{Q}^-$.
(3) $\psi(y) \in (\mathbb{F}_p[x]/\phi(x))\,[y]$ is a monic irreducible polynomial with $\psi(y) \neq y$.

We denote $\mathbf{t}_0(f)$ to be the set of all monic irreducible factors of $f(x)$ modulo p and denote $\mathbf{t}_1(f)$ to be the set of all types of order one obtained from the three classical dissections. Now, we are ready to recursively define types of arbitrary degree; in this definition, we implicitly assume we have access to the relevant data computed in the types of lower orders.

Definition 38. A *type of order* $n-1$ is a sequence of data

$$\mathbf{t} = (\phi_1(x); \lambda_1, \phi_2(x); \ldots; \lambda_{n-2}, \phi_{n-1}(x); \lambda_{n-1}, \psi_{n-1}(y)) \tag{5.1}$$

where the $\phi_i(x)$ are monic polynomials in $\mathbb{Z}[x]$, $\lambda_i \in \mathbb{Q}^-$, and $\psi_{n-1}(y)$ is a polynomial over a finite field such that $\mathbf{t}$ obeys the following properties:

(1) $\phi_1(x) \in \mathbb{Z}[x]$ is irreducible modulo p and $\psi_0(y)$ is the reduction of $\phi_1(y)$ modulo p in $\mathbb{F}[y]$. Define $\mathbb{F}_1 := \mathbb{F}[y]/(\psi_0(y))$.
(2) For all $1 \leq i < n-1$ the Newton polygon of i-th order, $N_i(\phi_{i+1})$, is one-sided with slope λ_i (we will define the Newton polygon of i-th order later).
(3) For all $1 \leq i < n-1$ the residual polynomial of i-th order (to be defined later), $R_i(\phi_{i+1})(y)$, is irreducible over $\mathbb{F}_i[y]$. For $\psi_i(y) \in \mathbb{F}_i$ the monic polynomial given by $R_i(\phi_{i+1})(y) \sim \psi_i(y)$; then we define

$$\mathbb{F}_{i+1} := \mathbb{F}_i[y]/(\psi_i(y)).$$

We continue with this notation for the rest of the paper so that $\mathbb{F}_n$ no longer refers to the field with n elements.
(4) ϕ_{i+1} has minimal degree among polynomials satisfying (2) and (3) for all $1 \leq i < n-1$.
(5) $\psi_{n-1}(y) \neq y \in \mathbb{F}_{n-1}[y]$ is a monic irreducible polynomial. We define $\mathbb{F}_n := \mathbb{F}_{n-1}[y]/(\psi_{n-1}(y))$.

Remark 39. A type of order $n-1$ determines a tower of finite fields

$$\mathbb{F} \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n.$$

Note that we may obtain a type of order i, $0 \leq i \leq n-1$, by the truncation

$$\mathrm{Trunc}_i(\mathbf{t}) := (\phi_1(x); \lambda_1, \phi_2(x); \ldots; \lambda_{i-1}, \phi_i(x); \lambda_i, \psi_i(y))$$

where

$$\mathrm{Trunc}_0(\mathbf{t}) := \psi_0(y).$$

With this definition, we have semigroup homomorphisms $N_i(-)$, $S_i(-)$, and $R_i(-)(y)$ such that for $P(x) \in \mathbb{Z}[x]$, $N_i(P)$ is the i-th order Newton polygon with respect to the type $\mathrm{Trunc}_i(\mathbf{t})$, $S_i(P)$ is the λ_i-side of $N_i^-(P)$, and $R_i(P)(y)$ is the residual

polynomial of i-th order with respect to λ_i. There is also the semigroup homomorphism

$$\omega_i : \mathbb{Z}[x] \to \mathbb{Z}_{\geq 0}$$
$$P(x) \mapsto \ell(N_i^-(P)).$$

For monic, separable $f(x) \in \mathbb{Z}[x]$, we say that a type $\mathbf{t}$ of order $n-1$ is *f-complete* if $\omega_n = 1$. In this case, the Newton polygon $N_{n-1}(f)$ is necessarily one-sided with degree one, so the $R_{n-1}(f)(y)$ is separable.

Notation 2. *We also introduce notation for the other data attached to a type of order $n-1$; for all $1 \leq i < n$ we have*

- $\lambda_i = -h_i/w_i$ *for* h_i,$w_i \in \mathbb{Z}_{>0}$ *coprime.*
- $f_i := \deg(\psi_i(y))$.
- $m_i := \deg(\phi_i(x))$. *Note* $m_{i+1} = m_i w_i f_i$.
- $\ell_i, \ell_i' \in \mathbb{Z}$ *are fixed integers such that* $\ell_i h_i - \ell_i' w_i = 1$.
- $z_i := y \mod \psi_i(y) \in \mathbb{F}_{i+1}^*$. *Note* $\mathbb{F}_{i+1} = \mathbb{F}(z_i)$.

We also define $f_0 := \deg(\psi_0(y)) = \deg(\phi_1(x))$, $z_0 := y \mod \psi_0(y) \in \mathbb{F}_1^*$, *and* $m_n := m_{n-1} w_{n-1} f_{n-1}$.

Definition 40. Let $\mathbf{t}$ be as in (5.1); then a monic polynomial $\phi_n(x) \in \mathbb{Z}[x]$ (suggestively notated) is said to be a *representative* of $\mathbf{t}$ if

- $\phi_n(x) \equiv \phi_1(x)^{a_0} \mod p$ for some $a_0 \in \mathbb{Z}_{>0}$.
- For all $1 \leq i \leq n-1$ the Newton polygon $N_i(\phi_n)$ is one-sided with slope λ_i and $R_i(\phi_n)(y) \sim \psi_i(y)^{a_i} \in \mathbb{F}_i[y]$ for some $a_i \in \mathbb{Z}_{>0}$.

The polynomial $\phi_n(x)$ in order $n-1$ plays the analogous role of an irreducible factor modulo p in order one. In [7], an explicit non-canonical representative of the type $\mathbf{t}$ is constructed recursively. We skip the construction in this thesis, but note the ϕ_n can be constructed with the following properties in terms of quantities from Notation 2:

$$\deg(\phi_n) = m_n, \quad \omega_n(\phi_n) = 1, \quad v_n(\phi_n) = w_{n-1} f_{n-1} v_n(\phi_{n-1})$$

where v_n is the valuation constructed in the next section. With this we may define $\mathbf{t}_n(f)$ to be all types of order n constructed from $\mathbf{t} \in \mathbf{t}_{n-1}(f)$ that are not f-complete.

5.2. **Valuations, Newton polygon, and residual polynomials in order n.** Before we define Newton polygons of higher order, we must construct an essential invariant of types of order $n-1$ in the form of a *discrete valuation*. We may generalize the idea of Definition 20 in the following way:

Definition 41. A *discrete valuation* on a field K is a map

$$v : K \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$$

such that for $a, b \in K$

(1) $v(a) = \infty$ if and only if $a = 0$.
(2) $v(ab) = v(a) + v(b)$.
(3) $v(a+b) \geq \min\{v(a), v(b)\}$.

We extend this as in Definition 20 to

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K(x)$$

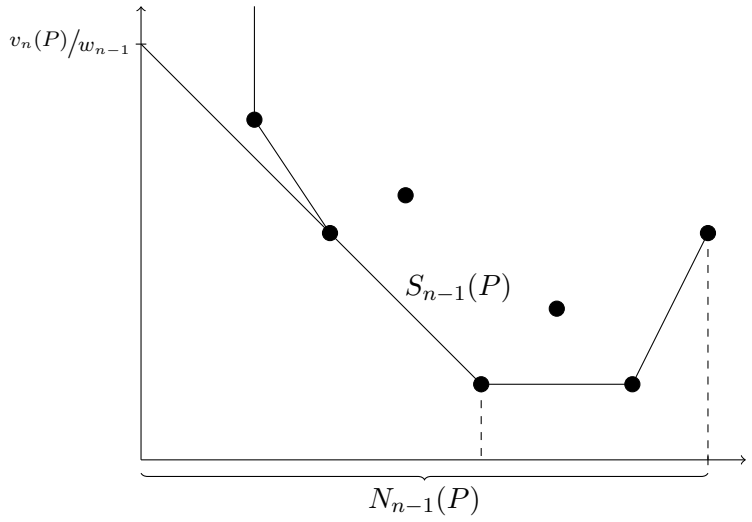
by defining $v : K(x) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ as

$$v(f(x)) = \min_{0 \leq i \leq n} \{v(a_i)\}.$$

The Montes algorithm constructs a discrete valuation in each order which has some nice properties.

Definition 42. Let $P(x) \in \mathbb{Z}[x]$; the *p-adic valuation of n-th order*, denoted v_n, attached to the type $\mathbf{t}$ in (5.1) is given by the geometric construction in Figure 7.

FIGURE 7



This discrete valuation was introduced by MacLane in [10] and [11]. Formally, we may define

$$H_{n-1} : S(\lambda_{n-1}) \to \mathbb{Z}_{\geq 0}$$

which maps a side $S \in S(\lambda_{n-1})$ to the intersection with the y-axis of the side S extended to a line. More precisely, if (s, μ) is the initial point of S, then

$$H_{n-1}(S) = \mu + |\lambda_{n-1}| s$$

so that $H_{n-1}(-)$ is a semigroup homomorphism. Now

$$v_n(P) := w_{n-1} H_{n-1}(S_{n-1}(P))$$

which is a semigroup homomorphism because it is the composition of three semigroup homomorphisms.

Definition 43. Let $\mathbf{t}$ be as in (5.1) with representative ϕ_n and $f(x) \in \mathbb{Z}[x]$ with ϕ_n-adic development

$$f(x) = \sum_i a_i(x)\phi_n(x)^i.$$

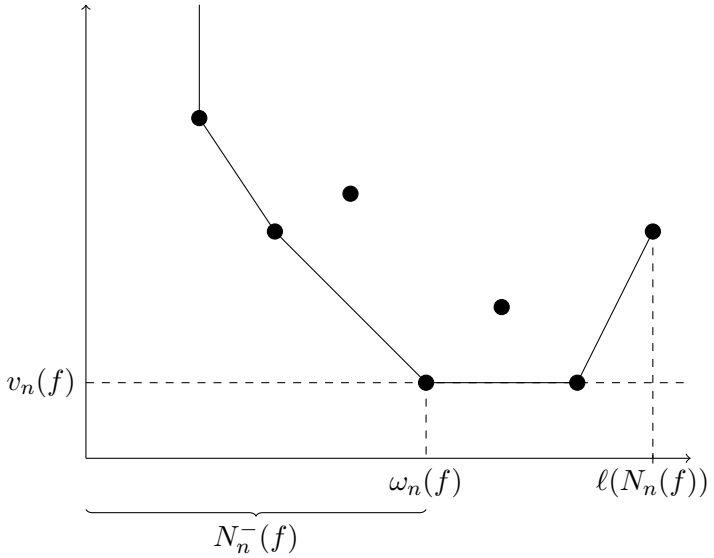
With our new discrete valuations in each order, we are able to define the *Newton Polygon in order* n, $N_n(f)$, as the lower convex envelope of the points

$$(i, v_n(a_i(x)\phi_n(x)^i) := (i, u_i).$$

The *principle part* $N_n^-(f)$ is the principle polygon constructed from the sides of negative slope.

Now that we have finally defined Newton polygons of higher order, we may update our general picture from order one in Figure 4 to the corresponding generic picture in level n (see Figure 8).

FIGURE 8. A generic Newton polygon in order n.



Before we can extract the coefficients of the residual polynomial in order n from $N_n^-(-)$, we must define the integer $t_{n-1}(i, f)$ for $f(x) \in \mathbb{Z}[x]$. We denote $(s_{n-1}(S), \mu_{n-1}(S))$ for the initial point of a side S; then

$$t_{n-1}(i, f) := \frac{s_{n-1}(S_{n-1}(f)) - \ell_{n-1}u_i}{w_{n-1}}.$$

Definition 44. Now, the *residual coefficients* encoded by the finite part of $N_n^-(f) := N$ for $0 \leq i \leq \omega_n$ are $c_i \in \mathbb{F}_n$ defined by

$$c_i := \begin{cases} 0 & \text{if } (i, u_i) \text{ lies strictly above } N \\ z_{n-1}^{t_{n-1}(i,f)} R_{n-1}(a_i)(z_{n-1}) & \text{if } (i, u_i) \text{ lies on } N. \end{cases}$$

As in order one, to the side $S_{n-1}(f) := S$ of N with initial point $s_{n-1}(S) := s$ we attach a residual polynomial $R_n(f)(y) := R_{\lambda_n}(f)(y)$ defined by

$$R_{\lambda_n}(f)(y) := c_s + c_{s+w}y + \cdots + c_{s+(d(S)-1)w}y^{d(S)-1} + c_{s+d(S)w}y^{d(S)} \in \mathbb{F}_n[y].$$

c_s and $c_{s+d(S)w}$ are non-zero by construction so in particular $y \nmid R_{\lambda_n}(f)(y)$.

Theorem 45 (Theorem of the product in order n)**.** *For any non-zero $f(x), g(x) \in \mathbb{Z}[x]$ and $\lambda_n \in \mathbb{Q}^-$*

$$N_n^-(fg) = N_n^-(f) + N_n^-(g)$$
$$R_{\lambda_n}(fg)(y) = R_{\lambda_n}(f)(y)R_{\lambda_n}(g)(y).$$

In particular, N_n^- and R_{λ_n} are semigroup homomorphisms.

Theorem 46 (Theorem of the polygon in order n)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $\omega_n(f) > 0$. Further, suppose $N_n^-(f) = S_1 + \ldots + S_g$ has g sides with slopes $\lambda_{n,1} < \cdots < \lambda_{n,g}$; then the sides of $N_n^-(f)$ determine a factorization of $f_{\boldsymbol{t}}(x)$ into monic polynomials*

$$f_{\boldsymbol{t}}(x) = F_1(x) \cdots F_g(x) \in \mathbb{Z}_p[x]$$

such that

(1) $N_n(F_i) = S_i$ up to translation.
(2) $\lambda_{n,i}$ finite implies $R_{\lambda_{n,i}}(F_i)(y) \sim R_{\lambda_{n,i}}(f)(y)$.
(3) any root $\alpha \in \overline{\mathbb{Q}}_p$ of $F_i(x)$, we have $v_p(\phi(\alpha)) = (v_n(\phi_n) + |\lambda_{n,i}|)/w_i \cdots w_{n-1}$.

Theorem 47 (Theorem of the residual polynomial in order n)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with $\omega_n(f) > 0$ and S be a side of $N_n^-(f)$ of slope $\lambda_n \in \mathbb{Q}^-$. Further let*

$$R_{\lambda_n}(f)(y) \sim \psi_{n,1}(y)^{e_1} \cdots \psi_{n,t}(y)^{e_t}$$

be the factorization of the residual polynomial into pairwise different monic irreducibles of $\mathbb{F}_n[y]$. Then, the factor $f_{\boldsymbol{t},\lambda_n}(x)$ of $f_{\boldsymbol{t}}(x)$ attached to the side S by the theorem of the polygon, is given by the factorization

$$f_{\boldsymbol{t},\lambda_n}(x) = G_1(x) \cdots G_t(x)$$

into a product of monic polynomials such that $N_n(G_i)$ is one sided with slope λ_n and

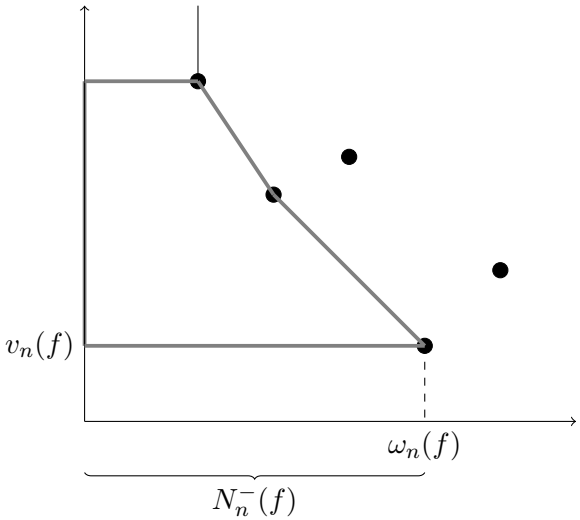
$$R_{\lambda_n}(G_i)(y) \sim \psi_{n,i}(y)^{e_i} \in \mathbb{F}_n[y]$$

for all $1 \le i \le t$.

5.3. **Indices.** We introduce an integer invariant in the form of *higher order indices* which regulate the Montes algorithm at each level along with the *theorem of the index* which guarantees the algorithm terminates in at most $\mathrm{ind}(f)$ steps. We can again interpret this invariant geometrically as combinatorial data associated to the principle polygon.

Definition 48. To a principle polygon, $N_n^-(f)$, in level $n-1$ associated to the type $\mathbf{t}$ in (5.1), we define $\operatorname{ind}(N_n^-(f))$ to be the number of integer lattice points in $N_n^-(f)$ with y-coordinate greater than or equal to $v_n(f)$ and less than or equal to maximum y coordinate on the finite part of the principle polygon (see Figure 9).

FIGURE 9. $\operatorname{ind}(N_n^-(f))$ is computed by counting the number of integer lattice points lying in (including the boundary) the demarcated region.



Then, we associate to the type $\mathbf{t}$

$$\operatorname{ind}_{\mathbf{t}}(f) := f_0 \dots f_{n-1} \operatorname{ind}(N_n^-(f)),$$

and define the index in level n for any $n \in \mathbb{Z}_{\geq 1}$ to be

$$\operatorname{ind}_n(f) := \sum_{\mathbf{t} \in \mathbf{t}_{n-1}(f)} \operatorname{ind}_{\mathbf{t}}(f).$$

This controls the Montes algorithm at each level, and the following theorem shows its important property.

Theorem 49 (Theorem of the index)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic, separable polynomial; then*

$$\operatorname{ind}(f) \geq \operatorname{ind}_1(f) + \dots + \operatorname{ind}_n(f)$$

where $\operatorname{ind}(f)$ *is the standard p-adic valuation of $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. Equality holds if and and only if* $\operatorname{ind}_{n+1}(f) = 0$*, and thus we see that as a by product, $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]])$ is computed when the algorithm terminates.*

References

[1] Matthew Baker. Algebraic number theory course notes, 2006.

[2] R. Dedekind. Üeber den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen. *Abhandlungen der Kniglichen Gesellschaft der Wissenschaften in Gottingen*, 23:3–38, 1878.

[3] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley and Sons, second edition, 1999.

[4] Harold M. Edwards. Dedekind's invention of ideals. *Bull. London Math. Soc.*, 15(1):8–17, 1983.

[5] David Ford, Sebastian Pauli, and Xavier-François Roblot. A fast algorithm for polynomial factorization over $\mathbb{Q}_p$. *J. Théor. Nombres Bordeaux*, 14(1):151–169, 2002.

[6] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théor. Nombres Bordeaux*, 23(3):667–696, 2011.

[7] Jordi Guàrdia, Jesús Montes, and Enric Nart. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.*, 364(1):361–416, 2012.

[8] Jordi Gurdia, Jess Montes, and Enric Nart. Higher newton polygons and integral bases. *Journal of Number Theory*, 147:549 – 589, 2015.

[9] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[10] Saunders MacLane. A construction for absolute values in polynomial rings. *Trans. Amer. Math. Soc.*, 40(3):363–395, 1936.

[11] Saunders MacLane. A construction for prime ideals as absolute values of an algebraic field. *Duke Math. J.*, 2(3):492–510, 1936.

[12] Jesús Montes. *Polígonos de Newton de orden superior y aplicaciones aritméticas,*. PhD thesis, Universitat de Barcelona, 1999.

[13] Ø. Ore. Newtonsche polygone in der theorie der algebraischen körper. *Mathematische Annalen*, 99:84–117, 1928.

[14] Sebastian Pauli. Factoring polynomials over local fields. *J. Symbolic Comput.*, 32(5):533–547, 2001.

[15] Olga Erzsebet Veres. *On the complexity of polynomial factorization over p-adic fields*. ProQuest LLC, Ann Arbor, MI, 2009. Thesis (Ph.D.)–Concordia University (Canada).

Department of Mathematics, University of Colorado, Campus Box 395, Boulder, Colorado 80309-0395

E-mail address: Ryan.Ibarra@Colorado.edu