Factoring Polynomials Modulo Composites

Adam Klivans

May 8, 1997

Abstract

This paper characterizes all the factorizations of a polynomial with coefficients in the ring Z_n where n is a composite number. We give algorithms to compute such factorizations along with algebraic classifications.

Contents

1 Introduction

This paper attempts to understand the computational and algebraic differences between polynomials over a field and polynomials over a ring. Polynomials over a field are well understood. Many important polynomial time algorithms in computational algebra have been developed by taking advantage of the underlying field structure. In the case where the polynomials are over a ring, however, very little seems to be known. In this paper we try to understand the algebraic and computational complexity of polynomials over the ring of the integers modulo n where n is a composite. In particular, we will attempt to compute and characterize all factorizations of a univariate polynomial into irreducibles. Perhaps understanding this polynomial ring will lead to a deeper understanding of the computational limits of circuits as well as faster algorithms in computational algebra. In the course of our discussion we will point out the many differences between working over fields versus over rings to illustrate the severity of the existing gap.

1.1 Circuit complexity theory

A motivation for this study comes from circuit complexity theory which is the study of determining the hardness (or relative ease) of a given problem by analyzing the circuits that represent it. A circuit can be thought of as a directed acyclic graph where the nodes are called gates. The edges leading into a node can be thought of as inputs, and the edges leaving a node carry the output of that gate on its given inputs. For the purposes of this paper, we are concerned only with boolean circuits, namely each input can take on a value equal to either 0 or 1. The nodes with zero in-degree should be thought of as inputs. When the inputs are set to some initial vector, the values will trickle through the circuit producing 1 or more output values.

Now it is clear how a circuit could be used to decide membership in an arbitrary set. We say that a circuit decides membership in a set S if for every candidate encoded in zeros and ones, our circuit outputs a '1' on that input if and only if the candidate is in S.

In this context, we wish to think of a family of circuits, one for each different input length. We can also measure the depth of a circuit in the obvious way. A family of circuits has constant depth if each circuit in the family has depth at most k regardless of the length of the input. This model of computation has lead to many interesting results such as the fact that the *parity function* cannot be computed by polynomial size constant depth circuits [FSS84]. We can make this model even more interesting by allowing gates other than simply AND, OR, and NOT. In fact, it is known that constant depth circuits which have MOD_p gates cannot compute the MOD_q function for any q that is not a power of p. What is the computational signifigance of having MOD_n gates where n is a composite?

We further restrict our model of computation to polynomials which represent boolean functions. We say that a polynomial f in n variables represents the OR function if, when restricted to inputs of 0's and 1's,

1. $f(x_1 \dots x_n) \neq 0$ when $x_i = 1$ for some $i \leq n$.
2. $f(x_1 \dots x_n) = 0$ when $x_i = 0$ for all $i \leq n$.

We measure the complexity ofpolynomial f by its degree. Recall the degree of a multivariate polynomial is the maximum over all monomials of the sum of the powers of the indeterminates in that monomial. It is known that for polynomials over a field (namely over the integers mod p) the lowest degree polynomial representing the OR function on N variables has degree $\lceil N/(p-1) \rceil$ [Smo87]. However, the bounds on the degree of a polynomial over a ring (the integers mod n) are not as precise. The best known lower bound on the degree of a polynomial representing the OR function mod n is $\Omega(\log N)$ [TB94], and fairly recently a surprising upper bound of $\mathrm{O}(N^{1/r})$ where r is the number of distinct primes dividing n was discovered [BBR94]. In [BBR94] we learn that a low a degree polynomial for OR would imply the existence of small, low-depth mod n circuits for the AND function.

2 Some Important Tools in $Z_n[x]$

2.1 The $Z_n[x]$ phenomena

Definition 2.1 *Let Z denote the ring of integers and Z_n Z/nZ the ring of integers modulo n.*

Definition 2.2 *Let $Z_n[x]$ denote the ring of polynomials with coefficients from Z_n.*

We first examine a few instances of weirdness in the ring $Z_n[x]$ with a few examples. The presence of zero divisors in the following rings allows for very strange constructions. Amazingly, for example, the polynomial x is not necessarily irreducible in $Z_n[x]$! In particular we can write the following factorization:

$$x \equiv (4x+3)(3x+4) \bmod 6$$

Here a congruence $f \equiv g \bmod n$ between polynomials means that $f - g$ has all coefficients congruent to 0 mod n. We show later how to prove that this is a factorization into irreducibles. Also note that

$$x^2 + 7 \equiv (x+1)(x+7) \equiv (x+3)(x+5) \bmod 8$$

All four factors above are in fact irreducible, and so there is no unique factorization in the composite case. We turn next to the first important tool needed here: the Chinese Remainder Theorem.

2.2 The Chinese Remainder Theorem

Theorem 2.3 *Let R be a commutative ring with identity. Let $A_1, A_2 \ldots A_k$ be ideals in R. Then the map $R \to R/A_1 \times R/A_2 \times \ldots \times R/A_k$ defined by $r \mapsto (r+A_1, r+A_2, \ldots, r+A_k)$ is a ring homomorphism with kernel $A_1 \cap \ldots \cap A_k$. If the ideals are pairwise comaximal (i.e., for each $i, j \in \{1, 2, \ldots k\}$ we have $A_i + A_j = R$), then the map is surjective, and we may assert*

$$R/(A_1 A_2 \cdots A_n) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

(A proof can be found in any abstract algebra book, for example [DF90].) In particular we may take R to be $Z_n[x]$ and its corresponding comaximal ideals to be the ideals $Z_{{p_i}^k}[x]$ for each prime factor p_i dividing n where $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. This gives us a nicer representation for polynomials in $Z_n[x]$. For a given $f \in Z_n[x]$, we can write f as the following tuple:

$$f = (f_1, f_2, \ldots, f_s)$$

where f_i equals f mod $p_i^{k_i}$. Operations on these tuples are pointwise, since the mapping is an isomorphism. From this, we see that an irreducible factor g of f corresponds to the following tuple:

$$(1, 1, \ldots, g_i, \ldots, 1, 1)$$

where g_i is irreducible mod $p_i^{k_i}$. Clearly no two tuples can multiply together to result in g since g_i is irreducible. Thus, every factorization in R must produdce products of tuples of the above form. We ignore units for the time being since they only trivially modify the above factorizations. This discussion gives us an immediate corollary:

Corollary 2.4 [vzGH96a] *Let $f \in Z_n[x]$ and $n = \prod_{1 \le i \le s} p_i^{k_i}$. The number of irreducible factors of $f \in Z_n[x]$ is the sum of the number of irreduicble factors of $f_i \in Z_{p_i^{k_i}}[x]$.*

We show given a factorization into these tuples how we can reconstruct a factorization in $Z_n[x]$.

Proposition 2.5 *Given $Z_n[x] \cong Z_{p_1^{k_1}}[x] \times \ldots \times Z_{p_s^{k_s}}[x]$ and $f_1 \cdots f_n$ a factorization of f into irreducibles where each f_i has the tuple form above, we can reconstruct a factorization in $Z_n[x]$ in polynomial time.*

Proof: Let $f_i = (g_1, g_2, \ldots, g_s)$. Let Coeff($h$,$i$) denote the coefficient of the ith power in the polynomial h.Let M be the degree of the largest polynomial in f_i. More precisely, we look at all the polynomial entries in the s-tuple for f_i and let M be the degree of the highest degree polynomial entry. Let ${f_i}^{(k)}$ denote the kth entry in the s-tuple corresponding to f_i. The corresponding coefficient of each power of x in f_i's representation in $Z_n[x]$ can be reconstructed by looking at its coefficient in each entry of f_i's s-tuple in the following manner.

$$f_i = \sum_{j=0}^{M} \mathrm{CRT}(f_i, j) x^j$$

where $\mathrm{CRT}(f_i, j)$ denotes the solution to the following set of equations:

$$\begin{aligned}
y &= \mathrm{Coeff}({f_i}^{(1)}, j) \bmod p_1^{k_1} \\
y &= \mathrm{Coeff}({f_i}^{(2)}, j) \bmod p_2^{k_2} \\
&\vdots \\
y &= \mathrm{Coeff}({f_i}^{(s)}, j) \bmod p_s^{k_s}
\end{aligned}$$

This can be calculated using the Chinese Remainder Theorem. The notation is complicated but the idea is simple. Given an s-tuple representing a polynomial, we can reconstruct its representation in $Z_n[x]$ by applying the Chinese Remainder Theorem coordinatewise. ■

With this result in hand, we can show that factoring polynomials in $Z_n[x]$ is quite difficult.

Theorem 2.6 [Sha93] *There is a polynomial time reduction from factoring integers to factoring polynomials in $Z_n[x]$*

Proof: Given some $n \in Z$ we attempt to factor it by examining the polynomial $f = x$ over $Z_n[x]$. Let $n = (-1)^k p_1^{k_1} \cdots p_s^{k_s}$. Recall that from the Chinese Remainder Theorem, f has an equivalent form as the s-tuple $(x, x, \ldots, x, x)$. Assume that we can factor f into irreducibles so that (up to a unit) we have

$$f = f_1 f_2 \cdots f_s$$

where each f_i is irreducible thus having the form

$$f_i = (1, 1, \ldots, 1, x, 1, \ldots, 1)$$

where x is in the ith position. So over Z_n, each f_i is of the form $a_i x + b_i$ mod n with a_i,$b_i \in Z$ and so

$$b_i \equiv \begin{cases} 0 \bmod p_i^{k_i} & \\ 1 \bmod p_j^{k_j} & \text{for } i \neq j \end{cases}$$

Thus the $\gcd(n, b_i) = p_i^{k_i}$ for $1 \leq i \leq s$. So our factorization of x immediately gives us a factorization $m_1 m_2 \cdots m_n$. We need only figure out the prime and exponent for each m_i. Assume that $m_i = p_i^{k_i}$. Then k_i is bounded by $\lceil \log m_i \rceil$. We can take jth roots where j varies from 2 to $\lceil \log m_i \rceil$. If none of the jth roots are in Z, we know m is prime. If one of the jth roots is in Z we can repeat the procedure on the result until a prime is reached and then easily reconstruct the exponent. Since the size of the exponent is logarithmic in m this a polynomial time procedure. Thus, the existence of a polynomial time algorithm to factor in $Z[x]$ is unlikely. (Compare this with the many randomized polynomial time algorithms (See [Ber70]) to factor in $F[x]$ where F is a field to see the contrast between rings and fields.) ∎

2.3 Irreducibility criteria in $Z_{p^k}[x]$

The Chinese Remainder Theorem reduces the problem to working over rings of the form $Z_{p^k}[x]$. Let $r = p^k$ from now on. We would like to determine what factors of a polynomial are actually irreducible. We establish some criterion to determine if a polynomial in $Z_{p^k}[x]$ is irreducible. A nice observation is the following:

Proposition 2.7 *Given an $f \in Z_{p^k}[x]$ not equal to* $0 \bmod p$ *we can write f as $f' + pg$ where p does not divide f'.*

Proof: Let

$$f = \sum_{i=0}^{n} (p^{j(i)} + a_i)x^i$$

where each $a_i < p$ and $j(i) < k$. From this we see

$$f = \underbrace{\sum_{i=0}^{n} p^{j(i)}x^i}_{pg} + \underbrace{\sum_{i=0}^{n} a_i x^i}_{f'}$$

■

Now we can deduce the following remark:

Proposition 2.8 *Let $f \in Z_{p^k}[x]$ not equal to $0 \bmod p$. If f is irreducible in $Z_p[x]$ then f is irreducible in $Z_{p^k}[x]$ for all $k \geq 1$.*

Proof: Assume f is reducible in Z_{p^k} for some k. Then $f \equiv gh \bmod p^k$ and using the above observation, $f \equiv (g_1 + pg_2)(h_1 + ph_2) \bmod p$. Hence, $f \equiv g_1 h_1 \bmod p$ contradicting irreducibility mod p. ■

This formula also gives a characterization of all the units in $Z_n[x]$.

Proposition 2.9 *Let $f \in Z_{p^k}[x]$ such that $f \neq 0 \bmod p$. Then f is a unit in $Z_{p^k}[x]$ if and only if f is of the form $a + pg$ where $a \in Z_p$.*

Proof: Every polynomial f can be written in the form $f_1 + pf_2$ where we have $\gcd(f_1, p) = 1$. Assume f is a unit and assume f_1 has degree ≥ 1. Since f is a unit, there exists $h = (h_1 + ph_2)$ such that $fh = 1$. This implies

$$f_1 h_1 + p((f_2 h_1 + f_1 h_2) + pf_2 h_2) = 1 + p \cdot 0$$

But f_1 has degree strictly bigger than 0, and both $gcd(f_1, p) = 1$ and $gcd(h_1, p) = 1$. Thus the monomial of highest degree in f_1 cannot have cancelled out. So $f_1 h_1$ could not possibly be the constant polynomial 1. Hence for f to be a unit, it must be of the above form.

If $f = a + pg$ where $a \in Z_p$ then $f = (1 - a^{-1}(-p)g)$. The following familiar identity is helpful:

$$\frac{1}{1-h} = 1 + h + h^2 + \cdots +$$

and thus

$$f^{-1} = 1 + a^{-1}(-p)g + (a^{-1}(-p)g)^2 + \cdots (a^{-1}(-p)g)^{k-1}$$

Notice that after the $k-1$ term, all of the terms have a factor of p^k in them which zero out. Our inverse is thus a well defined element of $Z_{p^k}[x]$. ■

This also tells us that if $f \bmod p$ is a unit, then $f \bmod p^k$ is a unit for all $k \geq 1$.

2.4 Hensel's Lemma

In order to further our analysis of irreducibility as well as develop a method of factorization, we introduce the most important mathematical tool of the paper:

Theorem 2.10 [Hensel's Lemma] *Let p be a prime, $k \geq 1$, and let f, g, $h \in Z[x]$ such that $f \equiv gh \not\equiv 0 \bmod p$ and $gcd(g \bmod p, h \bmod p) = 1$ in $Z_p[x]$. Then there exist polynomials $\tilde{g}$ and $\tilde{h}$ such that $f \equiv \tilde{g}\tilde{h} \bmod p^k$ with $\tilde{g} \equiv g \bmod p, \tilde{h} \equiv h \bmod p$.*

Proof: **[BS96]** We give an algorithm to construct g' and h' and prove its correctness.

Step 1. Find λ and $\mu \in Z_p[x]$ such that $\lambda g + \mu h = 1$. (We know such λ and μ exist since g and h are relatively prime. We can find them easily by using the Extended Euclidean Algorithm for polynomials.)

Step 2. Iteratively construct polynomials g' and h' according to the following for loop:

for $\boldsymbol{i = 2}$ to $\boldsymbol{k}$ do

$$\begin{aligned} &\boldsymbol{q := (f - gh)/(p^{i-1}) \bmod p} \\ &\boldsymbol{u := q\mu \bmod g} \\ &\boldsymbol{v := q\lambda \bmod h} \\ &\boldsymbol{g := g + p^{i-1}u} \\ &\boldsymbol{h := h + p^{i-1}v} \end{aligned}$$

end

Return$\boldsymbol{(g' = g, h' = h)}$

The proof of correctness is by induction on i. Assume that $f \equiv gh \bmod p^{i-1}$ (g and h are also monic). Notice that the construction of q makes sense since $f - gh \equiv 0 \bmod p^{i-1}$. We need only check that $(g+p^{i-1}u)(h+p^{i-1}v) \equiv f \bmod p^i$. Hence, we have

$$\begin{aligned}(g+p^{i-1}u)(h+p^{i-1}v) &\equiv gh+p^{i-1}(uh+vg)+p^{2i-2}uv \bmod p^i \\ &\equiv gh+p^{i-1}(uh+vg) \bmod p^i\end{aligned}$$

but notice

$$\begin{aligned}uh+vg &\equiv uh \bmod g \\ &\equiv q\mu h \bmod g \\ &\equiv q(1-\lambda g) \bmod g \\ &\equiv q \bmod g\end{aligned}$$

Similarly we can see that $uh+vg \equiv q \bmod h$. Since h and g are coprime, by the Chinese Remainder Theorem we see that $uh+vg=q$. Hence in our original equation we have

$$\begin{aligned}(g+p^{i-1}u)(h+p^{i-1}v) &\equiv gh+p^{i-1}q \bmod p^i \\ &\equiv f \bmod p^i\end{aligned}$$

Thus $\tilde{g}=(g+p^{i-1}u)$ and $\tilde{h}=(h+p^{i-1}v)$ are as required.

■

From Proposition 2.8, if g and h are irreducible then $\tilde{g}$ and $\tilde{h}$ are irreducible. Now we can show why we only care about monic polynomials.

Corollary 2.11 *Let $f \in Z_{p^k}[x]$ with $k \geq 1$. Finding the irreducible factors of f reduces to the case where f is monic.*

Proof: **[vzGH96a]** We can write f as $p^v g$ where gcd(p,g) $=1$. Then $g \equiv e_0 m_0 \bmod p$ where e_0 is a unit mod p and thus mod p^k. Since gcd(e_0,m)$=1$, we can use Hensel's Lemma to find a lifting such that $g \equiv em \bmod p^{k-v}$ where $e \equiv e_0 \bmod p$ and $m \equiv m_0 \bmod p$ where m is monic. But since we have factored out p^v from f, every factorization of f corresponds to a factorization of $g \bmod p^{k-v}$. Thus we need only look at the irreducible factors of p^v (which are trivial) and the irreducible factors of m up to units, but m is monic. Hence, we need only consider monic polynomials from now on. ■

Now it is somewhat clearer as to how to go about finding one factorization of a polynomial mod n. We first look at the irreducible factors of f mod

p and use Hensel's Lemma for each factor and for each prime divisor of n. Then we reconstruct the factorization mod n using the Chinese Remainder Theorem. This leaves us with two important questions. First, what happens if $f \equiv g^k \bmod p$ for some irreducible g (i.e., how do we lift in this case)? Secondly, how do we compute *all* the different factorizations of f?

2.5 A naive approach to factoring

At some point, all known methods for computing all of the factorizations of a polynomial require solving a system of linear equations. We will illustrate this by constructing an extremely poor factoring algorithm. Assume we want to compute all the factorizations of a polynomial $f \in Z[x] \bmod p^k$. Let us also assume that we are not interested in factorizations where any given factor has degree greater than or equal to the given polynomial. One way to do this is to solve a complicated system of equations (via the method of undetermined coefficients) with the knowledge that every factorization mod p^k corresponds to a unique factorization mod p. For example:

Example 2.12 *Let $f \in Z[x]$ where $f \equiv gh \bmod p$. We wish to compute all the factorizations of $f \bmod p^2$. Assume that f factors mod p into linear polynomials so that $g = g_0 + g_1 x$ and $h = h_0 + h_1 x$.*

Now notice that all factorizations mod p^2 must satisfy the following system of equations:

$$f \equiv (g + pG)(h + pH) \bmod p^2$$

where G and H are some unknown linear polynomials $\in Z_p[x]$. Then let $G = G_0 + G_1 x$ and $H = H_0 + H_1 x$. Expanding the above equation gives us $f \equiv gh + p(H_0 g_0 + H_1 g_0 x + H_0 g_1 x + H_1 g_1 x^2 + G_0 h_0 + G_1 h_0 x + G_0 h_1 x + G_1 h_1 x^2) + p^2(\dots) \bmod p^2$

Since we are working mod p^2 the last term drops out. We only need the coefficient of the p term to be zero for our factorization to work out properly. Hence we need

$$\begin{aligned} G_1 h_1 + H_1 g_1 &\equiv 0 \bmod p \\ G_1 h_0 + H_1 g_0 + H_0 g_1 + G_0 h_1 &\equiv 0 \bmod p \\ H_0 g_0 + G_0 h_0 &\equiv 0 \bmod p \end{aligned}$$

Notice that h_0, h_1, g_0, g_1 are fixed values since we compute the factorization of $f \bmod p$. Hence, we have a system of linear equations which can be solved rather easily. This approach begins to break down as we need to factor moduo larger powers of p as well as if we need to compute factors with larger degrees. The next section will give us a better approach to this process.

3 The Case of Small Discriminants

The problem of computing all factorizations of a polynomials can be divided into two radically different cases. The case when the discriminant is small requires important properties of the p-adic numbers. Abstractly, every factorization mod p^k of a polynomial whose discriminant is 'small' corresponds to a unique factorization over the p-adics. Thus, with a factorization from the p-adics our problem is greatly simplified as we shall see. We follow development partially outlined in [vzGH96a].

3.1 The p-adic numbers

Kurt Hensel invented the p-adic numbers in the early twentieth century in order to solve number theoretic problems. Since then they have been an important tool in both analysis and algebra for many different problems. We give some brief introductory material for concreteness concerning the p-adics (see [BS66] for a complete treatment of this material).

Definition 3.1 *Fix some prime p. A p-adic number, denoted $\{x_n\}$, is a sequence of integers satisying*

$$x_n \equiv x_{n-1} \bmod p^n.$$

Two sequences $\{x_n\}$ and $\{x'_n\}$ determine the same p-adic integer if and only if

$$x_n \equiv x'_n \bmod p^{n+1}.$$

It is easy to see that each p-adic integer has the following canonical form:

$$\{x_n\} = \{a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \dots\}$$

where each $a_i \in \{0 \dots p-1\}$. Let $Z_{(p)}$ denote the ring of p-adic integers where the addition and multiplication operations are performed coordinate-wise. It easy to see that for $x, y \in Z_{(p)}, xy$ and $x+y$ are p-adic integers and so our ring is well defined. We will introdce the more conventional notation for a p-adic integer, namely an infinite sum of the form $\alpha = \sum_{i \geq 0} p^i \alpha_i$ where $\alpha_i \leq p$ for all i later in this section. We now aim to show a fairly simple property, namely that

$Z_{(p)}[x]$ are a unique factorization domain. Compare this with earlier examples that show $Z_{p^k}[x]$ is not a UFD. The following theorem can be found in any book on abstract algebra:

Theorem 3.2 *If a ring R is a UFD then R[x] is a UFD*

Lemma 3.3 *If a p-adic integer* $\{x_n\}$ *is a unit then* $x_0 \neq 0 \bmod p$.

Proof: If $\{x_n\}$ is a unit then there exists a $\{y_n\}$ such that $\{x_n y_n\} = 1\ \forall n$. In particular $x_0 y_0 \equiv 1 \bmod p$ Hence x_0 must be relatively prime to p. ■

Theorem 3.4 *Every p-adic integer, distinct from zero, has a unique representation in the form* $\alpha = p^k \varepsilon$ *where* ε *is a unit.*

Proof: **[BS66]** Let $\alpha \in Z_{(p)}$. Then if α is a unit, take $k = 0$. If α is not a unit then let k be the smallest index for which

$$x_k \neq 0 \bmod p^k$$

From the definition of p-adic numbers, $x_{k+s} \equiv x_{k-1} \equiv 0 \bmod p^k$. Let $y_s = \frac{x_{k+s}}{p^k}$ for all $s \geq 0$. Notice that

$$p^k y_s - p^k y_{s-1} = x_{k+s} - x_{k+s-1} \equiv 0 \bmod p^{k+s}$$

and thus

$$y_s \equiv y_{s-1} \bmod p^s$$

Hence, $\{y_s\}$ determines p-adic unit. Clearly $\{x_n\} = p^k\{y_s\}$. ■

Theorem 3.5 $Z_{(p)}$ *is a UFD.*

Proof: Consider some $\alpha \in Z_{(p)}$. Then from Theorem 3.4, $\alpha = p^k \varepsilon$ for some unit ε. Hence, $\alpha = \underbrace{p \cdots p}_{\text{k times}}\ \varepsilon$. But p is trivially irreducible, so this could be the only factorization up to units. Hence, $Z_{(p)}$ is a UFD. ■

From Theorem 3.2, $Z_{(p)}[x]$ is a UFD. Now that we have established that $Z_{(p)}[x]$ is a UFD, we need to determine the relationship between factorizations in $Z_{(p)}[x]$ and factorizations in $Z_{p^k}[x]$. (This is done in **Section 3.3**) To do this we introduce a non-archimidean metric as well as an alternate way of viewing p-adic numbers.

Definition 3.6 *A metric δ is called non-archimidean if and only if*

$$\delta(x+y) \leq \max(\delta(x), \delta(y))$$

Definition 3.7 *We define the function v_p by the following equation*

$$v_p(a) \equiv \begin{cases} \nu & \textit{if } a \neq 0 \textit{ and } p^\nu \textit{ is the largest power of } p \textit{ dividing } a \\ \infty & \textit{if } a = 0 \end{cases}$$

The function v_p is usually called a *valuation*. It is easy to see that the function $p^{-v_p(a)}$ defines a non-archimidean metric on the p-adic integers. Let δ_p represent this p-adic metric.

With this metric in hand, we can form a more convenient representation of a p-adic integer. For any $\alpha = (\alpha_1, \alpha_2, \dots) \in Z_{(p)}$ we can write α as the following sum:

$$\alpha = \sum_{i \geq 0} \beta_i p^i$$

where $\beta_i = \alpha_i - \alpha_{i-1}$ and $\beta_0 = \alpha_0$. Normally, this series would diverge, but with our p-adic metric, larger powers of p result in smaller values from the p-adic metric. Let S_n denote the sum of the first n terms of α. Then $\delta_p(S_n) = \frac{1}{p^n}$. Hence our sum converges and our representation for α is well defined.

3.2 Resultants

Recall that in order to use Hensel's Lemma to lift a factorization of some polynomial f, we require f to have a factorization into a product of at least two relatively prime polynomials mod p. We would like to be able to detect the 'difficult' cases where f is a power of a single irreducible polynomial mod p. The following material is outlined in [CLO92]. For an excellent description of how resultants, discriminants, and polynomial greatest common divisors are computed, see [Akr89].

Lemma 3.8 *Let $f, g \in Z[x]$ be polynomials of degrees $l > 0$ and $m > 0$ respectively. Then f and g have a common factor if and only if there are polynomials $A, B \in Z[x]$ such that*

1. *A and B are not both zero*
2. *A has degree at most $m - 1$ and B has degree at most $l - 1$*
3. *$Af + Bg = 0$.*

Proof: **[CLO92]** Assume f and g have a common factor $h \in Z[x]$. Then $f = hf_1$ and $g = hg_1$ where $f_1, g_1 \in Z[x]$. We see

$$g_1 f + (-f_1)g = g_1 h f_1 - f_1 h g_1 = 0.$$

$A = g_1$ and $B = -f_1$ are as required. Now assume that polynomials A and B have the three above properties. By $(1), B \neq 0$. Proceed by contradiction and assume that f and g have no common factor. Then they are relatively prime and we can find polynomials A' and B' such that $A'f + B'g = 1$. Multiplying by B and keeping in mind the fact that $Bg = -Af$ we see that

$$\begin{aligned} B &= (A'f + B'g)B \\ &= A'Bf + B'Bg \\ &= A'Bf - B'Af \\ &= (A'B - B'A)f \end{aligned}$$

But B is nonzero and from the last equation must have degree at least that of f, namely l. This contradicts (2). Hence, f and g must have a common factor of positive degree. ■

Now given f and g we would like to see if we can compute such an A and B to determine if they do indeed have a common factor. This problem reduces to solving the following system of linear equations. Let

$$A = c_0 x^{m-1} + \cdots + c_{m-1}$$

$$B = d_0 x^{l-1} + \cdots + d_{l-1}$$

where the coefficients of the polynomials should be thought of as unknowns. We want to find a solution such that the equation $Af + Bg = 0$ holds. To do this we can also write out f and g

$$f = a_0 x^l + \cdots + a_l, a_0 \neq 0$$

$$g = b_0 x^m + \cdots + b_m, b_0 \neq 0$$

substituting appropriately we achieve the following rather large system of linear equations:

$$\begin{array}{llllll}
a_0 x_0 & + & b_0 d_0 & & = 0 & \text{coefficient of } x^{l+m-1} \\
a_1 c_0 + a_0 c_1 & + & b_1 d_0 + b_0 d_1 & & = 0 & \text{coefficient of } x^{l+m-2} \\
\ddots & & \ddots & & \vdots & \vdots \\
& a_l c_{m-1} & + & b_m d_{l-1} & = 0 & \text{coefficient of } x^0.
\end{array}$$

This is an appropriate time to introduce the Sylvester Matrix.

Definition 3.9 *Given polynomials f, g as above, the Sylvester matrix of f and g is the coefficient matrix of the above system of equations. We denote this Sylvester matrix as $S(f, g)$ by the following $(l+m) \times (l+m)$ matrix*

$$S(f,g) = \left(\begin{array}{ccccccc}
a_l & & & & b_m & & \\
a_{l-1} & \ddots & & & b_{m-1} & \ddots & \\
\vdots & & \ddots & & \vdots & & b_m \\
a_0 & & & a_l & \vdots & & b_{m-1} \\
& \ddots & & a_{l-1} & b_0 & & \vdots \\
& & \ddots & \vdots & & \ddots & \vdots \\
& & & a_0 & & & b_0 \\
\multicolumn{4}{c}{\underbrace{\hphantom{a_{l-1}\quad\ddots\quad\ddots\quad a_{l-1}}}_{l}} & \multicolumn{3}{c}{\underbrace{\hphantom{b_{m-1}\quad\ddots\quad b_{m-1}}}_{m}}
\end{array} \right) \in R^{(l+m)\times(l+m)}$$

the empty spaces are filled by zeros. The Sylvester matrix is the coefficient matrix of the above system of equations. The **resultant** *of f and g with respect to x denoted $Res(f, g)$ is the determinant of the Sylvester matrix. Hence,*

$$Res(f, g) = det(S(f, g))$$

An immediate result of the preceding discussion is the following proposition:

Proposition 3.10 *Given $f, g \in Z[x]$ of positive degree, the resultant $Res(f,g) \in Z$ is an integer polynomial in the coefficients of f and g. Furthermore, f and g have a common factor $\in Z[x]$ if and only if $Res(f,g) = 0$.*

Proof: **[CLO92]** The resultant is zero $\Leftrightarrow$ the coefficient matrix of equations has zero determinant $\Leftrightarrow$ the system of equations has a nonzero solution. ■

Another important consequence of resultants is the following proposition:

Proposition 3.11 *Given $f, g \in Z[x]$ of positive degree, there are polynomials $A, B \in Z[x]$ such that $Af + Bg = Res(f,g)$.*

Proof: We have previously analyzed a case where we were searching for a solution to the equation $Af + Bg = 0$. Now we analyze the case where we want a solution to the equation $A'f + B'g = 1$. We form the following similar system of equations:

$$\begin{array}{llllll}
a_0x_0 & + & b_0d_0 & & = 0 & \text{coefficient of } x^{l+m-1} \\
a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & & = 0 & \text{coefficient of } x^{l+m-2} \\
\ddots & & \ddots & & \vdots & \vdots \\
& a_lc_{m-1} & + & b_md_{l-1} & = 1 & \text{coefficient of } x^0.
\end{array}$$

Cramer's rule can be used to solve this system of equations resulting in the following solution (the details are worked out in CLO).

$$A' = \frac{1}{Res(f,g)} A$$

$$B' = \frac{1}{Res(f,g)} B$$

Multiplying through by Res(f,g) we see that

$$Af + Bg = Res(f,g)$$

■

To summarize, given $f, g \in Z[x]$ the $Res(f,g) \neq 0$ if and only if f and g are coprime. We also know that we can find polynomials A and B such that $Af + Bg = Res(f,g)$. Furthermore, for any polynomial $h \in Z[x]$ with deg(h)$< l + m$ there exist uniquely determined polynomials A and B such that $res(f,g)h = Af + Bg$. The uniqueness of A and B comes from the fact that h has degree less than $l + m$. The degree of h insures that the system of equations we have to solve is similar to the two others introduced in this section.

3.3 The correspondence to factoring over the p-adics

Definition 3.12 *Let $f = a_0x^l + \ldots + a_l \in Z[x]$. The discriminant of f is defined as follows:*

$$disc(f) = \frac{(-1)^{l(l-1)/2}}{a_0} Res\ (f, f')$$

where f' is the derivative of f.

It is well known that f is square-free if and only if its discriminant is non-zero.

Notation 3.13 *Let $g, h \in Z[x]$. Then $r(g,h) = v_p(res(g,h))$ and $d(g) = v_p(disc(g))$, where disc(g) is the discriminant of g.*

Now we can prove the major technical theorem of this section:

Theorem 3.14 [Hensel's Lemma II] *Let $p \in Z$ prime $k \in N$ and f,u,w $\in Z[x]$ be polynomials of degrees n+m, n, and m respectively with the following properties*

1. $f \equiv uw \bmod p^k$ *and the leading coefficients (lc) of f and uw are equal*
2. *the resultant $res(u, w)$ is nonzero*
3. $k \geq 2r(u, w)$

Then there are polynomials $g, h \in Z_{(p)}[x]$ such that

$$f = gh \in Z_{(p)}[x], g \equiv u \bmod p^{k-r(u,w)}, h \equiv w \bmod p^{k-r(u,w)}$$

Proof: **[vzGH96a]** Set $\rho = r(u, w)$. We will inductively construct polynomials φ_i and $\psi_i \in Z[x]$ such that if

$$f \equiv ab \bmod p^{k+i-1}$$

with $a, b \in Z[x]$ such that $a \equiv u \bmod p^{k-\rho}$ and $b \equiv w \bmod p^{k-\rho}$ then

$$f \equiv (a + p^{k-\rho+i-1}\psi_i)(b + p^{k-\rho+i-1}\varphi_i) \bmod p^{k+i}$$

Note that if we can do this then we will have proved the claim. If we have for every $i > 0$ such a polynomial, then we can sum over all positive i, and we will have a polynomial with p-adic coefficients that satisfies the above claims. It is important to realize that the infinite sum does **not** result in an element of the ring of formal power series. This is because φ_i and ψ_i have bounded degrees, and only the coefficients in our resulting sum can be thought of as an infinite sum.

Assume that $f \equiv uw \bmod p^k, i \geq 1$, and $a, b \in Z[x]$ are already constructed such that $f \equiv ab \bmod p^{k+i-1}$. Then $f = ab + p^{k+i-1}l$ where $l \in Z[x]$ and $deg(l) < n + m$ since $\mathrm{lc}(ab) = \mathrm{lc}(f)$. Notice that $a \equiv u \bmod p^{k-\rho}$ and $b \equiv w \bmod p^{k-\rho}$. Also, $k - \rho > \rho$ so a is equivalent to u and b is equivalent to w modulo a **higher** power than the largest power of p dividing the resultant of u and w. Thus $r(a, b)$ can be no larger than $r(u, w)$ (If it were larger, then we could calculate $r(a, b)$ and mod out by $p^{k-\rho}$ to find a larger $r(u, w)$). Since they are equivalent modulo $p^{k-\rho}$, $r(a, b) \geq r(u, w)$. Hence $r(a, b) = r(u, w)$. Now we can use Proposition 3.11 to find φ_i and $\psi_i \in Z[x]$ of degrees less than m, n such that

$$p^\rho l = a\varphi_i + b\psi_i$$

and thus

$$p^\rho l \equiv a\varphi_i + b\psi_i \bmod p^{\rho+1}$$

Then we see

$$f - (a + p^{k-\rho+i-1}\psi_i)(b + p^{k-\rho+i-1}\varphi_i)$$

$$\begin{aligned} &= f - ab - p^{k-\rho+i-1}(a\varphi_i + b\psi_i) - p^{2k-2\rho+2i-2}\varphi_i\psi_i \\ &\equiv p^{k+i-1}l - p^{k-\rho+i-1}p^\rho l - p^{2k-2\rho+2i-2}\varphi_i\psi_i \\ &\equiv 0 \bmod p^{k+i} \end{aligned}$$

because $i \geq 1$ and $k > 2\rho$. We do this for all $i \geq 0$ in order to construct the following polynomials:

$$g = u + \sum_{i \geq 1} p^{k-\rho+i-1}\psi_i$$

$$h = w + \sum_{i \geq 1} p^{k-\rho+i-1}\psi_i$$

Expanding out the above sums reveals that g and h have coefficients which are inifinite sums that correspond to a p-adic integer. Almost magically, $f = gh$ over $Z_{(p)}[x]$ since $f \equiv gh \bmod p^k$ for **all** k. By our above construction, $g \equiv u \bmod p^{k-\rho}$ and $h \equiv w \bmod p^{k-\rho}$. ■

Theorem 3.15 *Condition (c) is true if $k > disc(f)$.*

Proof: The proof, found in both [vzGH96a] and [BS66], goes as follows: Let $f = gh$ with $g, h \in Z_{(p)}[x]$. Then

$$disc(f) = disc(gh) = disc(g)disc(f)res(g,h)^2$$

Thus, $d(f) = d(g) + d(h) + 2r(g,h) \geq 2r(g,h)$. Since the discriminant and the resultant are polynomials in the coefficients of f, g, h, the same is true for factorizations over Z_{p^k}. ■

Hence, for any polynomial whose discriminant is smaller compared to the power of the prime, we know the following: Any factorization of $f \equiv gh \bmod p^k$ corresponds to a unique factorization over the p-adics. This factorization $f = \tilde{g}\tilde{h} \in Z_{(p)}[x]$ is equivalent to $gh \bmod p^{k-\rho(g,h)}$. In essence, given any two factorizations $f \equiv gh \bmod p^k$ and $f \equiv g'h' \bmod p^k$, $gh \equiv g'h' \bmod p^{k-\rho(g,h)}$. We note von zur Gathen formalizes this in the following way:

Proposition 3.16 *Let $f = \prod_{1 \leq i \leq l} g_i$ over $Z_{(p)}$ with $disc(f) \neq 0$, $l \geq 1$ and $g_i \in Z_{(p)}[x]$ monic and irreducible for $1 \leq i \leq l$. Let $f \equiv gh \bmod p^k$ with $g, h \in R[x]$ monic and $k > d(f)$. Then there exists a partition $\{1, \ldots, l\} = S \cup S'$ such that $g \equiv \prod_{i \in S} g_i \bmod p^{k-\rho}$ and $h \equiv \prod_{j \in S'} g_j$ with $\rho = r(\prod_{i \in S} g_i, \prod_{j \in S'} g_j)$. If g is irreducible over $Z_{p^k}[x]$ then there exists $1 \leq i \leq l$ such that $g \equiv g_i \bmod p^{k-r(g_i, \prod_{j \neq i} g_j)}$.*

Proof: The proof follows immediately from Theorem 3.14. Given some factorization $f = gh \bmod p^k$, we can lift this to a factorization $f = \tilde{g}\tilde{h}$. But factorization over $Z_{(p)}[x]$ is unique, hence the irreducible factors of f are partitioned among $\tilde{f}$ and $\tilde{g}$ and hence their respective projections mod $p^{k-r(g,h)}$. ■

3.4 An improved factorization method

Now we can give a much better algorithm for computing all of the factorizations of some $f \bmod p^k$. First we need to calculate one factorization into irreducibles of $f \bmod p^k$. Sometimes this can be done by a complicated set of lifting procedures (See Appendix A) or by Chistov's algorithm [Chi94] for computing the factorization of a polynomial over a local ring (namely the p-adics in this case). Chistov's algorithm gives us a factorization in $Z_{(p)}[x]$, but we can simply mod all of the factors by p^k to retrieve a factorization into irreducibles mod p^k.

In order to determine **all** factorizations we need to solve some systems of linear equations. They are considerably simpler, however, because of Theorem 3.14. Given $f \in Z[x]$ and a factorization $f \equiv \prod_{1 \le i \le l} g_i \bmod p^k$ we know for each irreducible factor u of f over $Z_{p^k}[x]$, $u \equiv g_i \bmod p^{k-r(g_i,h)}$ where $h = \prod_{j \ne i} g_j$. Hence any factorization of f must correspond to a solution of the equation found in [vzGH96a].

$$
\begin{aligned}
f &\equiv (g_i + p^{k-r(g_i,h)}\varphi)(h + p^{k-r(g_i,h)}\psi) \bmod p^k \\
&\Leftrightarrow p^{k-r(g_i,h)}(\varphi h + \psi g_i) - p^{2k-2r(g_i,h)}\varphi\psi \equiv 0 \bmod p^k \\
&\Leftrightarrow \varphi h + \psi g_i \equiv 0 \bmod p^{r(g_i,h)} \\
&\Leftrightarrow S(g_i,h)\begin{pmatrix} \varphi_{m-1} \\ \vdots \\ \varphi_0 \\ \psi_{n-1} \\ \vdots \\ \psi_0 \end{pmatrix} \equiv 0 \bmod p^{r(g_i,h)}
\end{aligned}
$$

where

$$\varphi = \sum_{0 \le i < m} \varphi_i x^i$$

$$\psi = \sum_{0 \le i < n} \psi_i x^i$$

Any solution to the above equation corresponds to a factorization mod p^k. After finding all solutions, we can set $g_i = g_{i+1}$ and $h = h/g_{i+1}$, and solve another system of equations until we have found all possible irreducible factors. If at each step there are at most N different solutions found then we could conceivably have N^l distinct factorizations into irreducibles. Since choosing any set of l factors (1 from a possible N at every step) will result in a factorization of $f \bmod p^k$. Fortunately, there are polynomial time algorithms to put the above Sylvester matrix in Smith normal form, giving us a relatively easy method for solving the system of equations and preserving solutions mod p^k.

4 Factoring when the Discriminant is Zero

When k is not bigger than 2ρ we cannot use the above machinery to help us in finding factorizations. As long as $disc(f)$ is non-zero (as long as our polynomials have at least two coprime factors mod p) we have some way of computing at least **one** factorization. If the discriminant of our polynomial f is zero, i.e., $f \equiv g^e \bmod p$ for some irreducible polynomial g, it is not clear how to even lift this factorization to one mod p^k. This section will look at these rather unfortunate cases outlined in [vzGH96b].

4.1 Lifting conditions

Theorem 4.1 [vzGH96b] *Let $f \equiv uw \bmod p^k \equiv g^e \bmod p$, g irreducible over $Z_p[x]$ and $e \geq 2$, $k \geq 1$ with $u, w \in Z[x]$ monic and $u \equiv g^l \bmod p, w \equiv g^{e-l} \bmod p$ for some $l \leq \frac{e}{2}$. Then the following are equivalent:*

1. *$\frac{f-uw}{p^k} \in Z[x]$ over Z_p divisible by g^l.*
2. *For every $\varphi \in Z[x]$ with deg(φ) < deg(u) there exists a polynomial $\psi \in Z[x]$ with deg(ψ) < deg(w) such that $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$.*
3. *There exist polynomials $\varphi, \psi \in Z[x]$ with deg(φ) < deg(u), and deg(ψ) < deg(w) such that $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$.*
4. *There exist polynomials $\varphi, \psi \in Z[x]$ with $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$.*

Proof: $(i) \Rightarrow (ii)$. Let $\frac{f-uw}{p^k} \equiv g^l\alpha \bmod p$ with $\alpha \in Z[x]$, and $\varphi, \psi \in Z[x]$ with $\deg(\varphi) < \deg(u)$, and $\psi \equiv \alpha - g^{e-2l}\varphi \bmod p$. Notice

$$
\begin{aligned}
f - (u + p^k\varphi)(w + p^k\psi) &\equiv f - uw - p^k(\varphi + \psi u) \\
&\equiv f - uw - p^k(\varphi g^{e-l} + (\alpha - g^{e-2l}\varphi)g^l) \\
&\equiv f - uw - p^k g^l \alpha \\
&\equiv 0 \bmod p^{k+1}
\end{aligned}
$$

(ii) $\Rightarrow$(iii) $\Rightarrow$ (iv). We are left with (iv) $\Rightarrow$ (i). Let $\varphi, \psi \in Z[x]$ with $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$. Then

$$
\begin{aligned}
\frac{f - uw}{p^k} &\equiv \varphi w + \psi u \\
&\equiv \varphi g^{e-l} + \psi g^l \\
&\equiv g^l(\varphi g^{e-2l} + \psi) \bmod p.
\end{aligned}
$$

∎

With this in hand we can prove show a certain class of polynomials to be irreducible mod p^k for all $k \geq 2$.

Definition 4.2 *We call $f = \sum_{0 \leq i \leq n} a_i x^i \in Z[x]$ an Eisenstein polynomial if if $a_n = 1$ and $a_i \equiv 0 \bmod p$ for $0 \leq i < n$ and $a_0 \not\equiv 0 \bmod p^2$.*

Corollary 4.3 *Let $p \in Z$ be prime and $f \in Z[x]$ an Eisenstein polynomial. Then f is irreducible $\mathrm{mod} p^k$ for all $k \geq 2$.*

Proof: **[vzGH96b]** Since f is Eisenstein, $f \equiv x^n \bmod p$. In this case, $g = x$. Let $1 \leq l \leq \frac{n}{2}$. Then

$$\frac{f - x^l x^{n-l}}{p} = \frac{f - x^n}{p} = \sum_{0 \leq i < n} \frac{a_i p\, i}{x}.$$

But $a_0 \not\equiv 0 \bmod p$ thus $\frac{f-uw}{p^2} \not\equiv 0 \bmod p$. We fail criterion (i) in Theorem 4.1, so f cannot be lifted to a factorization in $Z_{p^2}[x]$. Thus, f must be irreducible mod p^k for all k since if it were reducible mod p^k for some $k \geq 3$ we could simply mod the factors by p^2 and find a factorization mod p^2. ∎

4.2 Some examples

We can use the lifting criterion to create an (admittedly slow) algorithm for computing all the factorizations of a polynomial f that equals $g^e \bmod p$ for some irreducible $g \bmod p$. Say we want to find all factorizations mod p^k. We choose $1 \leq l \leq \frac{e}{2}$ starting at $l = 1$ and apply see if the factorization mod p can be lifted to p^2 by computing $\frac{f-uw}{p^k}$ and applying Theorem 4.1. At the lifting step for p^2 we make an arbitrary choice, namely we choose φ such that φ has degree less than u. This could be an unfortunate choice, however, because our choice of φ may preclude the possibility of lifting mod p^3. In [vzGH96b], we see some interesting examples:

Example 4.4 *Let $f = x^2 + 27x + 162$. Then $f \equiv x^2 \bmod 3$ and $\frac{f-x^2}{3} \equiv 0 \bmod 3$.*

Assume that we have chosen some φ as above to lift this to a factorization mod 9. Then we have

$$f \equiv (x + 3\varphi)(x + 3(-\varphi)) \equiv (x + 3\varphi)(x + 6\varphi) \bmod 9$$

where $0 \leq \varphi \leq 2$. Then

$$\frac{f-(x+3\varphi)(x+6\varphi)}{9} \equiv 2(\varphi+\varphi^2) \bmod 3.$$

So we can only lift this factorization to one mod 3^3 if $2(\varphi+\varphi^2) \equiv 0 \bmod 3$. This happens only when $\varphi = 0$ or 2. Thus, had we chosen $\varphi = 1$, we would not be able to lift this factorization.

Unfortunately, this procedure can get rather complicated as the next example will illustrate:

Example 4.5 *Let* $p = 3, f = x^{10}$, *and* $l = 10$.

After two lifting steps, we obtain the following factorization:

$$f \equiv uw \bmod 81, \text{where}$$

$u = x^4 + 3\varphi_3 x^3 + 3\varphi_2 x^2 + 9\varphi_1 x + 9\varphi_0$ and $w = x^6 + 78\varphi_3 x^5 + (78\varphi_2 + 9\varphi_3^2)x^4 + (72\varphi_1 + 18\varphi_2\varphi_3 + 54\varphi_3^3)x^3 + (72\varphi_0 + 9\varphi_2^2 + 54\varphi_1\varphi_3)x^2 + (54\varphi_0\varphi_3 + 54\varphi_1\varphi_2)x + 54\varphi_0\varphi_2 + 54\varphi_2^3$

and $0 \le \varphi_i < 27$ for $i \in \{2,3\}$, and $0 \le \varphi_i < 9$ for $i \in \{0,1\}$. Then

$$\begin{aligned} \frac{f-uw}{81} \equiv\ & 2\varphi_3 x^9 + 2\varphi_2 x^8 + (2\varphi_3^3 + 2\varphi_1)x^7 + (2\varphi_3^2 + 2\varphi_0 + \varphi_3^4)x^6 \\ & +(2\varphi_2^2\varphi_3 + \varphi_2\varphi_3^3)x^5 + (2\varphi_2^3 + \varphi_1^2)x^4 \\ & +(2\varphi_0\varphi_1 + \varphi_1\varphi_2^3)x^3 + (\varphi_0^2 + \varphi_2^4)x^2 \bmod 3 \end{aligned}$$

From the above lemma, we can only lift this factorization if g^l divides $f - uw/p^k \bmod p$. Hence we need the following to be true:

$$\begin{aligned} 2\varphi_0\varphi_1 + \varphi_1\varphi_2^3 &\equiv 0 \bmod 3 \\ \varphi_0^2 + \varphi_2^2 &\equiv 0 \bmod 3. \end{aligned}$$

These equations turn out to be satisfied if and only if $\varphi_2 \equiv 0 \bmod 3$ and $\varphi_0 \equiv 0 \bmod 3$. As the degree of f gets larger, the difficulty of solving these equations to find all factorizations grows quickly. In fact, the biggest obstacle to computing these factorizations is to determine which parameters will allow for liftings to higher powers of p. It is not clear how to simultaneously satisfy the all of the parameters at each step. Hence, the best algorithm known runs in exponential time, simply trying out all possible values for each parameter.

5 Further Algebraic Considerations

In this section we attempt to give some further purely algebraic considerations of factorizations in $Z_{p^k}[x]$ partially outlined in [McD74]. We will prove results for a more general ring than $Z_{p^k}[x]$ and show that all results apply to our case. All rings in this section are commutative and have identity. (a) denotes the principal ideal generated by a.

5.1 Local rings

Definition 5.1 *A* **local ring** *is a ring with a unique maximal ideal.*

Example 5.2 *$Z_{(p)}, Z_{p^k}$ and $Z_{p^k}[x]$ are all local rings whose unique maximal ideal in all cases is (p).*

Recall that R/m where m is a maximal ideal of R is actually a field. The field that results from taking R/m where m is our unique maximal ideal is called a local field. Let $k = R/m$. Define the natural projection from $R[x]$ to $k[x]$ by μ. In $Z_{p^k}[x]$, μ takes a polynomial in $Z_{p^k}[x]$ and reduces all of its coefficients modulo p.

We need the following long string of definitions to continue this development. Some of the definitions are repeated from previous sections for clarity.

Definition 5.3 *Let f and $g \in R[x]$ Then*

- f is **nilpotent** if there is an integer n such that $f^n = 0$.
- f is a **unit** if there is a polynomial h with $fh = 1$.
- f is **regular** is f is not a zero divisor.
- f is **prime** if (f) is a proper prime ideal.
- f is **irreducible** if f is not a unit and whenever $f = gh$ then g or h is a unit.
- f is **primary** if (f) is a primary ideal.
- f and g are **associated** if $(f) = (g)$.
- f and g are **coprime** if $R[x] = (f) + (g)$

The following proposition gives us some simple characterizations for the above definitions:

Proposition 5.4 [McD74] *Let $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$.*

1. *The following are equivalent*

   (a) *f is a unit*
   (b) *μf is a unit.*
   (c) *a_0 is a unit and $a_1 \dots a_n$ are nilpotent*

2. *The following are equivalent*
   (a) *f is nilpotent*
   (b) *$\mu f = 0$*
   (c) *$a_0, \dots, a_n$ are nilpotent*
   (d) *f is a zero divisor*
   (e) *there is a non-zero $a \in R$ with $af = 0$.*

3. *The following are equivalent*
   (a) *f is regular*
   (b) *$(a_0, a_1, \dots, a_n) = R$*
   (c) *a_i is a unit for some $0 \le i \le n$*
   (d) *$\mu f \neq 0$*

Proof: The proof of parts (a) and (b) follow immediately from Proposition 2.9 in the first section. Part (c) is quite easy as well. If f is regular then it is not a zero divisor. Hence, we cannot 'factor' out p from one of the coefficients. This implies that some $a_i \notin (p)$. Since (p) is our unique maximal ideal, a_i must be a unit. Since some a_i is a unit, $(a_0, a_1, \dots, a_n) = R$. Furthermore, since not all the coefficients are in (p), our projection onto $m[x]$ must be non-zero. Hence, $\mu f \neq 0$. ∎

5.2 Hensel's Lemma generalized

Now we can restate Hensel's Lemma in a more general setting:

Theorem 5.5 [Generalized Hensel's Lemma] *Let $f \in R[x]$ and*

$$\mu f = \bar{g_1} \cdots \bar{g_n}$$

where $\bar{g_1}, \dots, \bar{g_n}$ are pair-wise coprime. Then there exist $g_1, \dots, g_n \in R[x]$ such that

1. *$g_1, \dots, g_n$ are pair-wise coprime*
2. *$\mu g_i = \bar{g_i}$ for $1 \le i \le n$.*
3. *$f = g_1 \cdots g_n$.*

Proof: The proof is identical to that of the first Hensel's Lemma. All of the details are in [McD74]. ∎

5.3 Ideal decomposition

We build towards a nice characterization of all factorizations of a polynomial in such a ring. In order to do this, we need to apply some theorems from Primary Ideal Decomposition found in [Hun74]. Before this, we make a few observations.

Lemma 5.6 *Let I, J be comaximal ideals of a ring R. $I + J = I \cap J$.*

Proof: Recall that IJ is the set of all finite sums of the form ij such that $i \in I$ and $j \in J$. $IJ \subset I \cap J$ since for $a \in IJ$, $a = rij$ for some $r \in R$, and thus $a = (ri)j$ and $a = (rj)i$. Now let $a \in I \cap J$. Since I, J are comaximal, there exist $r_1, r_2 \in R$ such that $r_1 i + r_2 j = 1$. Hence $ar_1 i + ar_2 j = a$. But $a = ci$ and $a = bj$ for some $c, b \in R$. Thus $bjr_1 i + cir_2 j = c \Rightarrow ij(br_1 + cr_2) = a$. Hence $a \in IJ$. ■

Corollary 5.7 *Let $I_1, I_2, \ldots, I_n$ be pair-wise comaximal ideals. Then it follows that $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$.*

Definition 5.8 *Let I be an ideal of R. The* **radical** *of I, denoted Rad I, is the intersection over all prime ideals P that contain I. If the set of prime ideals containing I is empty then Rad I is defined to be R.*

Definition 5.9 *If Q is a primary ideal in a commutative ring R, then the radical P of Q is called the associated prime ideal of Q. We say that Q is P primary.*

Lemma 5.10 *Let R be a local ring. Then if (μg) is a primary ideal then (g) is a primary ideal.*

Proof: Let $ab \in (g)$. We assume that $b \notin (g)$. We need to show that $a^n \in (g)$ for some n.We know (μg) is a primary ideal by assumption. $\mu g = g + M$ where M is our unique maximal ideal. Since $ab \in (g)$, $\mu(ab) \in (\mu g) \Rightarrow ab + M = (a + M)(b + M) \in (g + M)$. But $(g + M)$ is primary. Hence

$$\begin{aligned} (a+M)^k &= (a^k + M) \in (g + M) \\ (a^k + M) &= ug + M \\ &\Leftrightarrow a^k - ug \in M. \end{aligned}$$

This implies that $a^k = ug + m$ for some $m \in M$ and $u \in R$. Now let d be the nilpotency of m and we see:

$$
\begin{aligned}
a^{kd} &= (ug+m)^d \\
&= \sum_{i=0}^{d} \binom{d}{i} g^i u^i m^{d-i} \\
&= gY + m^d \\
&= gY
\end{aligned}
$$

where d is the nilpotency of m and Y is what remains after factoring out a g from the above sum. Hence $a^{kd} \in (g)$ so (g) is primary. ■

Corollary 5.11 *Let $R = Z_{p^k}[x], e \in N$. Let g be an irreducible non-zero polynomial mod p and h and arbitrary element of $Z_{p^k}[x]$. Then $(g^e + ph)$ is a primary ideal. In particular, $(g^e + ph)$ is (g) primary.*

Proof: Notice that $g^e + ph \bmod p \equiv g^e \bmod p$ which is trivially a primary polynomial. By the above lemma, $g^e + ph$ must be primary. ■

We introduce the next two definitions and theorem for the proof of the main theorem of this section:

Definition 5.12 *We say an ideal C of R has a primary decomposition if $C = A_1 \cap A_2 \cap \cdots \cap A_n$ with each A_i a P_i primary ideal of R for some prime ideal P_i of R. If no A_i contains $A_1 \cap A_2 \cap \cdots A_n$ and if the ideals $P_1, \ldots, P_n$ are distinct then the primary decomposition is said to be reduced.*

Definition 5.13 *Let C, A_i, and P_i as above. If $P_i \not\subset P_j$ for all $j \neq i$ then P_i is said to be an isolated prime ideal of C.*

Theorem 5.14 *Let C be an ideal of R with two reduced primary decompositions*

$$A_1 \cap A_2 \cap \cdots \cap A_k = C = A'_1 \cap A'_2 \cap \cdots \cap A'_n$$

where A_i is P_i primary and A'_j is P'_j primary. Then k=s and (after reordering) $P_i = P'_i$ for $i = 1, 2, \ldots, k$. Futhermore if A_i and A'_i both are P_i primary and P_i is an isolated prime then $A_i = A'_i$.

The original statement of the theorem and proof can be found in [Hun74]. It is stated originally for R-modules, but we view a ring R as an R-module over itself and so everything applies naturally.

5.4 The unique factorization theorem

Now we can prove the much anticipated major theorem of this section.

Theorem 5.15 **[McD74]** *Let f be a regular polynomial in $R[x]$. Then*

1. $f = \delta g_1 \cdots g_n$ *where δ is a unit and $g_1 \cdots g_n$ are regular primary coprime polynomials.*
2. *If $f = \delta g_1 \cdots g_n = \beta h_1 \cdots h_m$ where δ and β are units and $\{g_i\}$ and $\{h_j\}$ are regular primary coprime polynomials then $n = m$ and, after reordering $(h_i) = (g_i), 1 \leq i \leq n$.*

Proof: First we prove (1). Let f be regular in $R[x]$. Then μf is non-zero. Hence $\mu f = \bar{\delta}\bar{g_1}^{e_1} \cdots \bar{g_n}^{e_n}$ where the g_i's are irreducible coprime polynomials in $k[x]$. In other words, we have projected our polynomial mod p to find its factorization into powers of irreducible coprime polynomials. Now, using Hensel's Lemma, we can find a factorization $f = \delta g_1 \cdots g_n$ where $\mu\delta = \bar{\delta}$ and $\mu g_i = \bar{g_i}^{e_i}$. Notice that each $g_i = g^e + ph$ for some irreducible polynomial g and some polynomial $h \in R[x]$. Thus by Lemma 5.10 $(g_i)'s$ and similary $(h_i)'s$ are primary.

Now we prove (2). Since we have $f = g_1 \cdots g_n = h_1 \cdots h_n$ we have the following series of equations:

$$\begin{aligned} (f) &= (g_1 \cdots g_n) = (h_1 \cdots h_n) \\ &\Leftrightarrow (g_1) \cdots (g_n) = (h_1) \cdots (h_n) \end{aligned}$$

But since the $(g_i)'s$ are pairwise comaximal we have that $(g_1)(g_2) \cdots (g_n) = (g_1) \cap (g_2) \cap \cdots \cap (g_n)$ and similarly for the $(h_i)'s$. The underlying prime ideal for each $(g_i) = (g^e + ph)$ is simply (g). Trivially, for g, h distinct irreducible polynomials mod p, $(g) \not\subset (h)$. Hence, every underlying prime ideal in our product is isolated. Thus, we have found two reduced primary decompositions for f where every P_i is isolated for every P_i primary ideal in the product. By the Theorem 5.14 after renumbering, the individual ideals must be equal. ∎

Thus our factorizations are unique up to ideals

6 Conclusions and Questions

6.1 Some conclusions

The discriminant of a polynomial determines whether or not it is hard to calculate all of its factorizations mod p^k. In all cases we can use a unique factorization modulo p to help find all the factorizations. This information alone is not very helpful. If the prime power we are factoring over is much larger than the discriminant, we can use the correspondence with the p-adic integers to form a relatively simple method to solve a system of equations in polynomial time.

If the discriminant is zero, we have difficulty characterizing the factorizations of our polynomials, because we cannot easily lift the factorization. This case results in a complicated systems of diophantine equations.

The Primary Decomposition Theory provides us with a nice characterization of the factorizations of a polynomial. Although the factorization of a polynomial is not unique in $Z_{p^k}[x]$, it is unique up to the ideals generated by the coprime factors. We would like to take advantage of this algebraic situation and come up with an algorithm that exploits it. Unfortunately, all of the known ideal membership problems rely upon a Gröbner Basis algorithm which runs in exponential time.

These results could be applied the multivariate case were it not for our current inability to lift multivariate factorizations. Applying this in the multivariate case could result in new bounds for polynomials representing boolean functions modulo n.

6.2 Questions

We would like to use the results to get bounds on the degree of a polynomial representing a boolean function. This could be done by examining its factorization over the p-adics. Unfortunately, these polynomials are all multi-variate, and our results do not directly apply. The problem is that when two multivariate polynomials f, g are relatively prime, there do not necessarily exist polynomials f', g' such that $fg' + gf' = 1$. Thus, Hensel's Lemma breaks down. An interesting problem is determining whether or not a multivariate factorization can be lifted and if so, how? This would provide us with a way to use all of the machinery developed for the univariate case.

It is also unclear as to how Primary Decomposition Theory can be used, outside of Gröbner Basis algorithms, to provide some insight on factorizations. Exploiting this natural algebraic structure seems quite possible.

Is there a feasible way of implementing/verifying Chistov's algorithm for factoring polynomials over $Z_{(p)}[x]$ in polynomial time? Currently, it seems far beyond what we can implement.

7 Acknowledgements

I greatly appreciate my advisor Professor Dana Scott's support throughout the entire process of writing this thesis. From the outset, Professor Scott allowed me to pursue mathematical topics of my own independent interest; his guidance enabled my success. Many thanks go to Andrej Bauer who suffered through the many technical details of this paper and selflessly devoted hours to assist me. His mathematical knowledge and Mathematica prowess were invaluable. I also appreciate Professor Steven Rudich's constant enthusiasm and inspiration which motivated the writing of this paper. I had useful conversations with Professor Ravindran Kannan and Glenn Durfee.

8 Appendix

This Appendix contains code for the Mathematica Symbolic Computation Package. It includes a function, CompFactor, which takes as input a polynomial in $Z[x]$ and will produce a factorization mod n for a specified composite. If the polynomial is of the form g^e mod p for some prime p dividing n, then the algorithm will not compute a factorization. This case corresponds to the case where the discriminant of f is zero and thus cannot be lifted without a tedious exponential time algorithm. Otherwise, the polynomial is factored into coprime factors using Hensel Lifting and the Chinese Remainder Theorem.

```
Get["NumberTheory‘NumberTheoryFunctions‘"];
Get["Algebra‘PolynomialPowerMod‘"];
Get["Algebra‘PolynomialExtendedGCD‘"];


ExtraCoeff[a_List,i_]:=
  If [a == {},
  (*then*)
    {},
  (*else*)
    Prepend[ExtraCoeff[Rest[a],i],Coefficient[First[First[a]],x^i]]
  ]

ExtraConCoeff[a_List]:=
  If [a == {},
  (*then*)
    {},
```

```
  (*else*),
    Prepend[ExtraConCoeff[Rest[a]],PolynomialMod[First[First[a]],x]]
  ]

ExtraModuli[a_List]:=
  If [a == {},
  (*then*)
    {},
  (*else*)
    Prepend[ExtraModuli[Rest[a]],First[Rest[First[a]]]]
  ]

(* Given the list {{fac1,m_1},{fac2,m_2}} we can reconstruct the polynomial
with this decomposition *)

ChinesePolyRem[a_List,n_]:=
Module[{ModuliList,pp,ResPoly},
      ModuliList = ExtraModuli[a];
      For[pp=0,pp<(n+1),pp++,
 If[pp==0,
(* then *)
ResPoly=ChineseRemainderTheorem[ExtraConCoeff[a],ModuliList],
(* else *)
  ResPoly = (ResPoly +
      (ChineseRemainderTheorem[
ExtraCoeff[a,pp],ModuliList])*x^pp)]];
      {ResPoly}]


(* This takes a polynomial f, its two factors mod p (g and h) as well as p
and the degree to lift to and produces a lifted factorization Based
 on Eric Bach's Algorithmic Number Theory book-- see Bibliography*)

HenselLift[f_,g_,h_,p_,k_]:=Module[{t,a,b,q,u,v,gg,hh},
t=PolynomialExtendedGCD[g,h,Modulus->p];
a=t[[2,1]];
b=t[[2,2]];
gg=g;
hh=h;
For[i=2,i<(k+1),i++,
q=PolynomialMod[(f-gg*hh)*(1/(p^(i-1))),p];
u=PolynomialMod[(q*b),g];
```

```
v = PolynomialMod[(q*a),h];
 gg = PolynomialMod[(gg + ((p^(i-1))*u)),p^i];
hh = PolynomialMod[(hh + ((p^(i-1))*v)),p^i]]; {gg,hh}]


PolyMult[a_,b_]:= (First[a]*First[b])

ProductPoly[a_] := Fold[PolyMult,{1,1},a]

(* This takes {{p1,m1},{p2,m2} ... } and produces p1*p2*p3..*pn *)

PolyProd[a_]:=
If[a=={},1,First[First[a]]*PolyProd[Rest[a]]]

/*This creates a tuple of n 1's with the irred polynomial in the kth
position, i.e. {1,1,1,irred,1,1,1} It corresponds to an irreducible factor
in the product ring */

CreateIrreducible [irred_,n_,k_,mmlist_]:=Module[{final},
final= {};
For[oo=1,oo<n+1,oo++,

If[oo==k,
(*then*)
 AppendTo[final,{irred,mmlist[[oo]]}],
        (*else*)
AppendTo[final,{1,mmlist[[oo]]}]]];final]



(* More helper functions *)
(* These put factorizations from the FactorList function into a more
acceptable form. I.e., {{x^2+2,3}} is translated as {(x^2+2)^3,1} *)


PowerHelp[f_]:={First[f]^(First[Rest[f]]),1}

MyFactorList [f_,p_]:=Map[PowerHelp,FactorList[f,Modulus->p]];



(* This takes a polynomial f, a list of its irreducible factors mod p
```

```
{{p1,exp},{p2,exp2},{p3,exp3} .. } and lifts it to a complete factorization
mod p^k.  n corresponds to the number of irred factors *)

LiftFactors[f_,a_List,n_,p_,k_]:=
Module[{productsofar,TempPolyList,LiftedList},

TempPolyList = a;
If[(a[[2,2]] == 1 && Length[a] == 2),{{1,1},{f,1}},
 (* else *)
If[Length[a] ==2, Print["Failure"],
 (* else *)
LiftedList={};
Tempf = f;
productsofar=PolyProd[a];
AppendTo[LiftedList,{1,1}];
TempPolyList = Rest[TempPolyList];
Firstfac = TempPolyList[[1,1]];
Secondfac = PolynomialQuotient[productsofar,Firstfac,x,Modulus->p];
For [jj=0,jj<n+1,jj++,
(    Print[jj];
 If[Length[TempPolyList]==1,
(* then *)
Return[{LiftedList,p^k}],
(* else *)
With[{FLiftFac =First[HenselLift[Tempf,Firstfac,Secondfac,p,k]],
SLiftFac =HenselLift[Tempf,Firstfac,Secondfac,p,k][[2]]},

If [Length[TempPolyList] == 2, (* only 2 factors to lift *)
(* then *)
(AppendTo[LiftedList,{FLiftFac,1}];
AppendTo[LiftedList,{SLiftFac,1}]);
TempPolyList = Rest[TempPolyList],
(* else *)
(TempPolyList = Rest[TempPolyList];
AppendTo[LiftedList,{FLiftFac,1}];
Tempf = SLiftFac;
Firstfac = TempPolyList[[1,1]];
Secondfac =
                  PolynomialQuotient[Secondfac,Firstfac,x,Modulus->p];)]]])];];]

(* CreateMasterList takes a polynomial f, and a list of factors (fac)
of some modulus. It reduces f by each element of fac and factors it using
```

```
previous procedures. Returned is a list of the following type:
{{{{1,1},{x,1},{3+x,1}},5},{{{1,1},{3+x,1},{5+x,1}},7}}

This corresponds to f's factorization mod 5 and mod 7 *)

CreateMasterList[f_, fac_List]:=
  Module[{TempFL,GoalList,n,currentp,currentexp,FacList},
TempFL = fac;
n = Length[fac];
GoalList={};
 For [ii=0, ii<n, ii++,
         currentp = First[First[TempFL]];
 currentexp = First[Rest[First[TempFL]]];
If[((FactorList[f,Modulus->currentp])[[2,2]] > 1 &&
      Length[FactorList[f,Modulus->currentp]] == 2),Abort[],Print["Liftable"]];
 FacList = MyFactorList[f,currentp];
 t = Length[FacList];
If[t==2,
(*then *)
AppendTo[GoalList,{{{1,1},{FacList[[2,1]],1}},currentp^currentexp}],
(*else *)
AppendTo[GoalList,LiftFactors[f,FacList,t,currentp,currentexp]]];
If [Rest[TempFL] == {},Return[GoalList],TempFL=Rest[TempFL]]];]

(* Final List takes the list created by CreateMasterList and expands
everything by converting it into irreducibles of the form (1,1,1,1,f,1,1,1)
and sending it to the poly chinese remainder theorem. It then reconstructs
the correct factors and spits out our factorization It gets the length
of this tuple from deg *)

FinalList [Master_List,deg_]:=
  Module[{TMaster,MModuliList,FinalOutput,Outerloop,Innerloop,Interoutput,
      Innerlist},
TMaster = Master;
MModuliList = Map[Last,Master];
FinalOutput={};
Outerloop = Length[Master];
For[iii=1,iii<Outerloop+1, iii++,
(
Inneroutput={};
Innerloop = Length[First[First[TMaster]] - 1];
           Innerlist = First[First[TMaster]];
```

```
For[jj=2,jj<Innerloop+1,jj++,
(AppendTo[Inneroutput,
First[ChinesePolyRem[CreateIrreducible
[Innerlist[[jj,1]],Outerloop,iii,MModuliList],deg]]];

(* debugging purposes *)

Print[MModuliList];
Print[CreateIrreducible[Innerlist[[(jj),1]],Outerloop,iii,MModuliList]];
Print[ChinesePolyRem[CreateIrreducible
[Innerlist[[(jj),1]],Outerloop,jj-1,MModuliList],deg]];)];
TMaster = Rest[TMaster]);
AppendTo[FinalOutput,Inneroutput];]; Flatten[FinalOutput]]

(* This gives the actual factorization. The master function *)

MasterFactor [f_,deg_,n_]:=
FinalList[CreateMasterList[f,FactorInteger[n]],deg]

CompFactor[poly_,modd_]:=
MasterFactor[poly,2*Exponent[poly,x],modd]
```

References

[Akr89] Alkiviadis G. Akritas. *Elements of Computer Algebra with Applications.* John Wiley and Sons, New York, 1989.

[BBR94] David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4:367–382, 1994.

[Ber70] E.R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24, 1970.

[BS66] Z. I. Borevich and I.R. Shafarevich. *Number Theory.* Academic Press, New York, 1966.

[BS96] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory*, volume 1. The MIT Press, Camrbidge, Massachusetts, 1996.

[Chi94] A.L. Chistov. Efficient factorization of polynomials over local fields. *J. Math. Sciences*, 70, 1994.

[CLO92] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Springer-Verlag, New York, 1992.

[DF90] Arthur Dummit and Thomas Foote. *Abstract Algebra.* Math Books, New York, 1990.

[FSS84] M. Furst, J.B. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17:13–27, April 1984.

[Hun74] Thomas W. Hungerford. *Algebra.* Springer-Verlag, New York, 1974.

[McD74] Bernard R. McDonald. *Finite Rings with Identity.* Marcel Dekker, Inc., New York, 1974.

[Sha93] A. Shamir. On the generation of polynomials which are hard to factor. In *25th Annual ACM Symposium on the Theory of Computing*, 1993.

[Smo87] R. Smolensky. On interpretation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates. *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 77–82, 1987.

[TB94] G. Tardos and D. A. M. Barrington. A lower bound on the mod 6 degree of the OR function, April 1994.

[vzGH96a] Joachim von zur Gathen and Silke Hartlieb. Factoring modular polynomials. *Proc. ISSAC*, 1996.

[vzGH96b] Joachim von zur Gathen and Silke Hartlieb. Factorization of Polynomials Modulo Small Prime Powers. Technical report, University of Paderborn, Germany, 1996.