Factorization modulo prime powers

Sayak Chakrabarti
170648

Supervised by
Prof. Rajat Mittal

Abstract

Polynomials can be factorized using various methods in fields which have been given by [Ber67], [CZ81], [KU11] in finite fields, [LLL82] over rationals, [Lan85] over number fields, [Chi87], [CG00] over p-adic fields etc. However there can be different factorizations when the ring is not a unique factorization domain. In this project we explore the ways of factorization in rings of the form Z/p^kZ for a given prime p and an integer $k \geq 1$ when it is given that the factorization splits the polynomial completely into linear factors.

Contents

1 Introduction

Polynomial factorization has been a famous question in the fields of mathematics and theoretical computer science. There has been extensive work in this area and since the later half of the 20^{th} century several researchers have come up with factoring algorithms over various fields, for e.g. over finite fields [Ber67], [CZ81], [KU11], over rationals [LLL82], number fields [Lan85], p-adic fields [Chi87], [CG00] etc. In our project we explore the techniques for factorization in rings of the form Z_p^k for a prime p and an integer k. This has been reduced from factoring in the ring Z_n for any composite integer n, the reduction of which follows easily from Chinese Remainder Theorem illustrated in the paper [vzGH96a]. This has widespread applications in error correcting codes and other branches of Computer Science. In this paper our problem statement is to provide a factorization technique such that it yields the maximum number of linear factors, from which we will eventually move on to providing a technique for maximum number of factors of a polynomial.
The non-trivial nature of this problem can be illustrated by the following example.

Example 1.1 : Consider the polynomial $x^2 \mod p^2$. This can yield one factorization $(x)^2$ and another $(x-p)(x+p)$, in which we are interested in the latter.

We have used the root find algorithm to find each representative root of a polynomial modulo prime powers in randomized polynomial time. The representative roots modulo p^k for a polynomial are of the form $A + p^i *$ where $A \in Z/p^iZ$ and $*$ represents all the values that in $Z/p^{k-i}Z$. This is a compact datastructure introduced in the paper [BLQ13] to find all the roots where the roots might be exponentially many. [DMS19] gives an exposition of the algorithm which can be used to find all the roots in the ring Z/p^kZ.
To find a factorization we first find the representative roots using the ROOT-FIND algorithm. Then building on the roots we attempt to find a factorization for the polynomial. We start by handling small degree polynomials first.

In the following sections we start with explaining root sets of polynomials (Section 3) as they bear resemblance with representative roots, explained later, as a set consisting of roots. After that a gentle introduction to p-ordering sequences has been given in section 4.
In section 5 we explain some lifting techniques, mainly based on the papers [vzGH96a], [vzGH98] as they give an idea of the factorization problem for integral polynomials modulo powers of primes. This is followed by Section 6 giving a description of Representative Roots and an algorithm to find roots of a polynomial in rings of our interest, which will be extensively used in our factorization techniques.

2 Preliminaries

Let $R(+,.)$ be a ring and S be a subset of R. We denote $aS = \{a + s | s \in S\}$ and $a + S = \{a + s | s \in S\}$ for any $a \in R$.
Throughout this paper we are mainly interested in rings which are of the form Z/nZ, often written as Z_n which is the ring taking modulo with n. However instead of n we work with p^k for some prime p and an integer $k \geq 1$ using the reduction using Chinese Remainder Theorem. Unless specified p will always denote a prime integer and k will be an integer greater than or equal to 1, while n be represented as a composite number.
Rest of the notations used as preliminaries have been explained in their respective sections to make this paper more self-contained.

3 Root Sets of polynomials modulo prime powers

Root set R modulo n refers to a set of integers in Z/nZ such that there exists a polynomial in $(Z/nZ)[x]$ the roots of which are exactly the elements of R.
The analysis of properties of root sets presented in this chapter is based on the paper [DM97].

For an integer j and another integer $m \geq 1$, we define

$$j^{\underline{m}} = j(j-1)(j-2)\dots(j-m+1)$$

Now for a prime p, the highest power of p in the factorization of $n \in N$ is denoted by $\epsilon_p(n)$. It can be easily shown that

$$\epsilon_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$$

$\epsilon_p(0)$ is defined to be $+\infty$
In the rest of this section we give some theorems on root sets of polynomials modulo powers of primes, and how the can be decomposed into root sets which are divisible by p.

Lemma 3.1: For integers $j, m \geq 0$ we have $\epsilon_p(j^{\underline{m}}) \geq \epsilon_p(m!)$
Proof: We have $\epsilon(j^{\underline{m}}) = \epsilon_p(\frac{j!}{(j-m)!}) = \epsilon_p(j!) - \epsilon_p((j-m)!)$. Now we have $[x] - [y] \geq [x-y]$ from which the following result follows:

$$\epsilon_p(j^{\underline{m}}) = \sum_{i=1}^{\infty} \lfloor \frac{n=j}{p^i} \rfloor - \sum_{i=1}^{\infty} \lfloor \frac{j-m}{p^i} \rfloor \geq \sum_{i=1}^{\infty} \lfloor \frac{m}{p^i} \rfloor = \epsilon_p(m!)$$

Lemma 3.2: If $j.m! \equiv 0 \mod p^k$ then for every $t \in Z_{p^k}$ we have $j.t^{\underline{m}} \equiv 0 \mod p^k$.
Proof of lemma 2.2 follows directly from lemma 2.1 as the power of p in $j.m!$ is less than that in $j.t^{\underline{m}}$.

Based on these results the following theorems can be inferred, proofs of which can be found in [DM97].

Theorem 3.3: Let R be a root set modulo a prime power p^k, for prime p and an integer k. Then for each $j = 0, 1, 2 \dots, p-1$, there is a polynomial f_j, the root set of which is exactly $R_j = \{r \in R | r \equiv j \mod p^k\}$

Theorem 3.4: Let $R_0, R_1, \dots R_{p-1}$ be root sets modulo p^k with R_j having elements congruent to j modulo p, then $R_0 \cup R_1 \cup \dots \cup R_{p-1}$ is a root set modulo p^k.

Theorem 3.3 shows that a root set can be decomposed into p disjoint segments with constant remainder modulo p while Theorem 3.4 says that given segments with constant remainder modulo p we can join them together to give a bigger root set.

Theorem 3.5: If R is a root set modulo n, then $j + R$ is also a root set modulo n for every $j \in Z_n$
Proof: If a polynomial $f(x)$ has a root set as R then the polynomial $f(x-j)$ has the root set $j + R$.

Based on these results we can restrict ourselves to finding root sets modulo p^k to finding root sets elements of which are divisible by p in Z_{p^k}.

4 p-ordering sequences and Factorial function generalization

This section shows how factorial functions can be generalized over subsets of integers other than the entire set of integers. For this we describe the concept of p-ordering introduced in the paper [Bha00]. In this section we deal with subsets of Z only as we do not need the generalized version in our problem of factoring polynomials. However a generalized version of these properties over arbitrary Dedekind Domains can be found in [Bha97].

Definition 4.1: Given an integer a and a prime p we define the function $v_p(a)$ as

$$\begin{aligned} v_p(a) &= v \qquad \text{if } a \neq 0 \text{ and } p^v | a \text{ but } p^{v+1} a \\ &= \infty \qquad \text{if } a = 0 \end{aligned}$$

Definition 4.2: [**p-ordering**] Let S be an arbitrary subset of Z and p be a given prime. A p-ordering of S is a sequence which is formed inductively as follows:

- Choose any element $a_0 \in S$
- Choose another element $a_1 \in S$ such that $v_p(a_1 - a_0)$ is minimum.
- Choose an element $a_2 \in S$ such that $v_p((a_2 - a_0)(a_2 - a_1))$ is minimum.

  $\vdots$
- For the k^{th} step choose $a_k \in S$ such that $v_p((a_k - a_0)(a_k - a_1)\dots(a_k - a_{k-1}))$ is minimumm.

Definition 4.3: We define $v_p(S,k)$ as the power of the prime p in the product $(a_k - a_0)(a_k - a_1)\dots(a_k - a_{k-1})$ where $\{a_n\}$ forms the p-ordering sequence.

Definition 4.4: We define the associated p-sequence as the sequence of powers of primes associated with a p-ordering sequence.

An important theorem with p-ordering sequences are:

Theorem 4.5: The associated p-sequence is unique for a given subset $S \subseteq Z$ and a given prime p.

Note that p-ordering sequence might not be unique as we can start with any element in a_0 and then as we inductively continue we can have a number of choices to choose from. But Theorem 4.5 states that the powers of the prime p associated with the p-ordering sequence is always unique despite the choice of the p-ordering, which has been proved in [Bha00].
We now show how a p-ordering sequence over subsets of Z behaves quite like the factorial function in Z based on the results shown in [Bha00] which gives us a motivation that this might be useful in considering p-ordering for our problem of factorization.

Definition 4.6: The factorial function of a set S upto k terms is denoted by $k!_S$ and is defined as

$$k!_S = \Pi_{(\text{prime } p)} v_p(S,k)$$

Note that when we have the set S as Z this gives us the value of factorial over integers.

Lemma 4.7: For non-negative integers k and l, $(k+l)!_S$ is a multiple of $k!_S l!_S$.

In the following part we give some lemmas showing how this generalized factorial function acts as normal factorial function over natural numbers, proofs of which can be directly found in [Bha00].
We denote $d(S,f) = gcd\{f(a)|a \in S\}$.

Lemma 4.8: For a primitive polynomial f of degree k, we have $d(S,f)|k!_S$.

Lemma 4.9: Let $a_0, a_1 \dots a_n \in S$ be any $n+1$ integers. Then we have $0!_S 1!_S 2!_S \dots n!_S | \Pi_{i<j}(a_i - a_j)$.

Lemma 4.10: The number of polynomials from S to Z_n is given by $\Pi_{k=0}^{n-1} \frac{n}{gcd(n,k!_S)}$.

From this we note that p-ordering sequence behaves as normal factorials too. Also suppose that $\{a_n\}$ is a p-ordering sequence in S then a_k is a root of $f(x) = (x - a_1)(x - a_2)\dots(x - a_{k-1}) \mod p^{v_p(S,k)}$, which motivates the question, if there is any p-ordering relation in the roots of a polynomial in a given set of integers.

5 Lifting of factorizations and Resultants

In this section we deal with lifting of a factorization. Lifting is basically the method of finding a factorization of a polynomial modulo higher powers of an ideal given a factorization modulo that ideal and subject to certain constraints. In our problem, we are restricted to working in the ring Z_{p^k} for some

prime p (the ideal is $\langle p \rangle$, an ideal of Z). The contents of this section are broadly based on the work by [vzGH96a], [vzGH96b] and the report by [Kli97].
First we need the notion of units in the ring $Z_{p^k}[x]$. An unit is defined as an element u such that $\exists u'$ in the same ring and we have $uu' = 1$.

Lemma 5.1: Given a polynomial $f(x)$ and a prime p we can write it as $f(x) = a(x) + pg(x)$ for $a(x) \in Z_p[x]$.
Proof : For $f(x) = \sum_i a_i x^i$ we can write it as $\sum_i (c_i + pb_i)x^i$ where c_i is the remainder on dividing a_i by p and b_i is the quotient. So we choose $g(x) = \sum_i b_i x^i$ and $a(x) = \sum_i c_i x^i$.

Theorem 5.2: For the ring $Z_{p^k}[x]$, an element is a unit if and only if it is of the form $a + pf(x)$ where $a \in Z_p \backslash \{0\}$ and $f(x) \in Z_{p^{k-1}}[x]$.
Proof: If we have a unit $u \in Z_{p^k}[x]$ and another element u' in the same ring such that $uu' = 1$. Now we know that $u = f_1 + pf_2$ and $u' = f_1' + pf_2'$ for some $f_1, f_1' \in Z_p[x]$ and $f_2, f_2' \in Z_{p^{k-1}}[x]$, from the previous lemma. From $uu' = 1$ in Z_{p^k} we have

$$(f_1 + pf_2)(f_1' + pf_2') = 1$$
$$\implies f_1 f_1' + p(\dots) = 1 + p.0$$
$$\implies f_1 f_1' = 1$$

Now f_1, f_1' are both polynomials and by multiplication their degrees cannot reduce. So we indeed have both of them as constants as right hand side of the equation does not consist of any variables. So $f_1, f_1' \in Z_p$ and since they are units they belong to the group of units, i.e. $Z_p \backslash \{0\}$.
Now for the only if direction. Suppose we have an element of the form $a + pf$ for $a \in Z_p$ and $f \in Z_{p^{k-1}}[x]$. So we have $f = a(1 - a^{-1}(-p)f)$. Consider the element obtained from the binomial expansion of $\frac{1}{1-h} = 1 + h + h^2 + h^3 + \dots$. We have

$$u^{-1} = a^{-1}(\frac{1}{(1 - a^{-1}(-p)f)}) = a^{-1}(1 + (a^{-1}(-p)f) + (a^{-1}(-p)f)^2 + \dots + (a^{-1}(-p)f)^{k-1})$$

This is true as the higher terms have a factor of p^k which is zero in Z_{p^k}. So we have an element u^{-1} which exists in $Z_{p^k}[x]$ such that $uu^{-1} = 1$, which implies u is a unit.
This also implies that if $f \mod p$ is a unit then $f \mod p^k$ is a unit as well, and vice versa.

Now we move on to finding factors of a polynomial in Z_{p^k} given a factorization in Z_p. We already have given factorizations in fields like in Z_p and in this section we introduce a lifting technique to "lift" this factorization to $\mod p^k$ from $\mod p$. This lifting technique is due to Hensel (explained in detail in [BS96]).

Theorem 5.3 [**Hensel's Lemma**] If p is a prime and $f, g, h \in Z[x]$ be polynomials with $\gcd(g, h) = 1$ in $Z_p[x]$ and $f \equiv gh \not\equiv 0 \mod p$ then there exists polynomials $\tilde{g}, \tilde{h}$ such that $f \equiv \tilde{g}\tilde{h} \mod p^k$ and $\tilde{g} \equiv g \mod p$, $\tilde{h} \equiv h \mod p$.
Proof: We give an algorithm for finding such $\tilde{g}$ and $\tilde{h}$. First find λ and μ in $Z_p[x]$, $\deg(\lambda) < \deg(h)$, $\deg(\mu) < \deg(g)$, such that $\lambda g + \mu h = 1 \mod p$ (This can be done using Extended Euclidean Algorithm which is explained in more detail in [vzGG99]).
Next we iteratively lift the factorization to modulo higher powers of p.

Algorithm 1: Hensel Lifting

Input : f, g, h, notation same as above
Output : $\tilde{g}, \tilde{h}$, notation same as above
For $i = 2, 3 \ldots k$; **do** {
$q \leftarrow \frac{f-gh}{p^{i-1}} \mod p$;
$u \leftarrow q\mu \mod g$;
$v \leftarrow q\lambda \mod h$;
$g \leftarrow g + p^{i-1}u$;
$h \leftarrow h + p^{i-1}v$;
};
return $\tilde{g} = g$, $\tilde{h} = h$;

The proof of correctness is my induction on i. Suppose that we have $f \equiv gh \mod p^{i-1}$, then the construction of q is valid as $p^{i-1}|f-gh$. Now it can be verified by substituting values of u, v, q and using the fact that $ug + vh \equiv q \mod g$ and $ug + vh \equiv q \mod h$ from which we get, using Chinese Remainder Theorem that $uh + vg \equiv q \mod p^i$, that $f - (g + p^{i-1}u)(h + p^{i-1}v) \equiv 0 \mod p^i$.
A more detailed proof can be found in [Kli97].

Theorem 5.4: Hensel's lifting is unique upto multiplication by units.
A proof of this can be found in [BS96].

Now notice that Hensel Lifting cannot be done if the polynomial does not factorize into coprime factors modulo p, which is basically when the polynomial f is of the form ϕ^n modulo p for some polynomial ϕ. [vzGH96a], [vzGH96b] had given algorithms by solving simultaneous equations to find the factorization of polynomials of these form. Before introduction to that algorithm we need to define Resultant of two polynomials.

Theorem 5.5: Let $f, g \in Z[x]$ be polynomials of degrees $l > 0$ and $m > 0$ respectively. Then f and g have a common factor of degree greater than or equal to 1 if and only if there exists polynomials A, B satisfying the conditions:

1. $A, B \neq 0$
2. $\deg(A) \leq m - 1$ and $\deg(B) \leq l - 1$
3. $Af + Bg = 0$

Proof: Suppose that we have f, g with a common factor h, $\deg(h) \geq 1$ and that $f = f_1 h, g = g_1 h$. Then consider the polynomials A, B as $A = g_1, B = -h_1$. It can be verified that all the three conditions are satisfied.
For the other direction, we are already given with polynomials A, B such that the three conditions are satisfied. Let us assume f, g does not have any common factor and hence their gcd is 1. So by Extended Euclidean Algorithm we can find polynomials A', B' with $\deg(B') <\deg(f)$, $\deg(B') <\deg(g)$ such that $A'f + B'g = 1$. Now since we have $Af + Bg = 0$, multiplying the previous equation by B we get

$$B = B(A'f + B'g) = A'Bf + B'(Bg) = (A'B - AB')f$$

Now we already had the condition that $B \neq 0$ and degree of B is strictly less than f which is violated by the above equation where the right hand side is either 0 or has a degree greater or equal to than that of f. This gives a contradiction and hence f and g must have a common factor of degree atleast 1.

Now in order to check if f and g have a common factor we need an algorithm to determine so. This problem reduced to finding a solution to a set of simultaneous equations. Let $A = c_0 + c_1 x + \ldots c_{m-1}x^{m-1}$ and $B = d_0 + d_1 x + \ldots d_{l-1}x^{l-1}$. We also write $f = a_0 + a_1 x + \ldots a_l x^l$ and $g = b_0 + b_1 + \ldots b_m x^m$. Substituting accordingly we get the set of simultaneous equations:

$$a_0c_0 \quad + \quad b_0d_0 \quad = 0 \qquad \text{Coefficient of } x^{l+m-1}$$

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

Now we introduce the sylvester matrix.

Definition 5.6 : Given polynomials f, g, notation as above, the Sylvester matrix of f and g is the coefficient matrix of the set of the above system of equations. Let us denote Sylvester matrix of f, g as $S(f, g)$ by the following $(l + m) \times (l + m)$ matrix:

$$\begin{pmatrix} a_l & & & & b_m & & \\ a_{l-1} & \ddots & & & b_{m-1} & \ddots & \\ \vdots & & \ddots & & \vdots & & b_m \\ & \ddots & & a_{l-1} & b_0 & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_0 & & & b_0 \end{pmatrix}$$

The empty spaces other than inside of the dots are filled with zero.
The Sylvester matrix is the coefficient matrix of the above system of equations. The resultant of polynomials f, g denoted by $Res(f, g)$ is the determinant of their Sylvester Matrix, i.e. $Res(f, g) = |S(f, g)|$.

Theorem 5.7: Given two polynomials $f, g \in Z[x]$, f and g have a common factor of degree greater than or equal to 1 if and only if $Res(f, g) = 0$.
Proof: f, g donot have a common factor when there exists polynomials A, B such that $Af + Bg = 1$. If we construct a vector of the form $\begin{pmatrix} A \\ B \end{pmatrix}$ them $S\times \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix}$ has a solution, i.e. the constant term is 1 and the rest of the coefficients of x^i are zero. Now they have a solution if $|S| \neq 0$, by Cramer's rule. From this the proof of Theorem 6.7 follows.

Theorem 5.8: Given $f, g \in Z[x]$, $\exists A, B \in Z[x]$ with degrees less than those of g and f respectively, such that $Af + Bg = Res(f, g)$.
Proof: If f, g have a common factor, then resultant is 0 and we know from Theorem 5.5 that these polynomials do exist. Suppose they donot have a common factor, we have A', B' with same degree constraints such that $A'f + B'g = 1$. Now from the equations:

$$\begin{array}{ccccccc} a_0c_0 & + & b_0d_0 & = 0 & & \text{Coefficient of } x^{l+m-1} \\ a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 = 0 & & & \text{Coefficient of } x^{l+m-2} \\ \ddots & & \ddots & \vdots & & \vdots \\ a_lc_{m-1} & + & b_md_{l-1} & = 1 & & \text{Coefficient of } x^0 \end{array}$$

We can solve these equations by Cramer's rule to give the determinant with some coefficients in the numerator and the determinant of the Sylvester matrix in denominator to give:

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

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

for some polynomials A and B, which we can find as we know A', B' from Extended Euclidean Algorithm. Now from $A'f + B'g = 1$ it follows that for such A, B, we have $Af + Bg = Res(f, g)$ where $\deg(A) = \deg(A')$, $\deg(B) = \deg(B')$.

Definition 5.9: We define the discriminant of a polynomial $f(x) = a_0 + a_1x + \dots a_lx^l$ as

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

where f' is the derivative of $f(x)$ wrt x.

We will denote $r(f, g) = v_p(f, g)$ and $d(f, g) = v_p(f, g)$ for polynomials $f, g \in Z[x]$ and prime p.

Theorem 5.10 [**Hensel's Lemma II**] Given a prime p, $k \in N$ and polynomials $f, u, w \in Z[x]$ of degrees $n + m, n, m$ respectively satisfying the following properties:

1. $f \equiv uw \mod p^k$ with $lc(f) = lc(uw)$
2. $Res(u, w) \neq 0$
3. $k \geq 2r(u, w)$

Then there are polynomials $g, h \in Z_{p^t}[x]$ such that $f \equiv gh$ in Z_{p^t}, $g \equiv u \mod p^{k-r(u,w)}$, $h \equiv w \mod p^{k-r(u,w)}$ for every t.
Proof: We provide an algorithm from which the proof follows. We have to inductively construct polynomials $\phi_i, \psi_i \in Z[x]$ such that if $f = ab \mod x^{k+i-1}$ with $a, b \in Z[x]$ with $a \equiv u \mod p^{k-r(u,w)}$, $b \equiv w \mod p^{k-r(u,w)}$, then we will have

$$f \equiv (a + p^{k-r(u,w)+i+1}\psi_i)(b + p^{k-r(u,w)+i+1}\phi_i) \mod p^{k+i}$$

Now from the fact that $a \equiv u \mod p^{k-r(u,w)}$, $b \equiv v \mod p^{k-r(u,w)}$, it can be shown that $r(a, b) = r(u, w)$. More elaborate proof can be found in Lemma 3.10 of [vzGH96a]. From theorem 6.8 we have polynomials A, B such that

$$res(a, b) = Aa + Bb$$
$$\implies Aa + Bb = p^{r(a,b)}l = p^{r(u,w)}l$$

for some polynomial l. Considering $\phi_i = A$ and $\psi_i = B$ the lifting properties can be verified, i.e. we can show

$$f - (a + p^{k-r(u,w)+i+1}\psi_i)(b + p^{k-r(u,w)+i+1}\phi_i) \equiv 0 \mod p^{k+i}$$

This proves Theorem 5.10.

This can be extended when f has more than 2 factors. Let $f = \Pi_{1 \leq i < l} g_i$ over $Z_{(p)}$, with $disc(f) \neq 0$, $l \geq 1$and $g_i \in Z_{(p)}$ be monic and irreducible for all i. Let $f \equiv gh \mod p^k$ with $g, h \in Z[x]$ and $k > d(f)$. Then there exists a partition $\{1, 2, \dots, l\} = S \cup S'$ such that $g \equiv \Pi_{i \in S} g_i \mod p^{k-\sigma)}$ and $h \equiv \Pi_{j \in S'} g_j \mod p^{k-\sigma}$ where $\sigma = r(\Pi_{i \in S} g_i, \Pi_{j \in S'} g_j)$.

This above lifting procedures given were when f had two coprime factors. However we cannot continue the same if f is a perfect power of some other polynomial. For this here is an algorithm for lifting proposed in the paper [vzGH96b].
Theorem 5.11 : Let $f \equiv uw \mod p^k$ and $f \equiv g^e \mod p$ for some polynomial g which is irreducible over $Z_p[x]$ and $e \geq 2$. We also have u, w as monic and $u \equiv g^l \mod p, w \equiv g^{e-l} \mod p$ for some $l \leq \frac{e}{2}$. Then the following are equivalent:

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

Proof: For (1) $\implies$ (2) we have $\frac{f-uw}{p^k} \equiv g^l\alpha \mod p$ for some $\alpha \in Z[x]$. For any ϕ, choose $\psi = \alpha - g^{e-2l}\phi \mod p$. From this is can be verified that $f \equiv (u+p^k\phi)(w+p^k\psi) \mod p^{k+1}$.
Now we have (2) $\implies$ (3) $\implies$ (4) trivially.
For (4) $\implies$ (1), let we have ϕ, psi as mentioned such that $f \equiv (u+p^k\phi)(w+p^k\psi) \mod p^{k+1}$. Then

$$\frac{f-uw}{p^k} \equiv \phi w + \psi u \equiv g^l(\phi g^{e-2l} + \psi) \mod p$$

This is the proof of theorem 5.11.

For using 6.11 we need to find a proper ϕ with coefficients as variables satisfying lifting condition such that the lifting continues for more powers than p^{k+1}. However these unknowns get really messy and some examples can be found in [vzGH96b].

6 Representative Roots and the ROOT-FIND Algorithm

Rings of the form Z_{p^k} for some prime p and integer $k \geq 1$ are not integral domains and hence polynomials of degree d can have more than d roots. The goal of this section is to use an algorithm which returns all the roots of the polynomial in randomized polynomial time. However the roots of a polynomial can be exponentially many, for which we use the concept of representative roots.
For example the polynomial $f(x) = x^2 - 9x + 8$ in Z_{7^4} has the set of roots $\{1, 8, 344, 351, 687, 694, 1030, 1037, 1373, 1380, 1716, 1723, 2059, 2066\}$, which are of the order $O(p^i)$, which is exponentially many. However it can be seen that all the roots of a polynomial in Z_{p^k} can be decomposed into sets of form $a + p^i y$ for some $a \in Z_{p^i}$ and $\forall y \in Z_{p^{k-i-1}}$. This gives us a notion of representative roots.
Representative roots are roots of a polynomial written in the form $a + p^i *$ which means that all the roots have the form $a + p^i y$ for every $y \in Z_{p^{k-i-1}}$. The symbol $*$ represents the entire ring $y \in Z_{p^{k-i-1}}$ and a is a p-adic integer. This can be seen as a compact datastructure to represent exponentially many values (exponential in $\log p$). For a in the form $a_0 + a_1 p + a_2 p^2 + \ldots a_{i-1} p^{i-1}$ for some a_j's $\in Z_p$ then we have the set of representative roots as

$$S_a = \{a_0 + a_1 p + a_2 p^2 + \ldots a_{i-1} p^{i-1} + y_1 p^i + y_2 p^{i+1} + \cdots + y_{k-i} p^{k-1} | y_j \in Z_p\}$$

We will consider $*$ as an entire ring, R and the following convention of writing will be followed:

- $u + \{*\} = \{u + *\}, u\{*\} = \{u*\} \forall u \in R$
- $c + \{a + b*\} = \{(a + c) + b*\}, c\{a + b*\} = \{ca + cb*\} \forall a, b, c \in R$

Representative roots and the notation $\{*\}$ has been explained in greater detail in the recent paper [DMS19] which gives a factorization technique for polynomials upto modulo p^4

Definition 6.1: For a p-adic number n of the form $a_0 + pa_1 + p^2 a_2 + \ldots p^m a_m$, we define the i^{th} coordinate of n as the coefficient of p^i in its p-adic representation, i.e. a_i in this case.

Definition 6.2: For two p-adic numbers l and n we say they are truncated upto i if j^{th} coordinate for both l and m are equal for $0 \leq j \leq i$. We say,

$$tr_p(l, m) = i$$

In our problem we use the ROOT-FIND algorithm introduced in [BLQ13] to give all the representative roots of a given polynomial in a ring of the form Z_{p^k} in randomized polynomial time. A better and more generalized version of that algorithm can be found in [DMS19].

Theorem 6.3 A polynomial of degree d over $Z/p^k Z$ can have atmost d many representative roots, all of which are returned by the ROOT-FIND algorithm.
A proof of Theorem 6.3 can be found in [BLQ13]

7 Main Results: Factorization using Representative Roots

Next we move on to factorization of polynomials using the representative roots obtained from the ROOT-FIND algorithm. We want to give a factorization such that we can get highest number of linear factors. We approach this problem with low degree polynomials looking at properties of roots and factorizations.

7.1 Degree 2 polynomials

Suppose we have a quadratic polynomial $f(x) = x^2 + ax + b$ in Z/p^kZ, where p is a prime. Using ROOT-FIND suppose we have a root $A + p^i*$ for some $A \in Z/p^iZ$ and $i < k, i \in Z$.

Theorem 7.1.1: For a quadratic polynomial in $f(x) = x^2 + ax + b$ in Z/p^kZ, given a representative root $r = A + p^i*$, we have a factorization $f(x) = (x - r)(x + (a + r)) \mod p^k$, where $r' = -(a + r)$ is another representative root.
Proof: To find a factorization the basic idea is to perform long division. We already know that, since it is a quadratic, any root r corresponds to a factor $(x - r)$ and by long division the quotient on dividing $f(x)$ by $(x - r)$ yields $(x + a + r)$, which is another factor of $f(x)$. This can be verified easily using the fact that $f(r) = r^2 + ar + b = 0 \mod p^k$.
So for a representative root $A + p^i*$, let us fix a variable $y \in *$, i.e. $y \in Z/p^{k-i-1}Z$, and hence $A + p^iy$ is a root of $f(x)$. Now we consider y as a variable and this represents a set of roots of $f(x)$ denoted by the same representative root for different values of y. Dividing $f(x)$ by $(x - (A + p^iy))$ gives the factor $(x+(a+A+p^iy))$, and hence giving a factorization pattern. For each value of $y \in *$, i.e. $y \in Z/p^{k-i-1}Z$, we will have a factorization determined by this.
From this we infer that the other representative root is $r' = -(a+A+p^i*)$. So r and r' differ in the fixed coordinate (the first i coordinates) by $a \mod p^i$ with a negative sign, and for each value of y as above in r, the corresponding coordinate will be negative of the coordinate in y added to the same coordinate in a.

Corollary 7.1.2 The $*$ in both representative roots of a quadratic have the same cardinality.
This means if the representative roots are $r_1 = \alpha_1 + p^{i_1}*$ and $r_2 = \alpha_2 + p^{i_2}*$, then $i_1 = i_2$.
Proof: This is true as for each value of y as in the previous proof there exists a factorization in linear which gives a corresponding root.

7.2 Degree 3 Polynomials

For a given polynomial $f(x) = x^3 + ax^2 + bx + c$ in Z/p^kZ, we attempt to find a factorization such that we get three linear factors.

From ROOT-FIND algorithm we can get sets of three distinct representative roots. If any two of them are equal then $f(x)$ is not square free but we can easily make it square free by checking which of its representative roots is a root of its derivative as well, and removing the linear factor for the root.
Hence we can assume that we have three distinct representative roots and attempt to find a factorization. The next theorem gives us an idea to find an algorithm to find the factors in terms of representative roots of the polynomial.

Theorem 7.2.1: If three distinct representative roots exist then we have a factorization containing three of them together.
Proof: This means if the roots are $r_1 = \alpha_1 + p^{i_1}*$, $r_2 = \alpha_2 + p^{i_2}*$, $r_3 = \alpha_3 + p^{i_3}*$ (where each of $i_1, i_2, i_3 < k$, as if they are exactly k, then we can divide by the linear factor corresponding to that root and continue with the degree 2 case), then we will have factorization $f(x) = (x - a_1)(x - a_2)(x - a_3)$ for some $a_1 \in r_1$, $a_2 \in r_2$, $a_3 \in r_3$. Since all the values of r_1, r_2, r_3 are roots of $f(x)$ and roots from all three sets of representative roots are present we will often write the factorization as $(x - r_1)(x - r_2)(x - r_3)$.
Proof: Suppose that there exists a factorization $f(x) = (x - a_1)(x - a_1')(x - a_3)$, where $a_1, a_1' \in r_1$, $a_3 \in r_3$. This can be written as $(x - (\alpha_1 + p^{i_1}y_1))(x - (\alpha_1 + p^{i_1}y_1'))(x - (\alpha_3 + p^{i_3}y_3))$, where y_i's belong to the corresponding $*$ set of each representative root.
Now this factorization of $f(x)$ will give powers of p greater than k for all values of x in r_2, as they are

the roots in Z/p^kZ. Now since $i_3 < k$, $tr_p(a_2, \alpha_)$ some power of p needs to be generated from the factors $(x - a_1), (x - a_1')$ to make it divisible by p^k. For this to occur, let any value $a_2 \in r_2$ be truncated with a_1 till r, a_1' till s, a_3 till t. So we must have $r + s + t \geq k$ as the power of p in their difference is exactly the index upto which it is truncated. We will use this fact to arrive at a contradiction.
First let us assume that $i_1 > i_2$. Now we know that $i_3 < k$ and hence some power of p must come from the first two factors when we evaluate the factorization with values from r_2. Now since $f(x)$ is zero modulo p^k for all values of r_2, i.e. $\alpha_2 + p^{i_2}*$, we will have values from r_1 truncated at a point which belongs to the constant part of r_2, i.e. truncated upto $\leq i_2$. This is true as a_1 and a_1' are fixed and for all values from r_2 it is divisible by p^k. Hence the index of truncation for each $a_2 \in r_2, f(a_2) = 0$ with a_1 and a_1' is always less than or equal to i_2.
Let $j = max(\{tr_p(a_2, a_1) \mid a_2 \in r_2\}, \{tr_p(a_2, a_1') \mid a_2 \in r_2\})$. We have $j < i_1$.
Also any number in a_1 or a_1' with coordinate greater than j do not result in making the powers of p less than k, and hence for any value in coordinates higher than j we will have p^k dividing it, i.e. a representative root of $f(x)$ in Z/p^kZ. But this root is a superset of r_1 and we already have r_1 as a distinct root with a definite i_1. But now we are getting another representative root truncated with r_1 upto j, which is a contradiction. Hence this case of $i_1 > i_2$ cannot give a factorization as above.
Now we assume $i_1 \leq i_2$. For any root $a_2 \in r_2$, it will be truncated upto less than i_2 places with both a_1 and a_1'. WLOG if it was truncated upto i_2 places (cannot be more than i_2 as after that we can use any value in $*$) with a_1, then a_1 would be a value in r_2 itself. So the factorization will now be of a form $(x - r_1)(x - r_2)(x - r_3)$ as desired. So we can say that it is truncated upto less than i_2 coordinates, i.e., upto some coordinate in α_2.
Now suppose $j = max(tr_p(a_1, \alpha_2), tr_p(a_1', \alpha_2))$. We have $j \leq i_1 < i_2$ (if $i_1 = i_2$, then having them truncated to i_1 would mean that they belong to the same set of representative roots and $\alpha_1 = \alpha_2$, but we have r_1 and r_2 as distinct) and with the similar arguement as above, this already generates a k power of p and the coordinates after j in r_2 can be anything. This again shows a contradiction as we have another representative root which is a superset of r_2 while we had a distinct representative root r_2 from the ROOT-FIND algorithm and pre-processing as explained before. Hence we cannot have a factorization as above too.
From this we conclude that a factorization of $f(x)$ must be of the form $(x - r_1)(x - r_2)(x - r_3)$.

From this we extend with the idea of an algorithm to find the factorization of a cubic polynomial in the ring Z_{p^k}.

Our main idea is to consider the factorization $(x - (\alpha_1 + p^{i_1}y_1))(x - (\alpha_1 + p^{i_1}y_1'))(x - (\alpha_3 + p^{i_3}y_3))$ in terms of the variables y_1, y_2, y_3, with notation same as the proof of theorem 8.2.1. Now we can expand this sum to find equations in terms of y_1, y_2, y_3 (more specifically $p^{i_1}y_1, p^{i_2}y_2, p^{i_3}y_3$) and comparing with the coefficients of $f(x) = x^3 + ax^2 + bx + c$ we get a set of simultaneous equations modulo p^k. We can also eliminate $p^{i_3}y_3$ by replacing it with $p^{i_1}y_1y_3 = -(a + \alpha_1 + p^{i_1}y_1 + \alpha_2 + p^{i_2}y_2 + \alpha_3)$ and solving the remaining equations for the rest of the roots.
However if we have less than 3 representative roots we can apply the same approach after checking its with its derivative in rings $Z_{p^{i_j}}$ for each j and separate out the repeating linear factor.

8 Future Work

We next want to move on to a general polynomial. However for that intuitively if we can find some factorization technique for degree 4 we can extend that idea to higher degrees.
For degree 4 polynomials the same proof does not proceed through for every case. Suppose that we want to use the same proof as of theorem 8.2.1. Let us assume that the monic polynomial $f(x)$ has 4 sets of representative roots r_1, r_2, r_3, r_4 and WLOG let us assume there exists a factorization $(x - a_1)(x - a_1')(x - a_3)(x - a_4)$ with $a_1, a_1' \in r_1, a_3 \in r_3, a_4 \in r_4$. We can now proceed with the same proof only if we have the condition $tr_p(r_2, a_3) + tr_p(r_2, a_4) < k$. However this might not always be the case, which raises the next question.

Question 8.1: Given a degree ≤ 4 polynomial modulo p^k with representative roots of the form

$\alpha_j + p^{i_j} *$, $\alpha_j \in Z_{p^{i_j}}$, what can be the maximum value of $|i_j - i_k|$.
For case of degree 2 we know that this is 0, however no such results have yet been discovered for higher degree polynomials.

Another question that can be raised for degree 3 polynomials modulo p^k is the following:

Question 8.2: For representative roots r_1, r_2, r_3, if $i_j + \sum_{m!=j} tr_p(\alpha_j, \alpha_m) \geq k$, notation as above, we will be able to arrive at a similar contradiction. What will this imply? Will it mean that $i_1 = i_2 = i_3$ or it will imply something else?

Now moving on to the case of degree 4, the following contains some ideas and intuitions into factoring using similar techniques.
As discussed in the case of degree 3 we can attempt to consider variables $y_i's$ to fix from the $*$ part of the representative roots and continue with solving equations. When we have a root the rest of the factorization reduces to the factorization of degree 3 case which has been illustrated in section 7.2. In order to fix the variables we need to find the representative root to which that part of the factor belongs to, which can be checking by factorizing the polynomial upto $\mod p^{i_j}$ for each j and checking if the rest of the part gives us linear factors. Also if there are more than one linear factor from the same representative root, we can check the gcd, if exists, with its derivative, modulo each of p^{i_j}. In this way we may proceed to handle the case of degree 4.
However, this method can get messy for higher degrees but there might be a way to reduce the solution of the set of equations to finding roots of polynomials of lesser degrees. Also since it has multivariates another approach might be to first find a bivariate factorization by extending the technique given in this paper using the way Kaltofen did in [Kal82] using Hensel Lifting. Solving this might lead to solving another problem proposed by [DMS19] on bivariate factorization applied to ROOT-FIND algorithm.

Furthermore instead of looking at maximum possible linear factors it might be interesting to proceed into the question of finding maximum possible factors, for example, if a degree 5 polynomial has two irreducible factors of degrees 1 and 4 or if it has 3 factors of degrees $1, 2$ and 2, by probably inductively considering factorizations of lower degrees solved before that.

References

[**Ber67**] Elwyn R. Berlekamp, Factoring polynomials over finite fields, *Bell System Technical Journal*, 46(8):1853-1859, 1967.

[**Bha97**] Manjul Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *Journal für die reine und angewandte Mathematik*, 490 (1997): 101-128, 1997.

[**Bha00**] Manjul Bhargava, Factorial Function and Generalizations, *The American Mathematical Monthly*, 107(9): 783-799, 2000.

[**BLQ13**] Jeremy Berthomieu, Gregoire Lecerf and Guillaume Quintin, Polynomial root-finding over local rings and application to error correcting codes, *Applicable Algebra in Engineering, Communication and Computing*, 24(6):413–443, 2013.

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

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

[**CG00**] David G Cantor and Daniel M Gordon, Factoring polynomials over p-adic fields, *International Algorithmic Number Theory Symposium*, pg 185–208.Springer, 2000.

[**Chi87**] AL Chistov, Efficient factorization of polynomials over local fields, *Dokl. Akad. Nauk SSSR*, 293(5):1073-1077, 1987.

[**CZ81**] David G. Cantor and Hans Zassenhaus, A new algorithm for factoring polynomials over finite fields, *Mathematics of Computation*, pg 587-592, 1981.

[**DM97**] Bruce Dearden and Jerry Metzger, Roots of Polynomials Modulo Prime Powers, *European Journal of Combinatorics*, 18(6): 601-606, 1997.

[**DMS19**] Ashish Dwivedi, Rajat Mittal and Nitin Saxena, Efficiently factoring polynomials modulo p^4, *International Symposium on Symbolic and Algebraic Computation*, pg 139-146, 2019

[**Kal82**] Erich Kaltofen, A polynomial-time reduction from bivariate to univariate integral polynomial factorization, 23^{rd} *Annual Symposium on Foundations of Computer Science*, pg 57-64, 1982.

[**Kli97**] Adam Klivans, Factoring Polynomials Modulo Composites, *SCS Technical Report Collection*, School of Computer Science, Carnegie Mellon University, 1997.

[**KU11**] Kiran S. Kedlaya and Christopher Umans, Fast polynomial factorization and modular composition, *SIAM Journal on Computing*, 40(6):1767-1802, 2011.

[**Lan85**] Susan Landau, Factoring polynomials over algebraic numberfields, SIAM Journal on Computing, 14(1):184–195, 1985.

[**LLL82**] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and Lazlo Lovasz, Factoring polynomials with rational coefficients, *Mathematische Annalen*, 261(4):515–534,1982.

[**vzGG99**] Joachim von zur Gathen and Jurgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge, UK, 1999.

[**vzGH96a**] Joachim von zur Gathen and Silke Hartlieb, Factoring modularpolynomials, *Proc. ISSA C*, 1996.

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

[**vzGH98**] Joachim von zur Gathen and Silke Hartlieb, Factoring modular polynomials, *Journal of Symbolic Computation*, 26(5):583–606, 1998.