Factorization of Polynomials modulo prime powers

Sayak Chakrabarti
Roll No- 170648
Supervised by: Prof. Rajat Mittal

Contents

Introduction

- Question of factorization has been a fundamental question in mathematics and computer science
- Several polynomial factorization over rings have been achieved by [Ber67], [CZ81], [KU11] in finite fields, [LLL82] over rationals, [Lan85] over number fields, [Chi87], [CG00] over p-adic fields etc
- We deal with rings of the form $\mathbb{Z}n$
- Chinese Remainder Theorem implies factorization over $\mathbb{Z}n \Rightarrow$ factorization over $\mathbb{Z}pk$

Problem Statement

- Given a prime p and a ring $\mathbb{Z}p^k$ for some integer $k \geq 1$, and a monic polynomial f(x)
- We want to find a factorization such that maximum number of distinct linear factors exist

Example:

Consider the polynomial f(x) = x^2 mod p^2. We want to find a factorization technique that returns (x-p)(x+p) instead of x.x

Preliminaries

- All polynomials are monic and have integer coefficients
- p will denote a prime, unless specified and k an integer greater than or equal to 1
- For any set $S \subseteq R$ where R is any ring, we denote $a.S = \{a.s \mid s \in S\}$ and $a+S = \{a+s \mid s \in S\}$

Root Sets of Polynomials modulo prime powers

- Based on the paper [DM97]

- **Definition:** Root set R modulo n refers to the set of integers in $\mathbb{Z}n$ such that there exists a polynomial with integer coefficients the roots of which are exactly all the elements of R

The non trivial nature of this statement can be seen from the fact that {0, p} is not a root set modulo p^2 as it will contain all the multiples of p as well

Root Sets of Polynomials modulo prime powers

Some main results from [DM97] are:

- If R is a root set modulo a prime power p^k then Rj = {r | r ∈ R, r ≡ j mod p} is another valid root set
- A root set R can be decomposed into R = R1UR2UR3…UR{p-1}
- For a root set R, j+R is also a valid root set for any j ∈ [p-1]

p-ordering Sequences

We are interested in p-ordering sequences over integers which were introduced in the paper [Bha00]. A generalization of p-ordering sequences over Dedekind rings was first introduced in [Bha97]. In order to define p-ordering sequences we need the following definition

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

$v_p(a) = v$ if $a \neq 0$ and v is the maximum power of p dividing a

$= \infty$ if $a = 0$

p-ordering Sequences

For a prime p and a given subset of integers S, a p-ordering sequence is defined inductively as follows:

- Choose an element a0 $\in$ S
- Choose a1 $\in$ S such that vp(a1-a0) is minimum
- Choose a2 $\in$ S such that vp((a2-a0)(a2-a1)) is minimum

⋮

- Choose ak $\in$ S such that vp((ak-a0)(ak-a1) . . . (ak-a{k-1})) is minimum

Factorial Function Generalization

Our next goal is to generalize factorial functions over arbitrary subsets of integers to show an important application of p-ordering sequences. Before that we need a couple of definitions.

Definition: We define vp(S,k) as the power of the prime p in the product (ak−a0)(ak−a1)...(ak−a{k−1}) where {an} forms the p-ordering sequence

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

Factorial Function Generalization

The factorial function of a setSuptokterms is denoted by k!_S and is defined as:

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

Factorial Function Generalization

Some lemmas proved in [Bha00] to show how this generalized factorial function behaves similarly like normal factorial function over integers are:

- For non-negative integerskandl, (k+l)!_S is a multiple of k!_Sl!_S.
- For a primitive polynomial f of degree k, we have d(S,f)|k!_S where d(S, k) = gcd{f(a) | a ∈ S}
- The number of polynomials fromStoZnis given by Π^{n−1}_{k = 0} n / gcd(n,k!_S)

Significance of p-ordering

From this we note thatp-ordering sequence behaves as normal factorials too. Also suppose that{an}is ap-ordering sequence inSthenakis a root off(x) = (x−a1)(x−a2)...(x−a_{k−1}) mod p^vp(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.

Lifting of Factorizations

We already have factorizations of polynomials in fields of the form $\mathbb{Z}p$. Lifting are techniques to to “lift” this factorization to rings of the form $\mathbb{Z}pk$ (modulo higher powers of the ideals).

Kurt Hensel gave a phenomenal lifting called the Hensel Lifting in which, given a polynomial f and a factorization of $f \equiv gh \bmod p$ where $\gcd(g, h) = 1$, then we can lift this factorization to $f \equiv g'h' \bmod p^k$ for any $k \geq 1$ such that $g' \equiv g$ and $h' \equiv h \bmod p$

Hensel lifting has been explained in greater detail in [BS96]

However Hensel Lifting cannot proceed if g and h are not coprime, more specifically if f(x) is a perfect power of some other polynomial modulo p.

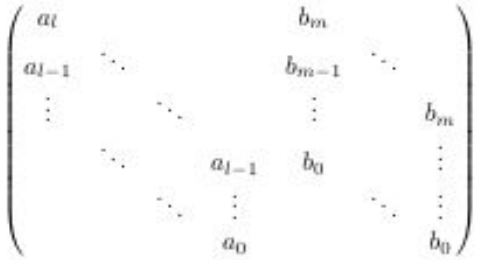
Resultants

Now we can prove that for any two polynomials f and g, there exists polynomials A, B with deg(A) < deg(g), deg(B) < deg(f) and Af+Bg = 0 if and only if f and g have a common factor. This motivates us to solve the following set of equations to find A and B.

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

Resultants

This motivates us to define the matrix with the coefficients of the polynomials f and g as follows:



This matrix is called the sylvester matrix of f and g, S(f, g). The determinant of this matrix is called the resultant denoted as res(f, g) = |S(f, g)|

Hensel's Lemma II

[vzGH96a] gave the Hensel's Lemma II to provide a more general version of the Hensel's Lifting. However the same problem of coprimality of factors are required, and we will show an example of how lifting behaves if we do not have this condition, explained in more details in [vzGH96b].

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

Hensel Lifting II

According to the algorithm presented by [vzGH96] for polynomials f, u, w $\in \mathbb{Z}[x]$ of degrees m+n, m, n respectively, if they satisfy the following properties:

1. $f \equiv uw \bmod p^k$
2. Res(u, w) is not zero
3. $k \geq 2r(u, w)$

Then we have a lifting to modulo p^i for every $i > k$.

[vzGH96b] extended this idea when f is a perfect power of some polynomial modulo p to give a lifting in terms of variables that can be solved using simultaneous equations.

Representative Roots

Next we want to find all the roots of a polynomial in a ring of the form $\mathbb{Z}pk$. However as noted earlier, a polynomial can have exponentially many roots (exponential in log p) in this ring. So we give an idea of representative roots which acts as a compact datastructure to represent these roots in polynomial space.

Representative roots are roots of a polynomial in the form A+p^i* where A $\in$ $\mathbb{Z}pi$ and * represents the entire ring ($\mathbb{Z}p^{k-i}$) that will follow after this. A representative root S_a (a set) has the canonical form:

$$S_a=\{a_0 + a_1p + a_2p^2 + \ldots a_{i-1}p^{i-1}+y_1p^i+y_2p^{i+1}+\cdots+y_{k-i}p^{k-1} \mid y_j \in Zp \}$$

Representative Roots

To find all the representative roots of a given polynomial, an algorithm called the ROOT-FIND algorithm first introduced in [BLQ13] and further modified and generalized to other rings in [DMS19] can be used. This algorithm runs in randomized polynomial time.

[BLQ13] also proves that for a polynomial of degree d there exists atmost d many representative roots.

Main Results

Next we move on to our main results where we factorize polynomials of degrees 2 and 3 separately. After that we will move on to future work and how to proceed to higher degree cases.

Degree 2 Case

Theorem: For a quadratic polynomial inf(x) =x^2+ax+b in $\mathbb{Z}$pk[x], 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 the other representative root.

This theorem can be easily proved by taking a variable y for a root A+p^iy, treating it as a constant and dividing f(x) by x-(A+p^iy). For different values of y we can check when r and r’ are not equal.

Degree 3 Case

For this case we give a theorem that provides us an understanding about how the factorizations behave when decomposed into linear factors.

Theorem: When 3 representative roots of a polynomial exist we have a factorization into linears such that elements from each representative root occur, i.e. if there is a factorization (x-a_1)(x-a_2)(x-a_3) then a_1, a_2, a_3 belong to different representative root sets.

Degree 3 Case: *Proof Idea*

Proof by contradiction by assuming in factorization into linears 2 roots fom same representative roots exist.
(x-(a_1+p^{i_1}y_1))(x-(a_1+p^{i_1}y'_1))(x-(a_3+p^{i_3}y_3)) be a factorization with the first two roots from r_1 and the third from r_3
Main idea is to try with all values of x in r_1 if i_1 < i_3 to show that i_3 is not maximal (Contradiction to a_3 being completely fixed and hence * would be a greater set).
If i_1>i_3 then try with all values of x in r_3 and this will give a similar contradiction.

Degree 3 Case: *Factorization*

For factorization we fix variables y_1, y_2, y_3 for the * part of each of the three representative roots to give factorization of the form (x-(a_1 + p^{i_1}y_1)(x-(a_2+p^{i_2}y_2)))(x- (a_3 + p^{i_3}y_3)).

Now we can solve for y_1, y_2, y_3 comparing coefficients with f(x).

Future Work

Our next goal would be to generalize a factorization in degree 4 case. However nothing about the nature of factorization and its roots has been proven yet. However if we want to arrive at a contradiction like degree 3 case, assuming a factorization of the form (x-a_1)(x-a'_1)(x-a_3)(x-a_4) exists with a_1, a'_1 in r_1, a_3 in r_3 and a_4 in r_4 then we need the condition tr_p(r_2, a_3) + tr_p(r_2, a_4) < k. This motivates the following question:

Question: Given a polynomial and its representative roots of the form A_j+p^{i_j}* , what can be the maximum value of {i_j-i_k}?

Future Work

Another contradiction can be brought from the proof of case of degree 3 which gives us the question:

Question: For representative roots r_1, r_2, r_3, if i_j + Σ_{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?

Future Work

Another way to approach the degree of case 4:

- Consider representative roots and fix variables y_1, y_2, y_3, y_4 for the * part
- Reduce to case of lower degrees (that of 3)

A question raised in [DMS19] asks if the factorization given there can be extended to bivariates. A same problem can be proposed after case 3 which can lead to case 4 getting solves. [Kal82] in his paper gave a bivariate factorization using Hensel's Lifting applied to univariate factorization.

Thank you!!

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 Functions and Generalizations, *The American Mathematical Monthly*, 107(9): 783-799, 2000.

[BLQ13] Jeremy Berthomieu, Grégoire 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, Cambridge, 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 Laszlo 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. ISSAC*, 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.