Journal of Symbolic Computation 104 (2021) 805–823

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Efficiently factoring polynomials modulo p^4

Ashish Dwivedi, Rajat Mittal, Nitin Saxena

CSE, Indian Institute of Technology, Kanpur, India

ARTICLE INFO

Article history:
Received 5 November 2019
Received in revised form 22 July 2020
Accepted 6 October 2020
Available online 15 October 2020

Keywords:
Efficient
Randomized
Factor
Local ring
Prime-power
Hensel lift

ABSTRACT

Polynomial factoring has famous practical algorithms over fields–finite, rational and p-adic. However, modulo prime powers, factoring gets harder because there is non-unique factorization and a combinatorial blowup ensues. For example, $x^2 + p \bmod p^2$ is irreducible, but $x^2 + px \bmod p^2$ has exponentially many factors in the input size (which here is logarithmic in p)! We present the first randomized poly($\deg f, \log p$) time algorithm to factor a given univariate integral polynomial f modulo p^k, for a prime p and $k \leq 4$.[1] Thus, we solve the open question of factoring modulo p^3 posed in (Sircana, ISSAC'17).

Our method reduces the general problem of factoring $f \bmod p^k$ to that of *root finding* of a related polynomial $E(y) \bmod \langle p^k, \varphi(x)^\ell \rangle$ for some irreducible $\varphi \bmod p$. We can efficiently solve the latter for $k \leq 4$, by incrementally transforming E. Moreover, we discover an efficient refinement of Hensel lifting to lift factors of $f \bmod p$ to those mod p^4 (if possible). This was previously unknown, as the case of repeated factors of $f \bmod p$ forbids classical Hensel lifting.

E-mail addresses: ashish@cse.iitk.ac.in (A. Dwivedi), rmittal@cse.iitk.ac.in (R. Mittal), nitin@cse.iitk.ac.in (N. Saxena).
URLs: https://www.cse.iitk.ac.in/users/ashish (A. Dwivedi), https://www.cse.iitk.ac.in/users/rmittal (R. Mittal), https://www.cse.iitk.ac.in/users/nitin (N. Saxena).

[1] A preliminary version of the paper was presented at the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC), 2019 Dwivedi et al. (2019b). The current journal version includes new sections and algorithms for better exposition with relevant non-trivial examples to explain the algorithms. It also contains a complete proof for factoring $f \bmod p^3$ which was left unproven in the conference version.

https://doi.org/10.1016/j.jsc.2020.10.001
0747-7171/© 2020 Elsevier Ltd. All rights reserved.

1. Introduction

Polynomial factorization is a fundamental question in mathematics and computing. In the last decades, quite efficient algorithms have been invented for various fields, e.g., over rationals (Lenstra et al., 1982), number fields (Landau, 1985), finite fields (Berlekamp, 1967; Cantor and Zassenhaus, 1981; Kedlaya and Umans, 2011) and p-adic fields (Chistov, 1987; Cantor and Gordon, 2000; Guàrdia et al., 2012). Being a problem of fundamental theoretical and practical importance, it has been very well studied; for more background refer to surveys, e.g., Kaltofen (1992); von zur Gathen and Panario (2001); Forbes and Shpilka (2015).

The same question over *composite* characteristic rings is believed to be computationally hard. For instance it is related to integer factoring (Shamir, 1993; Klivans, 1997). What is less understood is factorization over a local *ring*; especially, ones that are the residue class rings of $\mathbb{Z}$ or $\mathbb{F}_q[z]$. A natural variant is as follows.

Problem. Given a univariate integral polynomial f and a prime power p^k, with p prime and $k \in \mathbb{N}$; output a nontrivial factor of f mod p^k in randomized poly$(\deg f, k\log p)$ time.

Note that the polynomial ring $(\mathbb{Z}/\langle p^k\rangle)[x]$ is *not* a unique factorization domain. So f may have a number of factorizations exponential in the input size (which in our setting is $\deg(f)\log p$). For example, x^2+px has an irreducible factor $x+\alpha p$ mod p^2 for each $\alpha \in [p]$ and so x^2+px has exponentially many (wrt $\log p$) irreducible factors modulo p^2. This leads to a total breakdown in the classical factoring methods.

We give the first randomized polynomial time algorithm to non-trivially factor (or test for irreducibility) a polynomial f mod p^k, for $k \le 4$.

Additionally, when f mod p is a power of an irreducible, we provide (and count) all the lifts mod p^k *($k \le 4$) of any factor of f mod p, in randomized polynomial time.*

Usually, one factors f mod p and tries to "lift" this factorization to higher powers of p. If the former is a coprime factorization then Hensel lifting (Hensel, 1918) helps us in finding a non-trivial factorization of f mod p^k for any k. But, when f mod p is a power of an irreducible then it is not known how to lift to some factorization of f mod p^k. To illustrate the difficulty let us see some examples (also see von zur Gathen and Hartlieb (1996)).

Example 1 *(coprime factor case).* Let $f = x^2+10x+21$. Then $f \equiv x(x+1)$ mod 3 and Hensel lemma lifts this factorization uniquely mod 3^2 as $f \equiv (x+1\cdot 3)(x+1+2\cdot 3) \equiv (x+3)(x+7)$ mod 9. This lifting extends to any power of 3.

Example 2 *(power of an irreducible case).* Let $f = x^3+12x^2+3x+36$ and we want to factor it mod 3^3. Clearly, $f \equiv x^3$ mod 3. By brute force one checks that, the factorization $f \equiv x\cdot x^2$ mod 3 lifts to factorizations mod 3^2 as: $x(x^2+3x+3)$, $(x+6)(x^2+6x+3)$, $(x+3)(x^2+3)$. Only the last one lifts to mod 3^3 as: $(x+3)(x^2+9x+3)$, $(x+12)(x^2+3)$, $(x+21)(x^2+18x+3)$.

So the big issue is: efficiently determine which factorization, out of the exponentially many factorizations mod p^j, will lift to mod p^{j+1}?

1.1. Previously known results

Using Hensel lemma it is easy to find a non-trivial factor of f mod p^k when f mod p has two coprime factors. So the hard case is when f mod p is power of an irreducible polynomial. The first resolution in this case was achieved by von zur Gathen and Hartlieb (1998) assuming that k is "large". They assumed k to be larger than the maximum power of p dividing the discriminant of the integral f. Under this assumption (i.e. k is large), they showed that factorization modulo p^k is well behaved and it corresponds to the unique p-adic factorization of f (refer p-adic factoring Chistov (1987, 1994); Cantor and Gordon (2000); Guàrdia et al. (2012)). To show this, they used an extended version of

Hensel lifting (also discussed in Borevich and Shafarevich (1986)). Using this observation they could also describe *all* the factorizations modulo p^k, in a compact data structure. The complexity of von zur Gathen and Hartlieb (1998) was improved by Cheng and Labahn (2001).

The related questions of root finding and root counting of $f \bmod p^k$ are also of classical interest, see Niven et al. (2013); Apostol (2013). Root counting has interesting applications in arithmetic algebraic-geometry, for instance to compute Igusa's local zeta function of a univariate integral polynomial (Zuniga-Galindo, 2003; Denef and Hoornaert, 2001; Dwivedi and Saxena, 2020). To the best of our knowledge, the first randomized polynomial time root-finding algorithm can be deduced from Panayi's PhD work Panayi (1995). A root-counting algorithm based on Panayi's work is described in (Pauli and Roblot, 2001, Section 8). A recent result of (Berthomieu et al., 2013, Cor.4) explicitly resolves these problems (all root-finding and counting) in randomized polynomial time. Again, it describes *all* the roots modulo p^k, in a compact data structure. Neiger et al. (2017) improved the time complexity of Berthomieu et al. (2013). Very recently, Kopp et al. (2019) also found a randomized poly-time algorithm which counts all the roots of $f \bmod p^k$.

Derandomizing root counting problem remained open until very recently. A partial derandomization of root counting algorithm has been obtained by Cheng et al. (2018) last year; which runs in deterministic poly-time when $k = O(\log\log p)$. Finally, Dwivedi et al. (2019a) gave a deterministic poly$(\deg(f), k\log p)$-time algorithm for the problem, which also generalizes to count all the basic irreducible factors of $f \bmod p^k$; taking a step closer towards irreducibility testing of $f \bmod p^k$.

Going back to factoring $f \bmod p^k$, von zur Gathen and Hartlieb (1996) discusses the hurdles when k is small. The factors could be completely unrelated to the corresponding p-adic factorization, since an irreducible p-adic polynomial could be reducible mod p^k when k is small. We give an example from von zur Gathen and Hartlieb (1996).

Example 3. Polynomial $f = x^2 + 3^k$ is irreducible over $\mathbb{Z}/\langle 3^{k+1}\rangle$ and so over 3-adic field. But, it is reducible mod 3^k as $f \equiv x^2 \bmod 3^k$.

von zur Gathen and Hartlieb also pointed out that the distinct factorizations are completely different and not nicely related, unlike the case when k is large. An example taken from von zur Gathen and Hartlieb (1996) is,

Example 4. $f = (x^2 + 243)(x^2 + 6)$ is an irreducible factorization over $\mathbb{Z}/\langle 3^6\rangle$. There is another completely unrelated factorization $f = (x + 351)(x + 135)(x^2 + 243x + 249) \bmod 3^6$.

Many researchers tried to solve special cases, especially when k is constant. The only successful factoring algorithm is by Sălăgean (2005) over $\mathbb{Z}/\langle p^2\rangle$; it is actually related to Eisenstein's criterion for irreducible polynomials. The next case, to factor modulo p^3, is unsolved and was recently highlighted in Sircana (2017).

1.2. Our results

We saw that even after the attempts of last two decades we do not have an efficient algorithm for factoring mod p^3. Naturally, we would like to first understand the difficulty of the problem when k is constant. In this direction we make significant progress by devising a unified method which solves the problem when $k = 2, 3$ or 4 (and sketch the obstructions we face when $k \geq 5$). Our first result is,

Theorem 1. *Let p be prime, $k \leq 4$ and $f \in \mathbb{Z}[x]$ be a univariate integral polynomial. Then, $f \bmod p^k$ can be factored (find a non-trivial factor or report irreducible) in randomized poly($\deg f, \log p$) time.*

Remarks. (1) The procedure to factor $f \bmod p^4$ also factors mod p^3 and mod p^2 (and tests for irreducibility) in randomized poly($\deg f, \log p$) time. This solves the open question of efficiently factoring $f \bmod p^3$ (Sircana, 2017) and generalizes Sălăgean (2005).

(2) Our method can as well be used to factor a 'univariate' polynomial $f \in \left(\mathbb{F}_p[z]/\langle \psi^k\rangle\right)[x]$, for $k \leq 4$ and irreducible $\psi(z) \bmod p$, in randomized poly($\deg f, \deg\psi, \log p$) time.

Next, we do more than just factoring f modulo p^k for $k \le 4$: Given that f is power of an irreducible mod p (hard case for Hensel lemma), we show that our method works in this case to give all the lifts g mod p^k (possibly exponentially many) of any given factor $\tilde{g}$ of f mod p, for $k \le 4$.

Theorem 2. *Let p be prime, $k \le 4$ and $f \in \mathbb{Z}[x]$ be a univariate integral polynomial such that $f \bmod p$ is a power of an irreducible polynomial. Let $\tilde{g}$ be a given factor of $f \bmod p$. Then, in randomized poly($\deg f, \log p$) time, we can compactly describe (and count) all possible factors of $f \bmod p^k$ which are lifts of $\tilde{g}$ (or report that there are none).*

Remark. Theorem 2 can be seen as refinement of Hensel lifting method (Lemma 4) to $\mathbb{Z}/\langle p^k\rangle$, $k \le 4$. To lift a factor f_1 of f mod p, Hensel lemma relies on a cofactor f_2 which is coprime to f_1. Our method needs no such assumption and it directly lifts a factor $\tilde{g}$ of f mod p to (possibly exponentially many) factors g mod p^k.

1.3. Proof technique– root finding over local rings

Our proof involves two main techniques which may be of general interest.

Technique 1: Known factoring methods mod p work by first reducing the problem to that of root finding mod p. In this work, we efficiently reduce the problem of factoring f modulo the principal ideal $\langle p^k\rangle$ to that of finding roots of some polynomial $E(y) \in (\mathbb{Z}[x])[y]$ modulo a *bi-generated* ideal $\langle p^k, \varphi^\ell\rangle$, where φ is an irreducible factor of f mod p. This technique works for all $k \ge 1$.

Technique 2: Next, we find a root of the equation $E \equiv 0 \bmod \langle p^k, \varphi^\ell\rangle$, assuming $k \le 4$. With the help of the special structure of E we will efficiently find all the roots y (possibly exponentially many) in the local ring $\mathbb{Z}[x]/\langle p^k, \varphi^\ell\rangle$.

It remains open whether this technique extends to $k = 5$ and beyond (even to find a single root of the equation). The possibility of future extensions of our technique is discussed in Section 5.

1.4. Proof overview

Proof idea of Theorem 1. Firstly, assume that the given degree d integral polynomial f satisfies $f \equiv \varphi^e \bmod p$ for some $\varphi \in \mathbb{Z}[x]$ which is irreducible mod p. Otherwise, using Hensel lemma (Lemma 4) we can efficiently factor f mod p^k.

Any factor of such an f mod p^k must be of the form $(\varphi^a - py) \bmod p^k$, for some $1 \le a < e$ and $y \in (\mathbb{Z}/\langle p^k\rangle)[x]$. In Theorem 11, we first reduce the problem of finding such a factor $(\varphi^a - py)$ of f mod p^k to finding roots of some $E(y) \in (\mathbb{Z}[x])[y]$ in the local ring $\mathbb{Z}[x]/\langle p^k, \varphi^{ak}\rangle$. This is inspired by the p-adic power series expansion of the quotient $f/(\varphi^a - py)$. On going mod p^k we get a polynomial in y of degree $k-1$; which we want to be divisible by φ^{ak}.

The root y of $E \bmod \langle p^k, \varphi^{ak}\rangle$ can be further decomposed into coordinates $y_0, y_1, \ldots, y_{k-1} \in \mathbb{F}_p[x]/\langle\varphi^{ak}\rangle$ such that $y =: y_0 + py_1 + \cdots + p^{k-1}y_{k-1} \bmod \langle p^k, \varphi^{ak}\rangle$. When we take $k = 4$, it turns out that the root y only depends on the coordinates y_0 and y_1 (i.e. y_2, y_3 can be picked arbitrarily).

Next, we reduce the problem of root finding of $E(y_0 + py_1)$ in the ring $\mathbb{Z}[x]/\langle p^4, \varphi^{4a}\rangle$ to root finding in characteristic p; of some $E'(y_0, y_1)$ in the ring $\mathbb{F}_p[x]/\langle\varphi^{4a}\rangle$ (Lemma 14). We make use of a subroutine Root-Find given by Panayi (1995); Berthomieu et al. (2013) which can efficiently find all the roots of a univariate $g(y)$ in the ring $\mathbb{Z}/\langle p^j\rangle$. In fact, we need a slightly generalized version of it, to find all the roots of a given g in the ring $\mathbb{F}_p[x]/\langle\varphi(x)^j\rangle$ (Section 2.4).

Note that y_0, y_1 are in the ring $\mathbb{F}_p[x]/\langle\varphi^{4a}\rangle$ and so they can be decomposed as $y_0 =: y_{0,0} + \varphi y_{0,1} + \cdots + \varphi^{4a-1}y_{0,4a-1}$ and $y_1 =: y_{1,0} + \varphi y_{1,1} + \cdots + \varphi^{4a-1}y_{1,4a-1}$, with all $y_{i,j}$'s in the field $\mathbb{F}_p[x]/\langle\varphi\rangle$.

To get $E'(y_0, y_1) \bmod \langle p, \varphi^{4a}\rangle$ the idea is: first divide by p^2, and then to go modulo the ideal $\langle p, \varphi^{4a}\rangle$. Apply Algorithm Root-Find to solve $E(y_0 + py_1)/p^2 \equiv 0 \bmod \langle p, \varphi^{4a}\rangle$. This allows us to fix some part of y_0, say $a_0 \in \mathbb{F}_p/\langle\varphi^{4a}\rangle$, and we can replace it by $a_0 + \varphi^{i_0}y_0$, $i_0 \ge 1$. Thus, $p^3 | E(a_0 + \varphi^{i_0}y_0 + py_1) \bmod \langle p^4, \varphi^{4a}\rangle$ and we divide out by this p^3 (and change the modulus to $\langle p, \varphi^{4a}\rangle$). In

Lemma 14 we show that when we go modulo the ideal $\langle p, \varphi^{4a}\rangle$ to find a_0, we only need to solve a univariate polynomial equation in y_0 using Root-Find. So we only need to fix some part of y_0, that we called a_0, and y_1 is irrelevant. Finally, we get $E'(y_0, y_1)$ such that $E'(y_0, y_1) := E(a_0 + \varphi^{i_0} y_0 + py_1)/p^3 \bmod \langle p, \varphi^{4a}\rangle$. Importantly, the process yields at most *two* possibilities of E' (resp. a_0) to deal with.

Lemma 14 also shows that the bivariate $E'(y_0, y_1)$ is a special one of the form $E'(y_0, y_1) \equiv E_1(y_0) + E_2(y_0)y_1 \bmod \langle p, \varphi^{4a}\rangle$, where $E_1 \in (\mathbb{F}_p[x]/\langle\varphi^{4a}\rangle)[y_0]$ is a cubic univariate polynomial and $E_2 \in (\mathbb{F}_p[x]/\langle\varphi^{4a}\rangle)[y_0]$ is a linear univariate polynomial. We exploit this special structure to represent y_1 as a rational function of y_0, i.e., $y_1 \equiv -E_1(y_0)/E_2(y_0) \bmod \langle p, \varphi^{4a}\rangle$. The important issue is that we can calculate y_1 only when, on some specialization $y_0 = a_0$, the division by $E_2(a_0)$ is well defined. So we guess each value of $0 \le r \le 4a$ and ensure that the valuation (with respect to the powers of φ) of $E_1(y_0)$ is at least r but that of $E_2(y_0)$ is *exactly* r. Once we find such a y_0, we can efficiently compute y_1 as $y_1 \equiv -(E_1(y_0)/\varphi^r)/(E_2(y_0)/\varphi^r) \bmod \langle p, \varphi^{4a-r}\rangle$.

To find y_0, we find common solution of two equations: $E_1(y_0) \equiv E_2(y_0) \equiv 0 \bmod \langle p, \varphi^r\rangle$, for each guessed value r, using Algorithm Root-Find. Since the polynomial $E_2(y_0)$ is linear, it is easy for us to filter all y_0's for which valuation of $E_2(y_0)$ is *exactly* r (Lemma 16). Thus, we could efficiently find all (y_0, y_1) pairs that satisfy the equation $E'(y_0, y_1) \equiv 0 \bmod \langle p, \varphi^{4a}\rangle$.

Proof idea of Theorem 2. If $f \equiv \varphi^e \bmod p$ then any lift g of a factor $\tilde{g}(x) \equiv \varphi^a \bmod p$ of $f \bmod p$ will be of the form $g \equiv (\varphi^a - py) \bmod p^k$. So basically we want to find all the y's mod p^{k-1} that appear in the proof idea of Theorem 1 above. This can be done easily, because Algorithm Root-Find (Section 2.4) Panayi (1995); Berthomieu et al. (2013) describes all possible y_0's in a compact data structure. Moreover, using this, a count of all y's can be provided as well.

2. Preliminaries

2.1. Factoring and lifting

The following theorem by Cantor-Zassenhaus (Cantor and Zassenhaus, 1981) efficiently finds all the roots of a given univariate polynomial over a finite field.

Theorem 3 *(Cantor-Zassenhaus). Given a univariate degree d polynomial f over a given finite field $\mathbb{F}_q$, we can find all the irreducible factors of f in $\mathbb{F}_q[x]$ in randomized poly$(d, \log q)$ time.*

Currently, it is a big open question to derandomize the preceding theorem. The known deterministic algorithms are 'inefficient' for example, the well known Berlekamp's algorithm (Berlekamp (1967)) takes time $\tilde{O}(p \cdot (dn)^\omega)$ where $q = p^n$ for p prime and ω is matrix-multiplication exponent.

Below we state a lemma, originally due to Hensel (Hensel, 1918), for $\mathcal{I}$-adic lifting of *coprime* factorization for a given univariate polynomial. Over the years, it has acquired many forms in different texts; the version being presented here is due to Zassenhaus (Zassenhaus, 1969).

Lemma 4 *(Hensel's lemma and lift Hensel (1918)). Let R be a commutative ring with unity, and let $\mathcal{I} \subseteq R$ be an ideal. Given a polynomial $f \in R[x]$, let $g, h, u, v \in R[x]$ be polynomials, such that, $f = gh \bmod \mathcal{I}$ and $gu + hv = 1 \bmod \mathcal{I}$.*

Then, for any $\ell \in \mathbb{N}$, we can efficiently compute $g^*, h^*, u^*, v^* \in R[x]$ such that

$$f = g^*h^* \bmod \mathcal{I}^\ell \qquad \textit{(called } \text{lift of the factorization}\textit{)}$$

where $g^* = g \bmod \mathcal{I}$, $h^* = h \bmod \mathcal{I}$ and $g^*u^* + h^*v^* = 1 \bmod \mathcal{I}^\ell$.

Moreover, g^* and h^* are unique upto multiplication by a unit.

2.2. A bit of commutative algebra

In this subsection we present some basic results in commutative algebra which will be helpful in Section 4.

Zero-Divisors. Let $R[x]$ be the ring of polynomials over $R = \mathbb{Z}/\langle p^k\rangle$. The following lemma about zero divisors in $R[x]$ will be helpful.

Lemma 5. *A polynomial $f \in R[x]$ is a zero divisor iff $f \equiv 0 \bmod p$. Consequently, for any polynomials $f, g_1, g_2 \in R[x]$ and $f \not\equiv 0 \bmod p$, $fg_1 = fg_2$ implies $g_1 = g_2$.*

Proof. If $f \equiv 0 \bmod p$ then $f \cdot p^{k-1}$ is zero, and f is a zero divisor.

For the other direction, let $f \not\equiv 0 \bmod p$ and assume $fg = 0$ for some non-zero $g \in R[x]$. Let

- i be the biggest integer such that the coefficient of x^i in f is non-zero modulo p,
- and j be the biggest integer such that the coefficient of x^j in g has minimum valuation with respect to p.

Then, the coefficient of x^{i+j} in $f \cdot g$ has same valuation as the coefficient of x^j in g, implying that the coefficient is nonzero. This contradicts the assumption $f \cdot g = 0$.

The consequence follows because $f \not\equiv 0 \bmod p$ implies that f cannot be a zero divisor. □

Quotient ideals. We define the quotient ideal (analogous to division of integers) and look at some of its properties.

Definition 6 *(Quotient ideal).* Given two ideals I and J of a commutative ring R, we define the quotient of I by J as,

$$I : J := \{a \in R \mid aJ \subseteq I\}.$$

It can be easily verified that $I : J$ is an ideal. Moreover, we can make the following observations about quotient ideals.

Claim 7 *(Cancellation). Suppose I is an ideal of ring R and a, b, c are three elements in R. By definition of quotient ideals, $ca \equiv cb \bmod I$ iff $a \equiv b \bmod I : \langle c\rangle$.*

Claim 8. *Let p be a prime and $\varphi \in (\mathbb{Z}/\langle p^k\rangle)[x]$ be such that $\varphi \not\equiv 0 \bmod p$. Given an ideal $I := \langle p^\ell, \varphi^m\rangle$ of $\mathbb{Z}[x]$,*

1. *$I : \langle p^i\rangle = \langle p^{\ell-i}, \varphi^m\rangle$, for $i \leq \ell$, and*
2. *$I : \langle \varphi^j\rangle = \langle p^\ell, \varphi^{m-j}\rangle$, for $j \leq m$.*

Proof. We will only prove part (1), as the proof of part (2) is similar. If $c \in \langle p^{\ell-i}, \varphi^m\rangle$ then there exists $c_1, c_2 \in \mathbb{Z}[x]$, such that, $c = c_1 p^{\ell-i} + c_2\varphi^m$. Multiplying by p^i,

$$p^i c = c_1 p^\ell + c_2 p^i \varphi^m \in I \Rightarrow c \in I : \langle p^i\rangle.$$

To prove the reverse direction, if $c \in I : \langle p^i\rangle$ then there exists $c_1, c_2 \in \mathbb{Z}[x]$, such that, $p^i c = c_1 p^\ell + c_2\varphi^m$. Since $i \leq \ell$ and $p \not| \varphi$, we know $p^i | c_2$. So, $c = c_1 p^{\ell-i} + (c_2/p^i)\varphi^m \Rightarrow c \in \langle p^{\ell-i}, \varphi^m\rangle$. □

Lemma 9 *(Compute quotient). Given a polynomial $\varphi \in \mathbb{Z}[x]$ not divisible by p, define I to be the ideal $\langle p^\ell, \varphi^m\rangle$ of $\mathbb{Z}[x]$. If $g(y) \in (\mathbb{Z}[x])[y]$ is a polynomial such that $g \equiv 0 \bmod \langle p, \varphi^m\rangle$, then $p|g \bmod I$ and $g/p \bmod I : \langle p\rangle$ is efficiently computable.*

Proof. The equation $g \equiv 0 \bmod \langle p, \varphi^m\rangle$ implies $g = pc_1 + \varphi^m c_2$ for some polynomials $c_1, c_2 \in \mathbb{Z}[x][y]$. Going modulo I, $g \equiv pc_1 \bmod I$. Hence, $p|g \bmod I$ and $g/p \equiv c_1 \bmod I : \langle p\rangle$ (Claim 7).

If we write g in the reduced form modulo I, then the polynomial g/p can be obtained by dividing each coefficient of $g \bmod I$ by p. □

2.3. Representatives and representative roots

Let R be a commutative ring with addition $+$ and multiplication $\cdot$ and let S be a non-empty subset of R. The product of the set S with a scalar $a \in R$ is defined as $aS := \{as \mid s \in S\}$. Similarly, the sum of a scalar $u \in R$ with the set S is defined as $u + S := \{u + s \mid s \in S\}$. Note that the product and the sum operations used inside the set are borrowed from the underlying ring R. Also note that if S is the empty set then so are aS and $u + S$ for any $a, u \in R$.

Representatives. The symbol '$*$' in a ring R, wherever it appears, denotes any possible choice of an arbitrary element of R. For example, suppose $R = \mathbb{Z}/\langle p^k \rangle$ for a prime p and a positive integer k. In this ring, we will use the notation $y = y_0 + py_1 + \cdots + p^i y_i + p^{i+1}*$, where $i + 1 < k$ and each $y_j \in R/\langle p \rangle$, to denote a set $S_y \subseteq R$ such that

$$S_y = \{y_0 + \cdots + p^i y_i + p^{i+1} y_{i+1} + \cdots + p^{k-1} y_{k-1} \mid \forall y_{i+1}, \ldots, y_{k-1} \in R/\langle p \rangle\}.$$

Notice that the number of distinct elements in R represented by y is $|S_y| = p^{k-i-1}$.

We will sometimes write the set $y = y_0 + py_1 + \cdots + p^i y_i + p^{i+1}*$ succinctly as $y = v + p^{i+1}*$, where $v \in R$ stands for $v = y_0 + py_1 + \cdots + p^i y_i$.

In the following sections, we will add and multiply the set $\{*\}$ with scalars from the ring R. Let us define these operations as follows ($*$ is treated as an unknown)

- $u + \{*\} := \{u + *\}$ and $u\{*\} := \{u*\}$, where $u \in R$.
- $c + \{a + b*\} = \{(a + c) + b*\}$ and $c\{a + b*\} = \{ac + bc*\}$, where $a, b, c \in R$.

Another important example of the $*$ notation: Let $R_0 = \mathbb{F}_p[x]/\langle \varphi(x)^k \rangle$ for a prime p and an irreducible φ mod p. In this ring, we use the notation $y = y_0 + \varphi y_1 + \cdots + \varphi^i y_i + \varphi^{i+1}*$, where $i + 1 < k$ and each $y_j \in R_0/\langle \varphi \rangle$, to denote a set $S_y \subseteq R_0$ such that

$$S_y = \{y_0 + \cdots + \varphi^i y_i + \varphi^{i+1} y_{i+1} + \cdots + \varphi^{k-1} y_{k-1} \mid \forall y_{i+1}, \ldots, y_{k-1} \in R_0/\langle \varphi \rangle\}.$$

Representative roots. Let $R_0 = \mathbb{F}_p[x]/\langle \varphi(x)^k \rangle$ for a prime p and an irreducible φ mod p. Any element in R_0 can be written uniquely as $y = y_0 + \varphi y_1 + \cdots + \varphi^{k-1} y_{k-1}$, where each y_j is in the field $R_0/\langle \varphi \rangle$.

Let $g(y)$ be a polynomial in $R_0[y]$, then a set $y = y_0 + \varphi y_1 + \cdots + \varphi^i y_i + \varphi^{i+1}*$ will be called a *representative root* of g iff

- All elements in $y = y_0 + \varphi y_1 + \cdots + \varphi^i y_i + \varphi^{i+1}*$ are roots of g and,
- Not all elements in $y' = y_0 + \varphi y_1 + \cdots + \varphi^{i-1} y_{i-1} + \varphi^i*$ are roots of g.

We will sometimes represent the set of roots, $y = y_0 + \varphi y_1 + \cdots + \varphi^i y_i + \varphi^{i+1}*$, succinctly as $y = v + \varphi^{i+1}*$, where $v \in R_0$ stands for $y = y_0 + \varphi y_1 + \cdots + \varphi^i y_i$. Such a pair, $(v, i + 1)$, will be called a *representative pair*.

The significance of defining representative roots will be clear in Section 2.4.

2.4. Root finding modulo $\varphi(x)^i$

Let us denote the ring $\mathbb{F}_p[x]/\langle \varphi^i \rangle$ by R_0 (for an irreducible $\varphi(x)$ mod p). In this section, we give an algorithm to find all the roots $y \in R_0$ of a polynomial $g \in R_0[y]$. To the best of our knowledge, the algorithm to find roots modulo p^i first appeared in Panayi's PhD thesis Panayi (1995). Here, we adapt the algorithm by (Berthomieu et al., 2013, Cor.4) to find roots in R_0 in the form of representative roots. Recall the notation of $*$ and representative roots from Section 2.3.

Note that $R_0/\langle \varphi^j \rangle = \mathbb{F}_p[x]/\langle \varphi^j \rangle$, for $j \leq i$, and $R_0/\langle \varphi \rangle =: \mathbb{F}_q$ is the finite field of cardinality $q := p^{\deg(\varphi \bmod p)}$. A root y of g in R_0 has the following unique structure

$$y = y_0 + \varphi y_1 + \varphi^2 y_2 + \cdots + \varphi^{i-1} y_{i-1},$$

where each $y_j \in \mathbb{F}_q$ for all $j \in \{0, \dots, i-1\}$.

The **output** of this algorithm is simply a set of at most $\deg g$ many representative roots of g. This bound of $\deg g$ is a curious by-product of the algorithm (Berthomieu et al., 2013, Cor.4).

Algorithm 1 Root-finding in ring R_0.

```
1: procedure ROOT-FIND($g(y)$, $\varphi^i$)
2:     If $g(y) \equiv 0$ in $R_0/\langle\varphi^i\rangle$ return $*$ (every element is a root).
3:     Let $g(y) \equiv \varphi^\alpha \tilde{g}(y)$ in $R_0/\langle\varphi^i\rangle$, for the unique integer $0 \le \alpha < i$ and the polynomial $\tilde{g}(y) \in R_0/\langle\varphi^{i-\alpha}\rangle[y]$, s.t., $\tilde{g}(y) \not\equiv 0$
       in $R_0/\langle\varphi\rangle$ and $\deg(\tilde{g}) \le \deg(g)$.
4:     Using Cantor-Zassenhaus algorithm (Theorem 3) find all the roots of $\tilde{g}(y)$ in $R_0/\langle\varphi\rangle$.
5:     If $\tilde{g}(y)$ has no root in $R_0/\langle\varphi\rangle$ then return $\{\}$. (Dead-end)
6:     Initialize $S = \{\}$.
7:     for each root $a$ of $\tilde{g}(y)$ in $R_0/\langle\varphi\rangle$ do
8:         Define $g_a(y) := \tilde{g}(a + \varphi y)$.
9:         $S' \leftarrow$ROOT-FIND($g_a(y)$, $\varphi^{i-\alpha}$).
10:        $S \leftarrow S \cup (a + \varphi S')$.
11:    end for
12:    return $S$.
13: end procedure
```

Note that in Step 9 we ensure: $\varphi | g_a(y)$. So, in every other recursive call to ROOT-FIND the second argument reduces by at least one. The key reason why $|S| \le \deg g$ holds: The number of representative roots of g_a are upper bounded by the multiplicity of the root a of $\tilde{g}$.

The implication of Algorithm 1 is summed up in the following theorem due to Panayi (1995); Berthomieu et al. (2013).

Theorem 10. *(Panayi, 1995; Berthomieu et al., 2013, Cor.4) Given a bivariate $g \in R_0[y]$ where $R_0 = \mathbb{Z}[x]/\langle p, \varphi^i\rangle$, let $Z \subseteq R_0$ be the root set of $g(y)$. Then Z can be expressed as the disjoint union of at most $\deg_y(g)$ many representative pairs (a_0, i_0) ($a_0 \in R_0$ and $i_0 \in \mathbb{N}$).*

These representative pairs can be found in randomized poly($\deg_y(g), \log p, ak \deg\varphi$) time.

Notice that this compact description of the root set Z allows us to calculate the size of Z too. Let us see how Algorithm 1 can be used to factor the polynomial given in Example 2. We adapt the Algorithm 1 here in the context $R_0 = \mathbb{Z}/\langle p^k\rangle$.

Example 5. We have $g(x) = x^3 + 12x^2 + 3x + 36$ and $p^k = 3^3$. So $g \equiv x^3 + 12x^2 + 3x + 9 \bmod 27$.

Using Theorem 3, the only root of $\tilde{g}(x) := g \bmod 3$ is 0. So we shift g as $g(0 + 3x) \equiv 9(x + 4) \bmod 27$.

Dividing by 9 both sides we have, $g_a(x) \equiv x + 1 \bmod 3$ which has only root 2 modulo 3.

So we get exactly one representative root of $g \bmod 27$: $\quad x = 0 + 3(2) + 3^2 *$.

Putting $0, 1$ and 2 in place of $*$ we get the roots $-21, -15$ and -3 modulo 27. These correspond to degree one factors $(x + 21), (x + 12)$ and $(x + 3)$ of $g \bmod 27$ as we saw in Example 2.

2.5. Input preprocessing and proof organization

We give some assumptions here, on the given input polynomial $f \in \mathbb{Z}[x]$, which will be followed in further sections unless explicitly stated otherwise.

Preprocessing: Our task is to non-trivially factor a univariate integral polynomial $f \in \mathbb{Z}[x]$ of degree d modulo a prime power p^k. Without loss of generality, we can assume that $f \not\equiv 0 \bmod p$. Otherwise, we can efficiently divide f by the highest power of p possible, say p^ℓ, such that $f(x) \equiv p^\ell \tilde{f}(x) \bmod p^k$ and $\tilde{f}(x) \not\equiv 0 \bmod p$. In this case, it is equivalent to factor $\tilde{f}$ instead of f.

To simplify the input further, write $f \bmod p$ (uniquely) as a product of powers of coprime irreducible polynomials (Theorem 3). If there are two coprime factors of f, using Hensel lemma

(Lemma 4), we get a non-trivial factorization of $f \bmod p^k$. So we can assume that f is a power of a monic irreducible polynomial $\varphi \in \mathbb{Z}[x]$ modulo p. In other words, we can efficiently write

$$f \equiv \varphi^e + p\ell \bmod p^k$$

for a polynomial ℓ in $(\mathbb{Z}/\langle p^k\rangle)[x]$. We have $e \cdot \deg\varphi \leq \deg f$, for the integral polynomials f and φ.

Organization of paper: Factoring a univariate modulo p goes through root finding in an extension field of $\mathbb{F}_p$. Our factoring method passes through a similar stage. In Section 3, we reduce factoring $f \bmod p^k$ to root finding of $E \in (\mathbb{Z}[x])[y]$ modulo the bi-generated ideal $\langle p^k, \varphi^{ak}\rangle$ for some $a < e$.

Section 4 proves our main Theorems- 1 and 2. We show in Section 4.1 how to find (and count) roots of E in simpler case of $k = 3$. In rest of Section 4 we generalize the idea used for $k = 3$ to find (and count) roots of E for $k = 4$. In Section 5 we discuss the barriers for $k = 5$ and beyond in extending the idea for $k = 4$. Finally, we conclude in Section 6.

3. Factoring to root-finding

In this section we give a general framework to work on the problem of factoring $f \bmod p^k$– we reduce factoring $f \bmod p^k$ to root finding in a more general ring. The reduction seems quite natural and we hope that factoring $f \bmod p^k$, for arbitrary k can be done efficiently within this framework.

Following the preprocessing in Section 2.5, it is enough to factor $f \in \mathbb{Z}[x]$ such that

$$f \equiv \varphi^e + p\ell \bmod p^k,$$

where $\varphi \in \mathbb{Z}[x]$ is an irreducible polynomial modulo p. Up to multiplication by units, any non-trivial factor h of f has the form $h \equiv \varphi^a - py$, as $h \bmod p$ is a factor of $f \equiv \varphi^e \bmod p$, where $a < e$ and y is a polynomial in $(\mathbb{Z}/\langle p^k\rangle)[x]$.

Let us denote the ring $\mathbb{Z}[x]/\langle p^k, \varphi^{ak}\rangle$ by R. Also, denote the ring $\mathbb{Z}[x]/\langle p, \varphi^{ak}\rangle$ by R_0. We define an auxiliary polynomial $E \in R[y]$ via

$$E := f \cdot (\varphi^{a(k-1)} + \varphi^{a(k-2)}(py) + \cdots + \varphi^a (py)^{k-2} + (py)^{k-1}).$$

Theorem 11 reduces the problem of factoring $f \bmod p^k$ to the problem of finding roots of the univariate polynomial E in ring R. Thus, we convert the problem of finding factors of $f \in \mathbb{Z}[x]$ modulo a *principal ideal* $\langle p^k\rangle$ to root finding of a polynomial $E \in (\mathbb{Z}[x])[y]$ modulo a *bi-generated ideal* $\langle p^k, \varphi^{ak}\rangle$.

Theorem 11 *(Reduction theorem). Given a prime power p^k; let $f, h \in \mathbb{Z}[x]$ satisfy $f \equiv \varphi^e + p\ell \bmod p^k$ and $h \equiv \varphi^a - py \bmod p^k$, with $\ell, y \in (\mathbb{Z}/\langle p^k\rangle)[x]$ and $a \leq e$. Then, h divides f modulo p^k if and only if*

$$E \;=\; f \cdot (\varphi^{a(k-1)} + \varphi^{a(k-2)}(py) + \cdots + \varphi^a (py)^{k-2} + (py)^{k-1}) \;\equiv\; 0 \bmod \langle p^k, \varphi^{ak}\rangle.$$

Proof. Let Q denote the *ring of fractions* of the ring $(\mathbb{Z}/\langle p^k\rangle)[x]$. Since φ is not a zero divisor, $(E(y)/\varphi^{ak}) \in Q$.

We first prove the reverse direction. If $E \equiv 0 \bmod \langle p^k, \varphi^{ak}\rangle$, then (E/φ^{ak}) is a polynomial over $(\mathbb{Z}/\langle p^k\rangle)[x]$. Multiplying h with $(E/\varphi^{ak}) \bmod p^k$, we write,

$$(\varphi^a - py)((f/\varphi^{ak})\Sigma_{i=0}^{k-1}\varphi^{a(k-1-i)}(py)^i) \;\equiv\; (f/\varphi^{ak})(\varphi^{ak} - (py)^k) \equiv f \cdot \varphi^{ak}/\varphi^{ak} \equiv f \bmod p^k.$$

The first equality comes via geometric series. Hence, h divides f modulo p^k.

For the forward direction, assume that there exists some $g \in (\mathbb{Z}/\langle p^k\rangle)[x]$, such that, $f(x) \equiv h(x)g(x) \bmod p^k$. We get two factorizations of f in Q,

$$f = h \cdot g \quad \text{and} \quad f = h \cdot (E/\varphi^{ak}).$$

Subtracting the first equation from the second one,

$$h \cdot \left(g - (E/\varphi^{ak})\right) = 0.$$

Notice that h is not a zero divisor in $(\mathbb{Z}/\langle p^k\rangle)[x]$ (by Lemma 5) and is thus invertible in Q. So, $E/\varphi^{ak} = g$ in Q. Since g is in $(\mathbb{Z}/\langle p^k\rangle)[x]$, we deduce the equivalent divisibility statement: $E(y) \equiv 0 \bmod \langle p^k, \varphi^{ak}\rangle$. □

Following the reduction in this section, we move on to find roots of $E(y)$, when $k \le 4$, in the next section (Sec. 4).

4. Main results: the Proof of Theorems 1 and 2

In this section we will prove Theorems 1 and 2. We want to find (and count) all the factors $h \in (\mathbb{Z}/\langle p^k\rangle)[x]$ of the given degree d polynomial $f \in \mathbb{Z}[x]$ modulo p^k for $k \le 4$, where $f \equiv \varphi^e + p\ell \bmod p^k$ and $h = \varphi^a - py$ (Sec. 2.5).

We also recall the definitions from Section 3. We have $R := \mathbb{Z}[x]/\langle p^k, \varphi^{ak}\rangle$ and $R_0 = \mathbb{Z}[x]/\langle p, \varphi^{ak}\rangle$. For a factor h of f, define $E \in R[y]$ as

$$E := f \cdot (\varphi^{a(k-1)} + \varphi^{a(k-2)}(py) + \cdots + \varphi^a(py)^{k-2} + (py)^{k-1}).$$

The following two observations simplify our task of finding roots y of polynomial $E(y)$.

(1) First, due to symmetry, it is enough to find factors $h \equiv \varphi^a \bmod p$ with $a \le e/2$. The assertion follows because $f \equiv hg \bmod p^k$ implies, at least one of the factor (say h) must be of the form $\varphi^a \bmod p$ for $a \le e/2$. By Lemma 5, for a fixed $h \equiv \varphi^a - py \bmod p^k$, there is a unique $g \equiv \varphi^{e-a} - py' \bmod p^k$ such that $f \equiv hg \bmod p^k$. So, to find g, it is enough to find h.

(2) Second, observe that any root $y \in R$ (of $E \in R[y]$) can be seen as $y = y_0 + py_1 + p^2y_2 + \cdots + p^{k-1}y_{k-1}$, where each $y_i \in R_0$ for all i in $\{0, \ldots, k-1\}$. The following lemma decreases the required precision of a root y.

Lemma 12. *Let $y = y_0 + py_1 + p^2y_2 + \cdots + p^{k-1}y_{k-1}$ be a root of E, where $k \ge 2$ and $a \le e/2$. Then, all elements of the set $y = y_0 + py_1 + p^2y_2 + \cdots + p^{k-3}y_{k-3} + p^{k-2}*$ are also roots of E.*

Proof. Notice that the variable y is multiplied with p in $E(y)$, implying y_{k-1} is irrelevant. A similar argument is applicable for the coefficient y_{k-2} in any term involving $(py)^i$ for $i \ge 2$. The only surviving term containing y_{k-2} is $f\varphi^{a(k-2)}(py)$. The coefficient of y_{k-2} in this term is $\varphi^{a(k-2)}fp^{k-1}$, it also vanishes because

$$\varphi^{a(k-2)}f \equiv \varphi^{a(k-2)}\varphi^e \equiv \varphi^{ak}\varphi^{e-2a} \equiv 0 \bmod \langle p, \varphi^{ak}\rangle. \quad \square$$

Root-finding modulo a principal ideal. In next few sections we will see that finding roots of E in R goes through finding roots of intermediate polynomials in $R_0 = \mathbb{F}_p[x]/\langle\varphi^{ak}\rangle$ (i.e., modulo a principal ideal). Such an algorithm is described in Section 2.4, which is a slightly modified version of the theorem from (Berthomieu et al., 2013, Cor.4). It shows that all the roots of a polynomial $g \in R_0[y]$ can be efficiently described.

4.1. Finding all the factors modulo p^k when $k < 4$

In this section we partially prove Theorems 1 and 2, i.e., we efficiently find all the factors of $f \bmod p^2$ and $f \bmod p^3$. Although the case of $k = 2$ is already solved Sălăgean (2005), the case of $k = 3$ was left open in Sircana (2017). The ideas in this section (for $k \le 3$) will be generalized to solve the case $k = 4$.

Factoring f mod p^2. The reduction theorem (Theorem 11) and Lemma 12 make factoring mod p^2 easy: They imply that any root of E is independent of coordinates y_0 and y_1. So, either $h = \varphi^a - py$ can not be a factor of $f \bmod p^2$ or it is a factor for every value of $y \in R_0$. Substituting $y = 0$, we get that $h \equiv \varphi^a - py \bmod p^2$ is a factor of f if and only if $\varphi^a | f$ modulo p^2. In fact, we get a simple irreducibility criteria– *f mod p^2 factors if and only if $\varphi | f$ mod p^2* (first discovered by Sălăgean (2005)).

Factoring f mod p^3. Theorem 13 below solves the factoring problem modulo p^3.

Theorem 13. *Given $f \in \mathbb{Z}[x]$, a univariate polynomial of degree d and a prime $p \in \mathbb{N}$, we give (and count) all the distinct factors of $f \bmod p^3$ of degree at most d in randomized poly($d, \log p$) time.*

Note: We will assume that the leading coefficient of f is 1. Also, we will not distinguish two factors if they are same up to multiplication by a unit.

Proof of Theorem 13. By Theorem 3, a general f can be written as:

$$f(x) \equiv \prod_{i=1}^{n} f_i(x) \equiv \prod_{i=1}^{n} (\varphi_i^{e_i} + ph_i) \bmod p^3, \tag{1}$$

where $f_i(x) \equiv (\varphi_i^{e_i} + ph_i) \bmod p^3$ with $\varphi_i \bmod p^3$ being monic and irreducible mod p, $e_i \in \mathbb{N}$, and $h_i(x) \bmod p^3$ of degree $< e_i \deg(\varphi_i)$, for all $i \in [n]$.

Using Lemma 4, it is sufficient to consider the case $f \equiv \varphi^e + ph$.

By Reduction theorem (Theorem 11) finding factors of the form $\varphi^a - py \bmod p^3$ of $f \equiv \varphi^e + ph \bmod p^3$, for $a \le e/2$, is equivalent to finding all roots of the equation

$$E \equiv f \cdot (\varphi^{2a} + \varphi^a(py) + (py)^2) \equiv 0 \bmod \langle p^3, \varphi^{3a} \rangle.$$

Consider $R := \mathbb{Z}[x]/\langle p^3, \varphi^{3a} \rangle$ and $R_0 := \mathbb{Z}[x]/\langle p, \varphi^{3a} \rangle$ (analogous to Section 2).

Using Lemma 12, we know that all solutions of the equation $E \equiv 0 \bmod \langle p^3, \varphi^{3a} \rangle$ will be of the form $y = y_0 + p* \in R$, for a $y_0 \in R_0$. Substituting, we get

$$E \equiv ph\varphi^{2a} + (p^2 h\varphi^a)y_0 + (p^2\varphi^e)y_0^2 \equiv 0 \bmod \langle p^3, \varphi^{3a} \rangle.$$

Looking at this equation mod $\langle p^2, \varphi^{3a} \rangle$, we get that $h \equiv 0 \bmod \langle p, \varphi^a \rangle$ is a necessary condition for a root y_0 to exist. Define $h := \varphi^a g_1 + pg_2$ for unique $g_1, g_2 \in \mathbb{F}_p[x]$, the equation becomes

$$E \equiv p^2 g_2 \varphi^{2a} + (p^2 g_1 \varphi^{2a})y_0 + (p^2\varphi^e)y_0^2 \equiv 0 \bmod \langle p^3, \varphi^{3a} \rangle.$$

This equation is already divisible by p^2 as well as φ^{2a}. Using Claim 8, finding factors of the form $\varphi^a - py \bmod p^3$ is equivalent to finding all roots of the equation

$$g_2 + g_1 y_0 + \varphi^{e-2a} y_0^2 \equiv 0 \bmod \langle p, \varphi^a \rangle.$$

These roots can be obtained using one call to Root-find in randomized poly($d, \log p$) time. Note that any root y_0 given by Root-find is an element of $\mathbb{F}_p[x]/\langle \varphi^a \rangle$, implying its degree in x is $< a\deg(\varphi)$. This yields *monic* factors of $f \bmod p^3$ (with $0 \le a \le e/2$).

For $e \ge a > e/2$, we can replace a by $b := e - a$ in the above steps. Once we get a factor $\varphi^b - py \bmod p^3$, we output the cofactor $f/(\varphi^b - py) = (f/\varphi^{ak})(\varphi^{2a} + \varphi^a(py) + (py)^2)$ (which remains monic).

Since Theorem 10 gives the numbers of roots from Root-find, we also get a count on total number of factors in poly-time.

For a general f (Equation (1)), if N_i is the number of factors of $f_i \bmod p^3$, then $\prod_{i=1}^{n} N_i$ is the count on the number of distinct monic factors of $f \bmod p^3$. □

Let us illustrate the steps in the proof of Theorem 13 by an example.

Example 6. Let $f = x^4 + 18x^3 + 33x^2 + 54x + 9$ be an integral polynomial and pick $p = 3, k = 3$.

We need to find factors of $f \equiv x^4 + 18x^3 + 6x^2 + 9 \bmod 27$; since $f \equiv x^4 \bmod 3$, fix $\varphi := x \in \mathbb{Z}[x]$. Say, we want to find quadratic factors of $f \bmod 27$, so fix $a = 2$.

Recall the reduction theorem (Theorem 11), $(\varphi^a - py)$ is a factor of $f \bmod p^3$ iff

$$E := f \cdot (\varphi^{2a} + \varphi^a(py) + (py)^2) \equiv 0 \bmod \langle p^3, \varphi^{3a} \rangle.$$

$$\Leftrightarrow (x^4+18x^3+6x^2+9)[x^4+x^2(3y_0)+9y_0^2] \equiv 0 \bmod \langle 27, x^6\rangle. \qquad (y = y_0 \text{ [Lemma 12]})$$

$$\Leftrightarrow 9x^4y_0^2 + 18x^4y_0 + 9x^4 \equiv 0 \bmod \langle 27, x^6\rangle.$$

$$\Leftrightarrow y_0^2 + 2y_0 + 1 \equiv 0 \bmod \langle 3, x^2\rangle.$$

$$\Leftrightarrow (y_0+1)^2 \equiv 0 \bmod \langle 3, x^2\rangle.$$

Applying Panayi (1995); Berthomieu et al. (2013) (Theorem 10) on last equation, we get exactly one representative root $y_0 = 2 + x*$.

Choosing $y_1 = 0$ and $y_0 = 2+0$, we have a corresponding factor $(x^2 - 3(2+0)) \equiv (x^2+21) \bmod 27$. The co-factor of this is $(x^2+18x+12)$, giving

$$f \equiv x^4 + 18x^3 + 6x^2 + 9 \equiv (x^2+21)(x^2+18x+12) \bmod 27.$$

Remark. Observe that the core idea for p^3 was to first reduce root finding of E mod $\langle p^3, \varphi^{3a}\rangle$ to root finding modulo a principal ideal $\langle p, \varphi^a\rangle$. It was then solved by just one application of Theorem 10. For p^3, we only needed to deal with a univariate polynomial in y_0.

The approach for $k = 4$ is similar, though it requires several applications of Theorem 10 to go to principal ideal $\langle p, \varphi^{4a}\rangle$ (Sec. 4.2). Even after that, we are required to solve a bivariate equation modulo the principal ideal (as opposed to a univariate in the case $k = 3$).

We will fix $k = 4$ for the rest of Section 4. The barriers for $k > 4$ will be discussed in Section 5.

4.2. Reduction to root-finding modulo a principal ideal of $\mathbb{F}_p[x]$

In this subsection, the task to find roots of E modulo the bi-generated ideal $\langle p^4, \varphi^{4a}\rangle$ of $\mathbb{Z}[x]$ will be reduced to finding roots modulo the principal ideal $\langle \varphi^{4a}\rangle$ (of $\mathbb{F}_p[x]$).

Let us consider the equation $E \equiv 0 \bmod \langle p^4, \varphi^{4a}\rangle$. We have,

$$f(\varphi^{3a} + \varphi^{2a}(py) + \varphi^a(py)^2 + (py)^3) \equiv 0 \bmod \langle p^4, \varphi^{4a}\rangle. \tag{2}$$

Using Lemma 12, we can assume $y = y_0 + py_1$,

$$f(\varphi^{3a} + \varphi^{2a}p(y_0+py_1) + \varphi^a p^2(y_0^2 + 2py_0y_1) + (py_0)^3) \equiv 0 \bmod \langle p^4, \varphi^{4a}\rangle. \tag{3}$$

The idea is to first solve this equation modulo $\langle p^3, \varphi^{4a}\rangle$. Since $f \equiv \varphi^e \bmod p$, $e \geq 2a$, variable y_1 is redundant while solving this equation modulo p^3. The following lemma finds all representative pairs (a_0, i_0) for y_0, such that, $E(a_0 + \varphi^{i_0}y_0 + py_1) \equiv 0 \bmod \langle p^3, \varphi^{4a}\rangle$ for all $y_0, y_1 \in R$. Alternatively, we can state this in the polynomial ring $R[y_0, y_1]$. Dividing by p^3, we will be left with an equation modulo the principal ideal $\langle \varphi^{4a}\rangle$ (of $\mathbb{F}_p[x]$).

Lemma 14 *(Reduction to characteristic p). We efficiently compute a unique set S_0 of all representative pairs (a_0, i_0), where $a_0 \in R_0$ and $i_0 \in \mathbb{N}$, such that,*

$$E((a_0 + \varphi^{i_0}y_0) + py_1) \; = \; p^3E'(y_0, y_1) \;\; \bmod \langle p^4, \varphi^{4a}\rangle$$

for a polynomial $E'(y_0, y_1) \in R_0[y_0, y_1]$ (depending on (a_0, i_0)). Moreover,

1. *$|S_0| \leq 2$ and, if our algorithm fails to find E', then Eqn. (3) has no solution.*
2. *$E'(y_0, y_1) =: E_1(y_0) + E_2(y_0)y_1$, where $E_1 \in R_0[y_0]$ is cubic in y_0 and $E_2 \in R_0[y_0]$ is linear in y_0.*
3. *For every root $y \in R$ of E there exists $(a_0, i_0) \in S_0$ and $(a_1, a_2) \in R \times R$, such that $y = (a_0 + \varphi^{i_0}a_1) + pa_2$ and $E'(a_1, a_2) \equiv 0 \bmod \langle p, \varphi^{4a}\rangle$.*

We think of E' as the quotient $E((a_0 + \varphi^{i_0} y_0) + py_1)/p^3$ in the polynomial ring $R_0[y_0, y_1]$; and would work with it instead of E in the root-finding algorithm.

Proof. Looking at Eqn. (3) modulo p^2,

$$f\varphi^{2a}(\varphi^a + py_0) \equiv 0 \mod \langle p^2, \varphi^{4a}\rangle.$$

Substituting $f = \varphi^e + ph_1$, we get $(\varphi^e + ph_1)(\varphi^{3a} + \varphi^{2a}py_0) \equiv 0 \bmod \langle p^2, \varphi^{4a}\rangle$. Implying, $ph_1\varphi^{3a} \equiv 0 \bmod \langle p^2, \varphi^{4a}\rangle$. Using Claim 8 the above equation implies that,

$$h_1 \equiv 0 \mod \langle p, \varphi^a\rangle\,, \tag{4}$$

is a necessary condition for y_0 to exist.

We again look at Eqn. (3), but modulo p^3 now: $f(\varphi^{3a} + \varphi^{2a}py_0 + \varphi^a p^2 y_0^2) \equiv 0 \bmod \langle p^3, \varphi^{4a}\rangle$.

Notice that y_1 is not present because of its coefficient: $p^2 f\varphi^{2a} \equiv 0 \bmod \langle p^3, \varphi^{4a}\rangle$. Substituting $f = \varphi^e + ph_1$, we get,

$$(\varphi^e + ph_1)(\varphi^{3a} + \varphi^{2a}py_0 + \varphi^a p^2 y_0^2) \equiv 0 \bmod \langle p^3, \varphi^{4a}\rangle.$$

Removing the coefficients of y_0 which vanish modulo $\langle p^3, \varphi^{4a}\rangle$,

$$\varphi^{e+a}p^2y_0^2 + \varphi^{3a}ph_1 + \varphi^{2a}p^2h_1y_0 \equiv 0 \mod \langle p^3, \varphi^{4a}\rangle.$$

From Eqn. (4), h_1 can be written as $ph_{1,1} + \varphi^a h_{1,2}$, so

$$p^2\left(\varphi^{e+a}y_0^2 + \varphi^{3a}h_{1,2}y_0 + \varphi^{3a}h_{1,1}\right) \equiv 0 \mod \langle p^3, \varphi^{4a}\rangle.$$

We can divide by $p^2\varphi^{3a}$ using Claim 8 to get an equation modulo φ^a in the ring $\mathbb{F}_p[x]$. This is a quadratic equation in y_0. Using Theorem 10, we find the solution set S_0 with at most two representative pairs: for $(a_0, i_0) \in S_0$, every $y \in a_0 + \varphi^{i_0} * + p*$ satisfies,

$$E \equiv 0 \mod \langle p^3, \varphi^{4a}\rangle\,.$$

In other words, upon substituting $y = a_0 + \varphi^{i_0} y_0 + py_1$ in $E(y)$, we get

$$E(a_0 + \varphi^{i_0}y_0 + py_1) \equiv p^3E'(y_0, y_1) \mod \langle p^4, \varphi^{4a}\rangle,$$

for a "bivariate" polynomial $E'(y_0, y_1) \in R_0[y_0, y_1]$. This sets up the correspondence between the roots of E and E'.

Substituting $(a_0 + \varphi^{i_0}y_0 + py_1)$ in Eqn. (3), we notice that $E'(y_0, y_1)$ has the form $E_1(y_0) + E_2(y_0)y_1$ for a linear E_2 and a cubic E_1.

Finally, this reduction is constructive, because of Lemma 9 and Theorem 10, giving a randomized poly-time algorithm. □

4.3. *Finding roots of a* special *bi-variate* $E'(y_0, y_1)$ *modulo* $\langle p, \varphi^{4a}\rangle$

The final obstacle is to find roots of $E'(y_0, y_1)$ modulo $\langle\varphi^{4a}\rangle$ in $\mathbb{F}_p[x]$. The polynomial $E'(y_0, y_1) = E_1(y_0) + E_2(y_0)y_1$ is *special* because $E_2 \in R_0[y_0]$ is *linear* in y_0.

For a polynomial $u \in \mathbb{F}_p[x][\mathbf{y}]$ we define *valuation* $\mathrm{val}_\varphi(u)$ to be the largest r such that $\varphi^r|u$. Our strategy is to go over all possible valuations $0 \le r \le 4a$ and find y_0, such that,

- $E_1(y_0)$ has valuation at least r.
- $E_2(y_0)$ has valuation exactly r.

From these y_0's, y_1 can be obtained by 'dividing' $E_1(y_0)$ by $E_2(y_0)$. The lemma below shows that this strategy captures all the solutions.

Lemma 15 *(Bivariate solution). A pair* $(u_0, u_1) \in R_0 \times R_0$ *satisfies an equation of the form* $E_1(y_0) + E_2(y_0)y_1 \equiv 0 \bmod \langle p, \varphi^{4a}\rangle$ *if and only if* $\mathrm{val}_\varphi(E_1(u_0)) \geq \mathrm{val}_\varphi(E_2(u_0))$.

Proof. Let r be $\mathrm{val}_\varphi(E_2(u_0))$, where r is in the set $\{0, 1, \ldots, 4a\}$. If $\mathrm{val}_\varphi(E_1(u_0)) \geq \mathrm{val}_\varphi(E_2(u_0))$ then set $u_1 \equiv -(E_1(u_0)/\varphi^r)/(E_2(u_0)/\varphi^r) \bmod \langle p, \varphi^{4a-r}\rangle$. The pair (u_0, u_1) satisfies the required equation. (Note: If $r = 4a$ then we take $u_1 = *$.)

Conversely, if $r' := \mathrm{val}_\varphi(E_1(u_0)) < \mathrm{val}_\varphi(E_2(u_0)) \leq 4a$ then, for every u_1,
$\mathrm{val}_\varphi(E_1(u_0) + E_2(u_0)u_1) = r' \Rightarrow E_1(u_0) + E_2(u_0)u_1 \not\equiv 0 \bmod \langle p, \varphi^{4a}\rangle$. □

We can efficiently find all representative pairs for y_0, at most three, such that $E_1(y_0)$ has valuation at least r (using Theorem 10). The next lemma shows that we can efficiently filter all y_0's, from these representative pairs, that give valuation *exactly* r for $E_2(y_0)$.

Lemma 16 *(Reduce to a unit* E_2*). Given a linear polynomial* $E_2(y_0) \in R_0[y_0]$ *and an* $r \in [4a-1]$*, let* (b, i) *be a representative pair modulo* $\langle p, \varphi^r\rangle$*, i.e.,* $E_2(b + \varphi^i *) \equiv 0 \bmod \langle p, \varphi^r\rangle$*. Consider the quotient* $E_2'(y_0) := E_2(b + \varphi^i y_0)/\varphi^r$.

If $E_2'(y_0)$ *does not vanish identically modulo* $\langle p, \varphi\rangle$*, then there exists at most one* $\theta \in R_0/\langle\varphi\rangle$ *such that* $E_2'(\theta) \equiv 0 \bmod \langle p, \varphi\rangle$*, and this* θ *can be efficiently computed.*

Proof. Suppose $E_2(b + \varphi^i y_0) \equiv u + vy_0 \equiv 0 \bmod \langle p, \varphi^r\rangle$. Since y_0 is formal, we get $\mathrm{val}_\varphi(u) \geq r$ and $\mathrm{val}_\varphi(v) \geq r$. We consider the three cases (with respect to these valuations),

1. $\mathrm{val}_\varphi(u) \geq r$ and $\mathrm{val}_\varphi(v) = r$: $E_2'(\theta) \not\equiv 0 \bmod \langle p, \varphi\rangle$, for all $\theta \in R_0/\langle\varphi\rangle$ except $\theta = (-u/\varphi^r)/(v/\varphi^r) \bmod \langle p, \varphi\rangle$.
2. $\mathrm{val}_\varphi(u) = r$ and $\mathrm{val}_\varphi(v) > r$: $E_2'(\theta) \not\equiv 0 \bmod \langle p, \varphi\rangle$, for all $\theta \in R_0/\langle\varphi\rangle$.
3. $\mathrm{val}_\varphi(u) > r$ and $\mathrm{val}_\varphi(v) > r$: $E_2'(y_0)$ vanishes identically modulo $\langle p, \varphi\rangle$, so this case is ruled out by the hypothesis.

There is an efficient algorithm to find θ, if it exists; because the above proof only requires calculating valuations which entails division operations in the ring. □

Before the algorithm let us illustrate the process on Example 6.

Example 7. Consider the polynomial f from Example 6. We want to find factors of $f \equiv x^4 + 18x^3 + 33x^2 + 54x + 9 \bmod 81$. Fix $\varphi := x \in \mathbb{Z}[x]$ and $a = 2$.

Let us apply the reduction theorem (Theorem 11): $(\varphi^a - py)$ is a factor of $f \bmod p^4$ iff

$$E := f \cdot (\varphi^{3a} + \varphi^{2a}(py) + \varphi^a(py)^2 + (py)^3) \equiv 0 \bmod \langle p^4, \varphi^{4a}\rangle.$$

Putting the values $\varphi = x$, $p = 3$, $a = 2$ and substituting $y = y_0 + 3y_1$ [Lemma 12] we have,

$$(x^4+18x^3+33x^2+54x+9)[x^6+x^4 3(y_0+3y_1)+x^2 9(y_0+3y_1)^2+27(y_0+3y_1)^3] \equiv 0 \bmod \langle 81, x^8\rangle.$$

$$\Leftrightarrow 9x^4[(6x^2y_0 + 6x^2)y_1 + (3y_0^3 + y_0^2(x^2+6) + y_0(6x^3+2x^2+3) + 6x^3 + x^2)] \equiv 0 \bmod \langle 81, x^8\rangle.$$

Using Claim 8,

$$\Leftrightarrow (6x^2y_0 + 6x^2)y_1 + 3y_0^3 + y_0^2(x^2+6) + y_0(6x^3+2x^2+3) + 6x^3 + x^2 \equiv 0 \bmod \langle 9, x^4\rangle. \quad (5)$$

Reducing the last equation mod $\langle 3, x^4\rangle$ we have,

$$x^2y_0^2 + (2x^2)y_0 + x^2 \equiv 0 \bmod \langle 3, x^4\rangle.$$

$$\Leftrightarrow y_0^2 + 2y_0 + 1 \equiv 0 \bmod \langle 3, x^2\rangle.$$

Notice that this is the same equation as for the case of $k = 3$ in Example 6.

Applying Panayi (1995); Berthomieu et al. (2013) (Theorem 10) on last equation, we get exactly one representative root $y_0 = 2 + x*$.

We substitute $y_0 \to 2 + xy_0$ in Equation (5) and simplify to get,

$$(2xy_0)y_1 + xy_0^3 + 2y_0^2 + (2x)y_0 \equiv 0 \bmod \langle 3, x^2\rangle. \tag{6}$$

Equation (6) gives us $E_1(y_0) = xy_0^3 + 2y_0^2 + (2x)y_0 \bmod \langle 3, x^2\rangle$ and $E_2(y_0) = 2xy_0 \bmod \langle 3, x^2\rangle$.

We want the values of y_0's, such that, $val_x(E_1(y_0))$ is at least $val_x(E_2(y_0))$. Since $val_x(E_2(y_0))$ is 1, we are forced to have $y_0 = 0 \bmod \langle 3, x\rangle$. In that case, Equation (6) is identically zero, so y_1 is free to take any value mod $\langle 3, x^2\rangle$.

Taking $y_1 = 0$ and $y_0 = 2 + 0$ we have the corresponding factor $(x^2 - 3(2 + 0)) \equiv (x^2 + 75) \bmod 81$. The co-factor of this is $(x^2 + 18x + 39)$, giving

$$f \equiv x^4 + 18x^3 + 33x^2 + 54x + 9 \equiv (x^2 + 75)(x^2 + 18x + 39) \bmod 81.$$

4.4. Algorithm to find roots of $E(y)$

We have all the ingredients to give the algorithm for finding roots of $E(y)$ modulo ideal $\langle p^4, \varphi^{4a}\rangle$ of $\mathbb{Z}[x]$.

Input: A polynomial $E \in R[y]$ defined as $E := f \cdot (\varphi^{3a} + \varphi^{2a}(py) + \varphi^a(py)^2 + (py)^3)$.

Output: A set $Z \subseteq R_0$ and a *bad* set $Z' \subseteq R_0$, such that, for each $y_0 \in Z - Z'$, there are (efficiently computable) $y_1 \in R_0$ (Theorem 17) satisfying $E(y_0 + py_1) \equiv 0 \mod \langle p^4, \varphi^{4a}\rangle$. These are exactly the roots of E.

Also, both sets Z and Z' can be described by $O(a)$ many representatives (Theorem 17). (Recall that $a \le d$.) Hence, a $y_0 \in Z - Z'$ can be picked efficiently.

We prove the correctness of Algorithm 2 in the following theorem.

Theorem 17. *The output of Algorithm 2 (the set $Z - Z'$) contains exactly those $y_0 \in R_0$ for which there exist some $y_1 \in R_0$, such that, $y = y_0 + py_1$ is a root of E in R. We can compute the set of y_1 corresponding to a given $y_0 \in Z - Z'$ in poly($\deg f, \log p$) time.*

Thus, we efficiently describe (and exactly count) the roots $y = y_0 + py_1 + p^2y_2$ in R of E, where $y_0, y_1 \in R_0$ are as above and y_2 can assume any value from R.

Proof. The algorithm intends to output roots y of equation $E \equiv f \cdot (\varphi^{3a} + \varphi^{2a}(py) + \varphi^a(py)^2 + (py)^3) \equiv 0 \bmod \langle p^4, \varphi^{4a}\rangle$, where $y = y_0 + py_1 + p^2y_2$ with $y_0, y_1 \in R_0$ and $y_2 \in R$. From Lemma 12, any value of y_2 in $\mathbb{F}_p$ makes y a root, and we encode this by substituting the symbol $*$ for y_2.

Using Lemma 14, Algorithm 2 partially fixes y_0 from the set S_0 and reduces the problem to finding roots of an $E'(y_0, y_1) \bmod \langle p, \varphi^{4a}\rangle$. In other words, if we can find all roots (y_0, y_1) of $E'(y_0, y_1) \bmod \langle p, \varphi^{4a}\rangle$, then we can find (and count) all roots of $E(y) \bmod \langle p^4, \varphi^{4a}\rangle$. This is accomplished by Step 1. From Lemma 14, $|S_0| \le 2$, so loop at Step 3 runs only for a constant number of times.

Using Lemma 14, $E'(y_0, y_1) \equiv E_1(y_0) + E_2(y_0)y_1 \bmod \langle p, \varphi^{4a}\rangle$ for a cubic polynomial $E_1 \in R_0[y_0]$ and a linear polynomial $E_2 \in R_0[y_0]$.

We find all solutions of $E'(y_0, y_1)$ by going over all possible valuations of $E_2(y_0)$ with respect to φ. The case of valuation 0 is handled in Step 5 and valuation $4a$ is handled in Step 12. For the remaining valuations $r \in [4a - 1]$, Lemma 15 shows that it is enough to find $(z_0, z_1) \in R_0 \times R_0$ such that $\varphi^r | E_1(z_0)$ and $\varphi^r || E_2(z_0)$.

Algorithm 2 Finding all roots of $E(y)$ in R.

```
 1: Given $E(y_0+py_1)$, using Lemma 14, get the set $S_0$ of all representative pairs $(a_0,i_0)$, where $a_0 \in R_0$ and $i_0 \in \mathbb{N}$, such that $p^3|E((a_0+\varphi^{i_0}y_0)+py_1) \bmod \langle p^4,\varphi^{4a}\rangle$.
 2: Initialize sets $Z=\{\}$ and $Z'=\{\}$; seen as subsets of $R_0$.
 3: for each $(a_0,i_0) \in S_0$ do
 4:     Substitute $y_0 \mapsto a_0+\varphi^{i_0}y_0$, let $E'(y_0,y_1) = E_1(y_0)+E_2(y_0)y_1 \bmod \langle p,\varphi^{4a}\rangle$ be the polynomial obtained from Lemma 14.
 5:     If $E_2(y_0) \not\equiv 0 \bmod \langle p,\varphi\rangle$ then find (at most one) $\theta \in R_0/\langle\varphi\rangle$ such that $E_2(\theta) \equiv 0 \bmod \langle p,\varphi\rangle$. Update $Z \leftarrow Z \cup (a_0+\varphi^{i_0}*)$ and $Z' \leftarrow Z' \cup (a_0+\varphi^{i_0}(\theta+\varphi*))$.
 6:     for each possible valuation $r \in [4a]$ do
 7:         Initialize sets $Z_r=\{\}$ and $Z'_r=\{\}$.
 8:         Call Root-Find($E_1$, $\varphi^r$) to get a set $S_1$ of representative pairs $(a_1,i_1)$ where $a_1 \in R_0$ and $i_1 \in \mathbb{N}$ such that $E_1(a_1+\varphi^{i_1}y_0) \equiv 0 \bmod \langle p,\varphi^r\rangle$.
 9:         for each $(a_1,i_1) \in S_1$ do
10:             Analogously consider $E'_2(y_0) := E_2(a_1+\varphi^{i_1}y_0) \bmod \langle p,\varphi^{4a}\rangle$.
11:             Call Root-Find($E'_2$, $\varphi^r$) to get a representative pair $(a_2,i_2)$ ($\because E'_2$ is linear), where $a_2 \in R_0$ and $i_2 \in \mathbb{N}$ such that $E'_2(a_2+\varphi^{i_2}y_0) \equiv 0 \bmod \langle p,\varphi^r\rangle$.
12:             if $r=4a$ then
13:                 Update $Z_r \leftarrow Z_r \cup (a_1+\varphi^{i_1}(a_2+\varphi^{i_2}*))$ and $Z'_r \leftarrow Z'_r \cup \{\}$.
14:             else if $E'_2(a_2+\varphi^{i_2}y_0) \not\equiv 0 \bmod \langle p,\varphi^{r+1}\rangle$ then
15:                 Get a $\theta \in R_0/\langle\varphi\rangle$ (Lemma 16), if it exists, such that $E'_2(a_2+\varphi^{i_2}(\theta+\varphi y_0)) \equiv 0 \bmod \langle p,\varphi^{r+1}\rangle$. Update $Z'_r \leftarrow Z'_r \cup (a_1+\varphi^{i_1}(a_2+\varphi^{i_2}(\theta+\varphi*)))$.
16:                 Update $Z_r \leftarrow Z_r \cup (a_1+\varphi^{i_1}(a_2+\varphi^{i_2}*))$.
17:             end if
18:         end for
19:         Update $Z \leftarrow Z \cup (a_0+\varphi^{i_0}Z_r)$ and $Z' \leftarrow Z' \cup (a_0+\varphi^{i_0}Z'_r)$.
20:     end for
21: end for
22: Return $Z$ and $Z'$.
```

Notice that the number of valuations is bounded by $4a = O(\deg f)$. At Step 6, the algorithm runs through the possible values of the valuation r of $E_2(y_0) \in R_0[y_0]$ and subsequent computation finds all representative roots $b+\varphi^i*$ efficiently (using Theorem 10), such that,

$$E_1(b+\varphi^i y_0) \equiv E_2(b+\varphi^i y_0) \equiv 0 \bmod \langle p,\varphi^r\rangle .$$

The representative root $b+\varphi^i*$ is denoted by $a_1+\varphi^{i_1}(a_2+\varphi^{i_2}*)$ in Steps 13 and 16 of Algorithm 2.

Finally, we need to filter out those y_0's for which $E_2(b+\varphi^i y_0) \equiv 0 \bmod \langle p,\varphi^{r+1}\rangle$. This can be done efficiently using Lemma 16, where we get a unique $\theta \in R_0/\langle\varphi\rangle$ for which,

$$E_2(b+\varphi^i(\theta+\varphi y_0)) \equiv 0 \bmod \langle p,\varphi^{r+1}\rangle.$$

We store partial roots in two sets Z_r and Z'_r, where Z'_r contains the bad values filtered out by Lemma 16 as $b+\varphi^i(\theta+\varphi*)$ and Z_r contains all possible roots $b+\varphi^i*$. So, the set $Z_r - Z'_r$ contains exactly those elements z_0 for which there exists $z_1 \in R_0$, such that, the pair (z_0,z_1) is a root of $E'(y_0,y_1) \bmod \langle p,\varphi^{4a}\rangle$.

Note that size of each set S_1 obtained at Step 9 is bounded by three using Theorem 10 (E_1 is at most a cubic in y_0). Again using Theorem 10, we get at most one pair (a_2,i_2) at Step 11 for some $a_2 \in R_0$ and $i_2 \in \mathbb{N}$ (E'_2 is linear in y_0).

Now, for a fixed $z_0 \in Z_r - Z'_r$ we can calculate all z_1's by the equation

$$z_1 \equiv \tilde{z}_1 := -(C(y_0)/L(y_0)) \bmod \langle p,\varphi^{4a-r}\rangle.$$

Here $C(y_0) := E_1(z_0)/\varphi^r \bmod \langle p,\varphi^{4a-r}\rangle$ and $L(y_0) := E_2(z_0)/\varphi^r \bmod \langle p,\varphi^{4a-r}\rangle$. So, $z_1 \in R_0$ comes from the set $z_1 \in \tilde{z}_1+\varphi^{4a-r}*$. This can be done in poly($\deg f, \log p$) time.

Finally, the sets $Z = a_0+\varphi^{i_0}Z_r$ and $Z' = a_0+\varphi^{i_0}Z'_r$, for $(a_0,i_0) \in S_0$ and corresponding valid $r \in \{0,\dots,4a-1\}$, returned by Algorithm 2, describe the y_0 for the roots of $E(y_0+py_1) \bmod \langle p^4,\varphi^{4a}\rangle$. The number of representatives in each of these sets is $O(a)$, since $|S_0| \le 2$ and sizes of Z_r and Z'_r are only constant.

Since we can efficiently describe these y_0's and corresponding y_1's, and we know their precision, we can count all roots $y = y_0 + py_1 + p^2 * \subseteq R$ of $E(y) \bmod \langle p^4, \varphi^{4a}\rangle$. $\square$

4.5. Wrapping up Theorems 1 and 2

Proof of Theorem 1. We prove that given an arbitrary univariate $f \in \mathbb{Z}[x]$ and a prime p, a non-trivial factor of f modulo p^4 can be obtained in randomized poly($\deg f, \log p$) time (or the irreducibility of $f \bmod p^4$ gets certified).

If $f \equiv f_1 f_2 \bmod p$, where f_1, f_2 are two polynomials coprime in $F_p[x]$, then we can efficiently lift this factorization to the ring $(\mathbb{Z}/\langle p^4\rangle)[x]$, using Hensel lemma (Lemma 4), to get non-trivial factors of $f \bmod p^4$.

For the remaining case, $f \equiv \varphi^e \bmod p$ for an irreducible polynomial $\varphi(x)$ modulo p. The question of factoring $f \bmod p^4$ then reduces to root finding of a polynomial $E(y) \bmod \langle p^4, \varphi^{4a}\rangle$ by Reduction theorem (Theorem 11). Using Theorem 17, we get all such roots and hence a non-trivial factor of $f \bmod p^4$ is found. If there are no roots $y \in R$ of E, for all $a \le e/2$, then the polynomial f is irreducible (by symmetry, if there is a factor for $a > e/2$ then there is a factor for $a \le e/2$). $\square$

Proof of Theorem 2. We are given a univariate $f \in \mathbb{Z}[x]$ of degree d and a prime p, such that, $f \bmod p$ is a power of an irreducible polynomial $\varphi(x)$. So, f is of the form $\varphi(x)^e + ph(x) \bmod p^4$, for an integer $e \in \mathbb{N}$ and a polynomial $h \in (\mathbb{Z}/\langle p^4\rangle)[x]$ of degree $\le d$ (also, $\deg \varphi^e \le d$). By unique factorization over the ring $\mathbb{F}_p[x]$, if $\tilde{g}$ is a factor of $f \bmod p$ then, $\tilde{g} \equiv \tilde{v}\varphi^a \bmod p$ for a unit $\tilde{v} \in \mathbb{F}_p$.

First, we show that it is enough to find all the lifts of $\tilde{g}$, such that, $\tilde{g} \equiv \varphi^a \bmod p$ for an $a \le e$. If $\tilde{g} \equiv \tilde{v}\varphi^a \bmod p$, then any lift has the form $g(x) \equiv v(x)(\varphi^a - py) \bmod p^4$ for a unit $v(x) \in (\tilde{v} + p*) \subseteq (\mathbb{Z}/\langle p^4\rangle)[x]$. Any such $g(x)$ maps uniquely to a $g_1(x) := \tilde{v}^{-1}g(x) \bmod p^4$, which is a lift of $\varphi^a \bmod p$. So, it is enough to find all the lifts of $\varphi^a \bmod p$.

We know that any lift $g \in (\mathbb{Z}/\langle p^4\rangle)[x]$ of $\tilde{g}(x)$, which is a factor of f, must be of the form $\varphi^a - py \bmod p^4$ for a polynomial $y \in (\mathbb{Z}/\langle p^4\rangle)[x]$. By Reduction theorem (Theorem 11), we know that finding such a factor is equivalent to solving for y in the equation $E(y) \equiv 0 \bmod \langle p^4, \varphi^{4a}\rangle$. By Theorem 17, we can find all such roots y in randomized poly($d, \log p$) time, for $a \le e/2$.

If $a > e/2$ then we replace a by $b := e - a$, as $b \le e/2$, and solve the equation $E(y) \equiv 0 \bmod \langle p^4, \varphi^{4b}\rangle$ using Theorem 17. This time the factor corresponding to y will be, $g \equiv f/(\varphi^b - py) \equiv E(y)/\varphi^{4b} \bmod p^4$, using Reduction theorem (Theorem 11).

The number of lifts of $\tilde{g}(x)$ which divide $f \bmod p^4$ is the count of y's that appear above. This is efficiently computable via Algorithm 2. $\square$

5. Barriers to extension modulo higher powers p^k

The reader may wonder about polynomial factoring when k is greater than 4. In this section we will discuss the issues in applying our techniques to factor $f(x) \bmod p^5$.

Given $f \equiv \varphi^e \bmod p$, finding one of its factor $\varphi^a - py \bmod p^5$, for $a \le e/2$ and $y \in (\mathbb{Z}/\langle p^5\rangle)[x]$, is reduced to solving the equation

$$E \ := \ f \cdot (\varphi^{4a} + \varphi^{3a}(py) + \varphi^{2a}(py)^2 + \varphi^a(py)^3 + (py)^4) \ \equiv \ 0 \ \bmod \langle p^5, \varphi^{5a}\rangle \tag{7}$$

By Lemma 12, the roots of $E \bmod \langle p^5, \varphi^{5a}\rangle$ are of the form $y = y_0 + py_1 + p^2y_2 + p^3*$ in R, where $y_0, y_1, y_2 \in R_0$ need to be found.

First issue. The first hurdle comes when we try to reduce root-finding modulo the bi-generated ideal $\langle p^5, \varphi^{5a}\rangle \subseteq \mathbb{Z}[x]$ to root-finding modulo the principal ideal $\langle \varphi^{5a}\rangle \subseteq \mathbb{F}_p[x]$. In the case $k = 4$, Lemma 14 guarantees that we need to solve at most two related equations of the form $E'(y_0, y_1) \equiv 0 \bmod \langle p, \varphi^{4a}\rangle$ to find exactly the roots of $E \bmod \langle p^4, \varphi^{4a}\rangle$. Below, for $k = 5$, we show that we have exponentially many candidates for $E'(y_0, y_1, y_2) \in R_0[y_0, y_1, y_2]$ and it is not clear if there is any compact efficient representation for them.

Putting $y = y_0 + py_1 + p^2y_2$ in Eqn. (7) we get,

$$E(y) \ =: \ E_1(y_0) + E_2(y_0)y_1 + E_3(y_0)y_2 + (f\varphi^{2a}p^4)y_1^2 \ \equiv \ 0 \ \bmod \langle p^5, \varphi^{5a}\rangle, \tag{8}$$

where $E_1(y_0) := f\varphi^{4a} + f\varphi^{3a}py_0 + f\varphi^{2a}p^2y_0^2 + f\varphi^{a}p^3y_0^3 + fp^4y_0^4$ is a quartic in $R[y_0]$, $E_2(y_0) := f\varphi^{3a}p^2 + f\varphi^{2a}2p^3y_0 + f\varphi^{a}3p^4y_0^2$ is a quadratic in $R[y_0]$ and $E_3(y_0) := f\varphi^{3a}p^3 + f\varphi^{2a}2p^4y_0$ is linear in $R[y_0]$.

To divide Eqn. (8) by p^3, we go mod $\langle p^3, \varphi^{5a}\rangle$ obtaining

$$E(y) \equiv E_1(y_0) \equiv f\varphi^{4a} + f\varphi^{3a}py_0 + f\varphi^{2a}p^2y_0^2 \equiv 0 \bmod \langle p^3, \varphi^{5a}\rangle,$$

a univariate quadratic equation which requires the whole machinery used in the case $k = 3$. We get this simplified equation since $E_3(y_0) \equiv 0 \bmod \langle p^3, \varphi^{5a}\rangle$ and $E_2(y_0) \equiv f\varphi^{3a}p^2 \equiv \varphi^{e-2a}\varphi^{2a+3a}p^2 \equiv 0 \bmod \langle p^3, \varphi^{5a}\rangle$.

But, to really reduce Eqn. (8) to a system modulo the principal ideal $\langle\varphi^{5a}\rangle \subseteq \mathbb{F}_p[x]$, we need to divide it by p^4. So, we go mod $\langle p^4, \varphi^{5a}\rangle$:

$$E(y) \equiv E_1'(y_0) + E_2'(y_0)y_1 \equiv 0 \bmod \langle p^4, \varphi^{5a}\rangle$$

where $E_1'(y_0) \equiv E_1(y_0) \bmod \langle p^4, \varphi^{5a}\rangle$ is a cubic in $R[y_0]$ and $E_2'(y_0) \equiv E_2(y_0) \bmod \langle p^4, \varphi^{5a}\rangle$ is linear in $R[y_0]$. This requires us to solve a special bivariate equation which requires the machinery used in the case $k = 4$.

Now, the problem reduces to computing a solution pair $(y_0, y_1) \in (R_0)^2$ of this bivariate equation. We can apply the idea used in Algorithm 2 to get all valid y_0 efficiently, but since y_1 is a function of y_0, we need to compute exponentially many y_1's. So, there seem to be exponentially many candidates for $E'(y_0, y_1, y_2)$, that behaves like $E(y)/p^4$ and lives in $(\mathbb{F}_p[x]/\langle\varphi^{5a}\rangle)[y_0, y_1, y_2]$. At this point, we are forced to compute all these E's, as we do not know which one will lead us to a solution of Eqn. (8).

Second issue. Even if we resolve the first issue and get a valid E', we are left with a trivariate equation to be solved mod $\langle p, \varphi^{5a}\rangle$ (Eqn. (8) after shifting y_0 and y_1 then dividing by p^4). We could do this when k was 4, because we could easily write y_1 as a function of y_0. Though, it is unclear how to solve this trivariate equation now as it is *nonlinear* in both y_0 and y_1.

For $k > 5$ the difficulty will only increase because of the recursive nature of Eqn. (7) with more and more unknowns (with higher degrees).

6. Conclusion

The study of von zur Gathen and Hartlieb (1998, 1996) sheds some light on the behavior of the factoring problem for integral polynomials modulo prime powers. It shows that for "large" k the problem is similar to the factorization over p-adic fields (already solved efficiently by Cantor and Gordon (2000)). But, for "small" k the problem seems hard to solve in polynomial time. We do not even know a practical algorithm.

This motivated us to study the case of constant k, with the hope that this will help us invent new tools. In this direction, we made significant progress by giving a unified method to factor f mod p^k for $k \leq 4$. We also refined Hensel lifting for $k \leq 4$, by giving all possible lifts of a factor of f mod p, in the classically hard case of f mod p being a power of an irreducible.

We gave a general framework (for any k) to work on, by reducing factoring in a big ring to root-finding in a smaller ring. We leave it open whether we can factor f mod p^5, and beyond, within this framework.

We also leave it open, to efficiently get all the solutions of a *bivariate* equation, in $\mathbb{Z}/\langle p^k\rangle$ or $\mathbb{F}_p[x]/\langle\varphi^k\rangle$, in a compact representation. Surprisingly, we know how to achieve this for univariate polynomials (Panayi, 1995; Berthomieu et al., 2013). This, combined with our work, will probably give factoring mod p^k, for any k.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We thank anonymous reviewers for helpful comments, valuable suggestions and for providing useful references (in particular Panayi (1995)). We thank Vishwas Bhargava for introducing us to the open problem of factoring f mod p^3. N.S. thanks the funding support from DST (DST/SJF/MSA-01/2013-14). R.M. would like to thank support from DST through grant DST/INSPIRE/04/2014/001799.

References

Apostol, T.M., 2013. Introduction to Analytic Number Theory. Springer Science & Business Media.

Berlekamp, E.R., 1967. Factoring polynomials over finite fields. Bell Syst. Tech. J. 46 (8), 1853–1859.

Berthomieu, J., Lecerf, G., Quintin, G., 2013. Polynomial root finding over local rings and application to error correcting codes. Appl. Algebra Eng. Commun. Comput. 24 (6), 413–443. https://link.springer.com/article/10.1007/s00200-013-0200-5.

Borevich, Z.I., Shafarevich, I.R., 1986. Number Theory, vol. 20. Academic Press.

Cantor, D.G., Gordon, D.M., 2000. Factoring polynomials over p-adic fields. In: International Algorithmic Number Theory Symposium. Springer, pp. 185–208.

Cantor, D.G., Zassenhaus, H., 1981. A new algorithm for factoring polynomials over finite fields. Math. Comput., 587–592.

Cheng, H., Labahn, G., 2001. Computing all factorizations in $\mathbb{Z}_N[x]$. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. ISSAC'01, pp. 64–71.

Cheng, Q., Gao, S., Rojas, J.M., Wan, D., 2018. Counting roots of polynomials over prime power rings. In: Thirteenth Algorithmic Number Theory Symposium, ANTS-XIII. Mathematical Sciences Publishers. arXiv:1711.01355.

Chistov, A.L., 1987. Efficient factorization of polynomials over local fields. Dokl. Akad. Nauk SSSR 293 (5), 1073–1077.

Chistov, A.L., 1994. Algorithm of polynomial complexity for factoring polynomials over local fields. J. Math. Sci. 70 (4), 1912–1933.

Denef, J., Hoornaert, K., 2001. Newton polyhedra and Igusa's local zeta function. J. Number Theory 89 (1), 31–64.

Dwivedi, A., Mittal, R., Saxena, N., 2019a. Counting basic-irreducible factors mod p^k in deterministic poly-time and p-adic applications. In: Shpilka, A. (Ed.), 34th Computational Complexity Conference. CCC 2019. In: Leibniz International Proceedings in Informatics (LIPIcs), vol. 137. Schloss Dagstuhl–Leibniz-Zentrum Fuer Informatik, Dagstuhl, Germany, 15. http://drops.dagstuhl.de/opus/volltexte/2019/10837.

Dwivedi, A., Mittal, R., Saxena, N., 2019b. Efficiently factoring polynomials modulo p^4. In: Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation. ISSAC'19. ACM, New York, NY, USA, pp. 139–146. http://doi.acm.org/10.1145/3326229.3326233.

Dwivedi, A., Saxena, N., 2020. Computing Igusa's local zeta function of univariates in deterministic polynomial-time. In: Proceedings of Algorithmic Number Theory Symposium, ANTS XIV. University of Auckland, New Zealand, in press. Mathematical Sciences Publishers, arXiv:2006.08926.

Forbes, M.A., Shpilka, A., 2015. Complexity theory column 88: challenges in polynomial factorization. ACM SIGACT News 46 (4), 32–49.

Guàrdia, J., Nart, E., Pauli, S., 2012. Single-factor lifting and factorization of polynomials over local fields. J. Symb. Comput. 47 (11), 1318–1346. https://doi.org/10.1016/j.jsc.2012.03.001.

Hensel, K., 1918. Eine neue Theorie der algebraischen Zahlen. Math. Z. 2 (3), 433–452.

Kaltofen, E., 1992. Polynomial factorization 1987–1991. In: Latin American Symposium on Theoretical Informatics. Springer, pp. 294–313.

Kedlaya, K.S., Umans, C., 2011. Fast polynomial factorization and modular composition. SIAM J. Comput. 40 (6), 1767–1802.

Klivans, A., 1997. Factoring polynomials modulo composites. Tech. Rep. Carnegie-Mellon Univ, Pittsburgh PA, Dept of CS.

Kopp, L., Randall, N., Rojas, J., Zhu, Y., 2019. Randomized polynomial-time root counting in prime power rings. Math. Comput. 1.

Landau, S., 1985. Factoring polynomials over algebraic number fields. SIAM J. Comput. 14 (1), 184–195.

Lenstra, A.K., Lenstra, H.W., Lovász, L., 1982. Factoring polynomials with rational coefficients. Math. Ann. 261 (4), 515–534.

Neiger, V., Rosenkilde, J., Schost, É., 2017. Fast computation of the roots of polynomials over the ring of power series. In: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation. ACM, pp. 349–356.

Niven, I., Zuckerman, H.S., Montgomery, H.L., 2013. An Introduction to the Theory of Numbers. John Wiley & Sons.

Panayi, P.N., 1995. Computation of Leopoldt's P-adic regulator. Ph.D. thesis. University of East Anglia.

Pauli, S., Roblot, X.-F., 2001. On the computation of all extensions of a p-adic field of a given degree. Math. Comput. 70 (236), 1641–1659.

Sălăgean, A., 2005. Factoring polynomials over $\mathbb{Z}_4$ and over certain Galois rings. Finite Fields Appl. 11 (1), 56–70.

Shamir, A., 1993. On the generation of multivariate polynomials which are hard to factor. In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing. ACM, pp. 796–804.

Sircana, C., 2017. Factorization of polynomials over $\mathbb{Z}/(p^n)$. In: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation. ACM, pp. 405–412.

von zur Gathen, J., Hartlieb, S., 1996. Factorization of polynomials modulo small prime powers. Tech. Rep. Paderborn Univ.

von zur Gathen, J., Hartlieb, S., 1998. Factoring modular polynomials. J. Symb. Comput. 26 (5), 583–606.

von zur Gathen, J., Panario, D., 2001. Factoring polynomials over finite fields: a survey. J. Symb. Comput. 31 (1–2), 3–17.

Zassenhaus, H., 1969. On Hensel factorization, I. J. Number Theory 1 (3), 291–311.

Zuniga-Galindo, W., 2003. Computing Igusa's local zeta functions of univariate polynomials, and linear feedback shift registers. J. Integer Seq. 6 (2), 3.