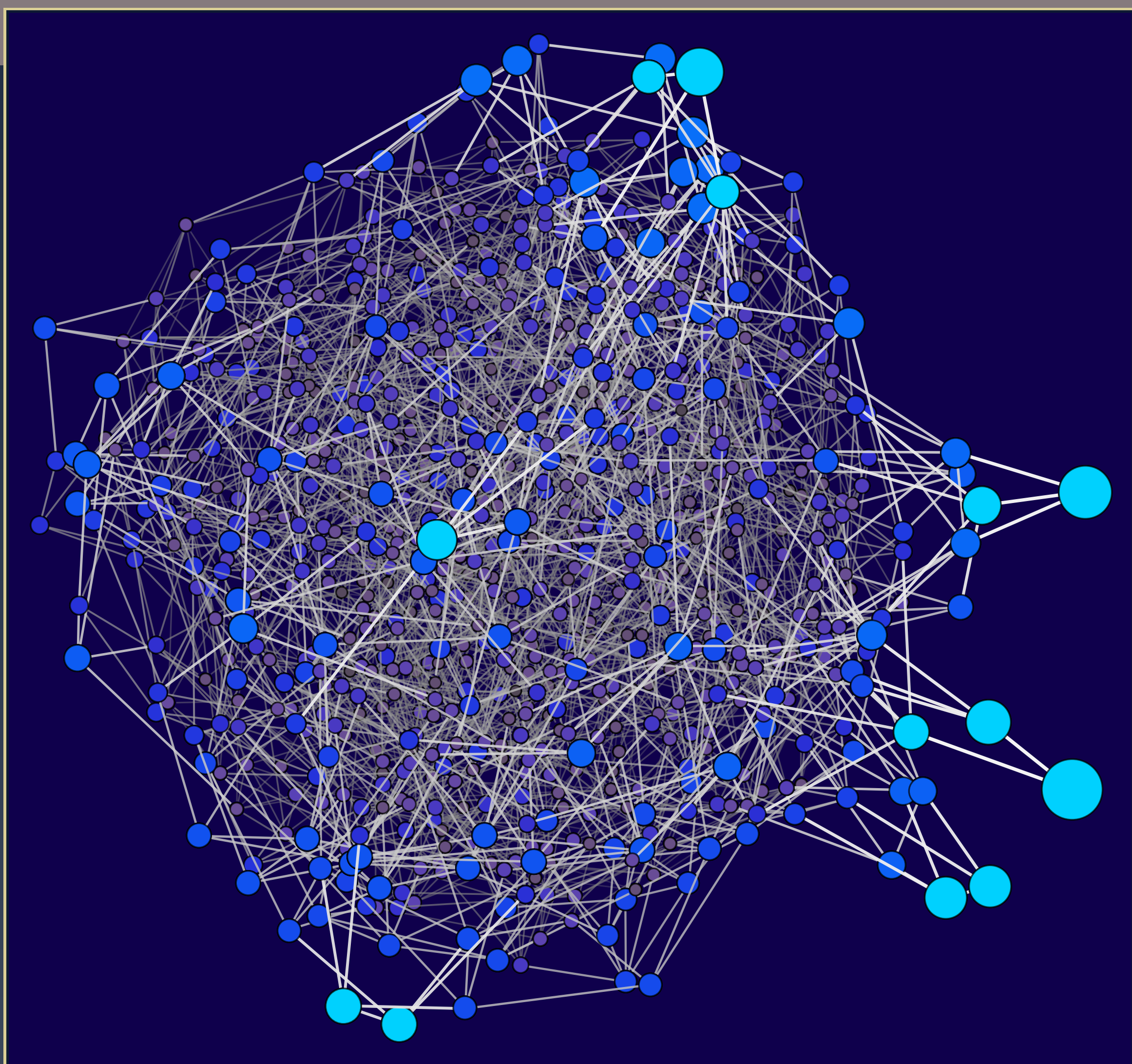
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Computing Igusa's local zeta function of univariates in deterministic polynomial-time

Ashish Dwivedi and Nitin Saxena



msp

THE OPEN BOOK SERIES 4 (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.197

Computing Igusa's local zeta function of univariates in deterministic polynomial-time

Ashish Dwivedi and Nitin Saxena

Igusa's local zeta function $Z_{f,p}(s)$ is the generating function that counts the number of integral roots, $N_k(f)$, of $f(\boldsymbol{x}) \bmod p^k$, for all k. It is a famous result, in analytic number theory, that $Z_{f,p}$ is a rational function in $\mathbb{Q}(p^s)$. We give an elementary proof of this fact for a univariate polynomial f. Our proof is constructive as it gives a closed-form expression for the number of roots $N_k(f)$.

Our proof, when combined with the recent root-counting algorithm of Dwivedi, Mittal and Saxena (Computational Complexity Conference, 2019), yields the first deterministic poly($|f|$, log p)-time algorithm to compute $Z_{f,p}(s)$. Previously, an algorithm was known only in the case when f completely splits over $\mathbb{Q}_p$; it required the rational roots to use the concept of generating function of a tree (Zúñiga-Galindo, J. Int. Seq., 2003).

1. Introduction

Over the years, the study of zeta functions has played a foundational role in the development of mathematics. They have applications in diverse science disciplines; in particular, machine learning [72], cryptography [2; 3], quantum cryptography [45], statistics [72; 47], theoretical physics [31; 53], string theory [51], quantum field theory [27; 31] and biology [57; 77]. Basically, a zeta function counts some mathematical objects. Often zeta functions show special analytic, or algebraic properties, the study of which can reveal striking information about the encoded object.

A classic example is the famous Riemann zeta function [54] (also known as the Euler–Riemann zeta function) which encodes the density and distribution of prime numbers [16; 64]. Later many *local* (i.e., associated to a specific prime p) zeta functions were studied; e.g., the Hasse–Weil zeta function [73; 74], which encodes the count of zeros of a system of polynomial equations over finite fields (of a specific characteristic p). The study of this function led to the development of modern algebraic geometry (see [19; 30]).

In this paper we are interested in a different local zeta function known as Igusa's local zeta function. It encodes the count of roots modulo prime powers of a given polynomial defined over a local field.

MSC2010: primary 11S40, 68Q01, 68W30; secondary 11Y16, 14G50.
Keywords: Igusa, local, zeta function, discriminant, valuation, deterministic, root, counting, modulo, prime power.

Formally, *Igusa's local zeta function* $Z_{f,p}(s)$, attached to a polynomial over p-adic integers

$$f(\boldsymbol{x}) \in \mathbb{Z}_p[x_1, \dots, x_n]$$

is defined as

$$Z_{f,p}(s) := \int_{\mathbb{Z}_p^n} |f(\boldsymbol{x})|_p^s \cdot |d\boldsymbol{x}|,$$

where $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$, $|\cdot|_p$ denotes the absolute value over p-adic numbers $\mathbb{Q}_p$, and $|d\boldsymbol{x}|$ denotes the Haar measure on $\mathbb{Q}_p^n$ normalized so that $\mathbb{Z}_p^n$ has measure 1.

Weil [75; 76] defined these zeta functions inspired by those of Riemann. Later they were studied extensively by Igusa [34; 35; 36]. Using the method of resolution of singularities, Igusa proved that $Z_{f,p}(s)$ converges to a rational function. Later the convergence was proved by Denef [20] via a different method (namely, p-adic cell decomposition). The Igusa zeta function is closely related to *Poincaré series* $P(t)$, attached to f and p, defined as

$$P(t) := \sum_{i=0}^{\infty} N_i(f) \cdot (p^{-n}t)^i,$$

where $t \in \mathbb{C}$ with $|t| < 1$, and $N_i(f)$ is the count on roots of $f \bmod p^i$ (also $N_0(f) := 1$). In fact, it has been shown in [33] that

$$P(t) = \frac{1 - t \cdot Z_{f,p}(s)}{1 - t}$$

with $t =: p^{-s}$. So rationality of $Z_{f,p}(s)$ implies rationality of $P(t)$ and vice versa; thus proving a conjecture of [52] that $P(t)$ is a rational function. This relation makes the local zeta function interesting in arithmetic geometry (see [33; 21; 50; 44] for more on the Igusa zeta function).

Many researchers have tried to calculate the expression for the Igusa zeta function for various polynomial families [17; 56; 66; 1; 22; 48; 65; 32; 58; 79; 81] and this has led to the development of various methodologies; for example, the stationary phase formula (SPF), the Newton polygon method, resolution of singularities, etc. These methods have been fruitful in various other situations [23; 82; 83; 59; 39; 40; 84; 68; 61; 85]. However, not much has been said about their algorithmic aspect except in the case of resolution of singularities [6; 9; 8; 67]. These algorithms are impractical [7]. Indeed, the computation of the Igusa zeta function for a general multivariate polynomial seems to be an intractable problem since root-counting of a multivariate polynomial over a finite field is known to be #P-hard [28; 26].

In this paper, we focus on the computation of the Igusa zeta function when the associated polynomial is *univariate*. The Igusa zeta function for a univariate polynomial f is connected to root-counting of f modulo prime powers p^k, which is itself an interesting problem. It has applications in factoring [13; 14; 10], coding theory [4; 60], elliptic curve cryptography [43], arithmetic algebraic geometry [80; 22; 21], and the study of root sets [62; 15; 5; 18; 49]. After a long series of work [70; 71; 38; 60; 4; 63; 12; 42; 25], this problem was recently resolved in [24].

In the case of univariate polynomials one naturally expects an elementary proof of convergence, as well as an efficient algorithm to compute the Igusa zeta function. Our main result is:

> We give the first deterministic polynomial time algorithm to compute the rational function form of the Igusa zeta function associated to a given univariate polynomial $f \in \mathbb{Z}[x]$ and prime p.

To the best of our knowledge, this result was previously achieved only for the restricted class of univariate polynomials using methods that were sophisticated and nonexplicit. For example, Zúñiga-Galindo [80] achieved this for univariate polynomials which completely split over $\mathbb{Q}$ (with the factorization given in the input), using the stationary phase formula (see Section 1.2). The methods to compute the Igusa zeta function for a multivariate, e.g., Denef [20], continue to be impractical in the case of univariate polynomials. On the other hand, our approach is elementary, uses explicit methods, and completely solves the problem.

1.1. ***Our results.*** We will compute the Igusa zeta function $Z_{f,p}(s)$ by finding the related Poincaré series $P(t) =: A(t)/B(t)$.

Theorem 1. *We are given a univariate integral polynomial $f(x) \in \mathbb{Z}[x]$ of degree d, with coefficients of magnitude bounded by $C \in \mathbb{N}$, and a prime p. Then, we compute the Poincaré series $P(t) = A(t)/B(t)$, associated with f and p, in deterministic poly$(d, \log C + \log p)$-time.*

The degree of the integral polynomial $A(t)$ is $\tilde{O}(d^2 \log C)$ and that of $B(t)$ is $O(d)$.

Remarks. **(1)** Our method gives an elementary proof of rationality of $Z_{f,p}(s)$ as a function of $t = p^{-s}$.

(2) Previously, Zúñiga-Galindo [80] gave a deterministic polynomial time algorithm to compute $Z_{f,p}(s)$, if f completely splits over $\mathbb{Q}$ and the roots are provided. Our Theorem 1 works for *any* input $f \in \mathbb{Z}[x]$ (see Section 1.2 for further discussion).

(3) Cheng et al. [12] could compute $Z_{f,p}(s)$ in deterministic polynomial time, in the special case where the degree of $A(t)$, $B(t)$ is constant.

(4) Dwivedi et al. [24], using [80], remarked that $Z_{f,p}(s)$ could be computed in deterministic polynomial time, in the special case when f completely splits over $\mathbb{Q}_p$ *without* the roots being provided in the input. The detailed proof of this claim was not given and the convergence relied on the old method of [80].

We achieve the rational form of $Z_{f,p}(s)$ by getting an explicit formula for the number of zeros $N_k(f)$, of f mod p^k, which sheds new light on the properties of the function $N_k(\cdot)$. Eventually, it gives an elementary proof of the rationality of the Poincaré series $\sum_{i=0}^{\infty} N_i(f) \cdot (p^{-1}t)^i$.

Corollary 2. *Let k be large enough, namely, $k \geq k_0 := O(d^2(\log C + \log d))$. Then, we give a closed form expression for $N_k(f)$ (in Theorem 21).*

Interestingly, if f has nonzero discriminant, then $N_k(f)$ is constant (independent of k) for all $k \geq k_0$.

1.2. ***Further remarks and comparison.*** To the best of our knowledge, there have been very few results on the complexity of computing Igusa's zeta function for univariate polynomials [80; 12]. Other very specialized algorithms are for bivariate polynomials (e.g., hyperelliptic curves) [11], and for the polynomial $x^q - a$ [65]. In a recent related work [78, Appendix A], a different proof of rationality of Igusa's zeta function for univariate polynomials based on tree based algorithm of [42] is given.

An old proof technique called the *stationary phase formula* is the standard method used in the literature to compute Igusa's zeta function for various families of polynomials. Our work, on the other hand, uses elementary techniques and a tree-based root-counting algorithm [24] to compute some fixed parameters (independent of k) involved in our formula of $N_k(f)$, for all $k \geq k_0$.

It is to be noted that just efficiently computing $N_k(f)$, for "several" k, is not enough to compute the rational form of $Z_{f,p}(s)$; neither does it imply the rationality of $Z_{f,p}(s)$ directly.

Our algorithm is *deterministic* and works for general $f \in \mathbb{Z}_p[x]$ (provided f has computable representation). For earlier methods to work for $f \in \mathbb{Z}_p[x]$ they may need factoring over p-adics $\mathbb{Z}_p$ or $\mathbb{Q}_p$ (for example [80]), but deterministic algorithms there are unknown. See [13; 14; 10] for randomized factoring algorithms.

1.3. ***Proof idea.*** We will compute the rational form of Igusa's zeta function via computing the rational form of corresponding Poincaré series

$$P(t) := \sum_{i=0}^{\infty} N_i(f) \cdot (p^{-1}t)^i.$$

In addition, our method proves that the Poincaré series is a rational function of t, in the case of univariate polynomial $f(x)$, via first principles; instead of using advanced tools like the stationary phase method or Newton polygon method or resolution of singularity.

To compute the rational form of Poincaré series, the idea is to compute the coefficient sequence

$$\{N_0(f), \dots, N_k(f), \dots\}$$

in a closed form. That is to say, we wish to get an explicit formula for $N_k(f)$, the number of roots of $f \bmod p^k$, only in terms of k; with the hope that this will help in getting a rational function for the Poincaré series $P(t)$.

Indeed in Theorem 21, we show that such a formula exists for each $N_k(f)$ for sufficiently large k. We achieve this by establishing a connection among roots of $f \bmod p^k$ and $\mathbb{Z}_p$-roots of $f \in \mathbb{Z}_p[x]$. Let f have n distinct $\mathbb{Z}_p$-roots $\alpha_1, \dots, \alpha_n$. An important concept we define is that of "neighborhood" of an $\alpha_i \bmod p^k$ (Definition 18); these are basically roots of $f \bmod p^k$ "associated" to α_i. In Lemma 15, we show that *each* root $\overline{\alpha}$ of $f \bmod p^k$ is associated to a *unique* $\mathbb{Z}_p$-root α_i of f: $\overline{\alpha}$ closely approximates α_i but is quite far from other α_js, for all $j \in [n]$, $j \neq i$. So, the root-set of $f \bmod p^k$ can be partitioned into n subsets $S_{k,i}$, $i \in [n]$, where neighborhood $S_{k,i}$ is the set of those roots of $f \bmod p^k$ which are associated to $\mathbb{Z}_p$-root α_i.

Let the multiplicity of root α_i be e_i; then $f(x) =: (x - \alpha_i)^{e_i} f_i(x)$ over $\mathbb{Z}_p$, where $f_i(\alpha_i) \neq 0$. We call f_i the *α_i-free part* of f. Then, for $\overline{\alpha}$ to be a root of $f \bmod p^k$ we must have

$$f(\overline{\alpha}) = (\overline{\alpha} - \alpha_i)^{e_i} \cdot f_i(\overline{\alpha}) \equiv 0 \bmod p^k.$$

Lemma 16 says that f_i possesses equal valuation ν_i, for all roots of $f \bmod p^k$ associated to α_i, i.e, ones in $S_{k,i}$. That is, the maximum power of p dividing $f_i(\overline{\alpha})$ is the same as that for $f_i(\overline{\beta})$, as long as $\overline{\alpha}, \overline{\beta} \in S_{k,i}$. Note that $v_p((\overline{\alpha}-\alpha_i)^{e_i} \cdot f_i(\overline{\alpha})) \geq k$ if and only if $v_p((\overline{\alpha}-\alpha_i)) \geq (k-\nu_i)/e_i$.

Eventually, these two lemmas together give us the size of the neighborhood, $|S_{k,i}| = p^{k-\lceil (k-\nu_i)/e_i \rceil}$. Moreover, the neighborhoods disjointly cover all the roots of $f \bmod p^k$. Hence, $N_k(f) = \sum_{i=1}^{n} |S_{k,i}|$. This is a formula for $N_k(f)$, when k is large. But still the two parameters ν_i and e_i are unknown as, unlike in [80], we are not provided the factorization of f over $\mathbb{Z}_p$ (nor could we find it in deterministic polynomial time).

To compute ν_i, e_i, we use the help of the root-counting algorithm of [24], which gives us the value of $N_k(f)$, and the underlying root-set structure that it developed. We show that each representative root $\overline{\alpha}_i$ of $f \bmod p^k$ is indeed the neighborhood $S_{k,i}$ (Theorem 19), shedding new light on the root-set mod prime powers.

Now we can get two equations, for the two unknowns ν_i, e_i, by calling the algorithm of [24] twice: first for $k = k_i$ and second for $k = k_i + e_i$, where k_i is such that $(k_i - \nu_i)/e_i$ is an integer (e.g., we can try all k_i in the range $[k_0, \ldots, k_0 + \deg(f)]$). So, we can efficiently compute ν_i, e_i for a particular *representative root* $\overline{\alpha}_i$, $i \in [n]$. So, this calculation also reveals some new parameters of representative roots which were not mentioned in earlier related works [4; 24].

2. Preliminaries

2.1. *Root-set of a univariate polynomial mod prime powers.* We recall a structural property (and related objects) of the root-set of univariate polynomials in the ring $\mathbb{Z}/\langle p^k \rangle$ [24; 25].

Proposition 3. *The root-set of an integral univariate polynomial f, over the ring of integers modulo prime powers, is the disjoint union of at most* $\deg(f)$ *many efficiently representable subsets.*

We call these efficiently representable subsets *representative roots*, as defined and named in [25, Section 2]. This property of root-sets in $\mathbb{Z}/\langle p^k \rangle$ is indeed a generalization of the property of root-sets over a field: there are at most $\deg(f)$ many roots of $f(x)$ in a field.

To present representative roots formally, we first reiterate some notation from [25, Section 2].

Representatives. An abbreviation $*$ will be used to denote all of the underlying ring R. So for the ring $R = \mathbb{Z}/\langle p^k \rangle$, $*$ denotes all the p^k distinct elements. Perceiving any element of R in base-p representation, like $x_0 + px_1 + \cdots + p^{k-1}x_{k-1}$ where $x_i \in \{0, \ldots, p-1\}$ for all $i \in \{0, \ldots, k-1\}$, the set

$$\boldsymbol{a} := a_0 + pa_1 + \cdots + p^{l-1}a_{l-1} + p^l *$$

"represents" the set of all the elements of R which are congruent to $a_0 + pa_1 + \cdots + p^{l-1}a_{l-1} \bmod p^l$. Throughout the paper we call such sets *representatives* and we denote them using bold small letters, like $\boldsymbol{a}$, $\boldsymbol{b}$ etc.

Let us denote the *length* of a representative $\boldsymbol{a}$ by $|\boldsymbol{a}|$, so if $\boldsymbol{a} := a_0 + pa_1 + \cdots + p^{l-1}a_{l-1} + p^l *$ then its length is $|\boldsymbol{a}| = l$. Now we formally define representative roots of a univariate polynomial in $\mathbb{Z}/\langle p^k \rangle$.

Definition 4 (representative roots). A set

$$\boldsymbol{a} = a_0 + pa_1 + \cdots + p^{l-1}a_{l-1} + p^l *$$

is called a *representative root* of $f(x)$ modulo p^k if each $\alpha \in \boldsymbol{a}$ is a root of $f(x) \bmod p^k$, but, not all $\beta \in \boldsymbol{b} := a_0 + pa_1 + \cdots + p^{l-2}a_{l-2} + p^{l-1}*$ are roots of $f(x) \bmod p^k$.

It was first observed in [4] that there are at most $\deg(f)$-many representative roots and they gave an efficient randomized algorithm to compute all these representative roots (for a simple exposition of the algorithm, see [25, Section B]).

We need a deterministic algorithm for our purpose (in Section 3.4) to count, if not find, the representative roots (as well as count the roots in each representative root). So we use the deterministic polynomial time algorithm of [24] which returns all these representative roots implicitly in the form of a data-structure they call *maximal split ideals* (MSI). The two explicit parameters, *length* and *degree* of an MSI immediately gives the count on the number of representative roots (as well as roots) encoded by them, which suffices for our purpose. A similar idea to use triangular ideals for encoding roots first appeared in [12], to count roots deterministically, but for "small" k.

We now define MSI from [24, Section 2].

Definition 5 ([24, Section 2], maximal split ideals). A triangular ideal

$$I = \langle h_0(x_0), \ldots, h_l(x_0, \ldots, x_l) \rangle,$$

where $0 \le l \le k-1$ and each $h_i(x_0, \ldots, x_i) \in \mathbb{F}_p[x_0, \ldots, x_i]$, is called a *maximal split ideal* of $f(x) \bmod p^k$ if

(1) the number of common zeros of $h_0, \ldots, h_l$ in ${\mathbb{F}_p}^{l+1}$ is $\prod_{i=0}^{l} \deg_{x_i}(h_i)$, where $\deg_{x_i}$ denotes the individual degree wrt x_i, and

(2) for every common zero $(a_0, \ldots, a_l) \in {\mathbb{F}_p}^{l+1}$ of $h_0, \ldots, h_l$, $f(x)$ vanishes identically modulo p^k with the substitution $x \to a_0 + pa_1 + \cdots + p^l a_l + p^{l+1}x$ but not with $x \to a_0 + \cdots + p^{l-1}a_{l-1} + p^l x$.

For an MSI I given by its generators $h_0(x_0), \ldots, h_l(x_0, \ldots, x_l)$ we define its *length* to be $l+1$ and *degree*, denoted as $\deg(I)$, to be the number of common zeros of its generators, which is $\prod_{i=0}^{l} \deg_{x_i}(h_i)$ by definition.

Essentially, I is encoding some representative roots of $f \bmod p^k$ in the form of common roots of its generators. Indeed, condition (2) of the definition is similar to that of representative roots. If $(a_0, \ldots, a_l)$ is a common zero of the generators then by condition (2), $a_0 + pa_1 + \cdots + p^l a_l + p^{l+1}*$ follows all the conditions to be a representative root. Then, it is apparent that:

Lemma 6 ([24, Lemmas 6 and 8]). *The length of an MSI I is the length of each representative root encoded by it and the degree of I is the count on these representative roots. Thus, we get the count on the roots of $f \bmod p^k$ encoded by I as $\prod_{i=0}^{l} \deg_{x_i}(h_i) \times p^{k-l-1}$.*

We state the result of [24] which returns all the representative roots, in MSI form, in deterministic polynomial time.

Theorem 7 (compute $N_k(f)$ [24]). *In deterministic poly($|f|, k\log p$)-time one gets the maximal split ideals which collectively contain exactly the representative roots of a univariate polynomial $f(x) \in \mathbb{Z}[x]$ modulo prime power p^k.*

Using Lemma 6 we can count them, and all roots of $f \bmod p^k$, in deterministic polynomial time.

2.2. ***Some definitions and notation related to f.*** We are given an integral univariate polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree d with coefficients of magnitude at most $C \in \mathbb{N}$, and a prime p. Then, f can also be thought of as an element of $\mathbb{Z}_p[x]$ (as $\mathbb{Z} \subseteq \mathbb{Z}_p$), where $\mathbb{Z}_p$ is the *ring of integers of p-adic rational numbers* $\mathbb{Q}_p$. In such a field $\mathbb{Q}_p$ (called a nonarchimedean *local* field) there exists a valuation function $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$. Formally, the *valuation* $v_p(a)$ of $a \in \mathbb{Z}_p$ ($\mathbb{Z}_p$ is a UFD) is defined to be the highest power of p dividing a, when $a \neq 0$, and ∞ when $a = 0$. This definition extends to the rationals $\mathbb{Q}_p$ naturally as $v_p(a/b) := v_p(a) - v_p(b)$, where $b \neq 0$ and $a, b \in \mathbb{Z}_p$ (see [41]).

Now we define the factors of f in $\mathbb{Z}_p[x]$ as follows (note: we do not require f to be monic).

Definition 8. Let the p-adic integral factorization of f into coprime irreducible factors be

$$f(x) \;=:\; \prod_{i\in[n]} (x-\alpha_i)^{e_i} \cdot \prod_{j=1}^{m} g_j(x)^{t_j},$$

where each α_i is a $\mathbb{Z}_p$-root of f with *multiplicity* e_i. Each $g_j(x) \in \mathbb{Z}_p[x]$ has multiplicity t_j; it is irreducible over $\mathbb{Z}_p$ and has no $\mathbb{Z}_p$-root.

For example, over $\mathbb{Z}_2$, $f = 2x^2 + 3x + 1 = (x+1)\cdot(2x+1)$ has $n = m = 1$.

Definition 9. For each $i \in [n]$, we define $f_i(x) \in \mathbb{Z}_p[x]$, called the *$\alpha_i$-free part of f*, as $f_i(x) := f(x)/(x-\alpha_i)^{e_i}$. We denote the *valuation* $v_p(f_i(\alpha_i))$ as ν_i, for all $i \in [n]$.

The *radical* of a univariate polynomial $h(x)$ over a field $\mathbb{F}$ is defined to be the univariate polynomial, denoted by $\mathrm{rad}(h)$, which is the product of coprime irreducible factors of h. This gives rise to the following definition.

Definition 10. Define $\mathrm{rad}(f) := \left(\prod_{i=1}^{n}(x-\alpha_i)\right)\cdot\left(\prod_{j=1}^{m} g_j(x)\right)$. Analogously, the radical of f_i, for each $i \in [n]$, is defined as $\mathrm{rad}(f_i) := \mathrm{rad}(f)/(x-\alpha_i)$.

The *discriminant* of a polynomial $h(x) \in \mathbb{F}[x]$ is defined as $D(h) := h_m^{2m-1}\cdot\prod_{1\le i<j\le m}(r_i - r_j)^2$, where $\mathbb{F}$ is a field, the r_i's are the roots of $h(x)$ over the algebraic closure $\overline{\mathbb{F}}$, the degree of h is m, and h_m is its leading coefficient.

The discriminant $D(h)$ is an element of $\mathbb{F}$. It is clear by the definition that all the roots of h are distinct if and only if $D(h) \neq 0$; i.e., the discriminant of the radical is nonzero.

Definition 11. We denote by Δ the valuation with respect to p of the discriminant of the radical of f, i.e, $\Delta := v_p(D(\mathrm{rad}(f)))$.

We see that Δ must be finite, since roots of $\mathrm{rad}(f)$ are distinct. The following fact is easily established by the definition of discriminant and the fact that $\alpha_1, \ldots, \alpha_n$ are also roots of $\mathrm{rad}(f)$.

Fact 12. For $i \neq j \in [n]$, we have $v_p(\alpha_i - \alpha_j) \leq \Delta/2 < \infty$.

For our algorithm, Δ will be crucial in informing us about the behavior of the roots of $f \bmod p^k$.

Properties of discriminants.

(1) Over $\mathbb{Z}_p$, if $u(x) \mid w(x)$ then $D(u) \mid D(w)$ and $v_p(D(u)) \leq v_p(D(w))$.

(2) The discriminant of a linear polynomial is defined to be 1.

(3) If $w(x) = (x - a) \cdot u(x)$ then by the definition of discriminant, it is clear that $D(w) = D(u) \cdot u(a)^2$.

(4) The discriminant $D(h)$ of a degree-l univariate polynomial $h(x) := h_l x^l + \cdots + h_1 x + h_0$, over $\mathbb{Z}_p$, is also a multivariate polynomial over $\mathbb{Z}_p$ in the coefficients $h_0, \ldots, h_l$ (see [46, Chapter 1]). Moreover, it is computable in time polynomial in the size of a given h (e.g., using the determinant of a Sylvester matrix [69, Chapter 11, Section 2]).

3. Proof of main results

3.1. ***Interplay of $\mathbb{Z}_p$-roots and $(\mathbb{Z}/\langle p^k\rangle)$-roots.*** In this section we will establish a connection between $(\mathbb{Z}/\langle p^k\rangle)$-roots and $\mathbb{Z}_p$-roots of the given f, when k is sufficiently large, i.e, $k > d\Delta$ (see Section 2.2 for the related notation).

Recall that $\alpha_1, \ldots, \alpha_n$ are the distinct $\mathbb{Z}_p$-roots of f (Definition 8). The following claim establishes a notion of "closeness" of any $\overline{\alpha} \in \mathbb{Z}_p$ to an α_j. Later we will apply this to a representative root $\overline{\alpha}$.

Claim 13 (close to a root). For some $j \in [n]$, $\overline{\alpha} \in \mathbb{Z}_p$, if $v_p(\overline{\alpha} - \alpha_j) > \Delta/2$, then $v_p(\overline{\alpha} - \alpha_i) = v_p(\alpha_j - \alpha_i) \leq \Delta/2$, for all $i \neq j$, $i \in [n]$.

Proof. The valuation $v_p(\overline{\alpha} - \alpha_i)$ is equal to $v_p(\overline{\alpha} - \alpha_j + \alpha_j - \alpha_i)$. Since $v_p(\overline{\alpha} - \alpha_j) > \Delta/2$ and $v_p(\alpha_j - \alpha_i) \leq \Delta/2$ (by Fact 12), we deduce $v_p(\overline{\alpha} - \alpha_i) = \min\{v_p(\overline{\alpha} - \alpha_j), v_p(\alpha_j - \alpha_i)\} = v_p(\alpha_j - \alpha_i) \leq \Delta/2$. □

The following lemma says that an irreducible cannot take values with ever-increasing valuation.

Lemma 14 (valuation of an irreducible). *Let $h(x) \in \mathbb{Z}_p[x]$ be a polynomial with no $\mathbb{Z}_p$-root, and discriminant $D(h) \neq 0$. Then, for any $\overline{\alpha} \in \mathbb{Z}_p$, $v_p(h(\overline{\alpha})) \leq v_p(D(h))$.*

Proof. We give the proof by contradiction, i.e, we show that if $v_p(h(\overline{\alpha})) > v_p(D(h))$, then $h(x)$ has a root in $\mathbb{Z}_p$.

Define $v_p(D(h)) =: d(h)$. Let $\overline{\alpha} \in \mathbb{Z}_p$ such that $h(\overline{\alpha}) \equiv 0 \bmod p^\delta$, for $\delta > d(h)$. Then we write $h(x) = (x - \overline{\alpha}) \cdot h_1(x) + p^\delta \cdot h_2(x)$. The two things to note here are:

(1). $D(h) \equiv D(h \bmod p^\delta) \bmod p^\delta$ by discriminants' property (4) in Section 2.2. Also, $D(h) \neq 0$ is given.

(2). Let $h'(x)$ be the first derivative of $h(x)$ and let $i := v_p(h'(\overline{\alpha}))$. Then, we claim that $\delta > d(h) \geq 2i$.

Consider $h'(x) = h_1(x) + (x - \overline{\alpha})h_1'(x) + p^\delta h'_2(x)$. So, $h'(\overline{\alpha}) \equiv h_1(\overline{\alpha}) \bmod p^\delta$. By property (3) (Section 2.2) of discriminants, $D(h) \equiv D((x - \overline{\alpha}) \cdot h_1(x)) \equiv D(h_1) \cdot h_1(\overline{\alpha})^2 \equiv D(h_1) \cdot h'(\overline{\alpha})^2 \bmod p^\delta$. Then, since $D(h) \neq 0 \bmod p^\delta$, we deduce $2i \leq d(h) < \delta$.

Now, we show that the root $\overline{\alpha}$ of $h \bmod p^{\delta}$ *lifts* to roots of $h \bmod p^{\delta+j}$, for all $j \in \mathbb{Z}^{+}$. This is due to Hensel's lemma (see [69, Chapter 15]); for completeness we give the proof.

By Taylor expansion, we have $h(\overline{\alpha}+p^{\delta-i}x) = h(\overline{\alpha}) + h'(\overline{\alpha}) \cdot p^{\delta-i}x + h''(\overline{\alpha}) \cdot p^{2(\delta-i)}x^2/2! + \cdots$.

Note that there exists a unique solution $x_0 \equiv (-h(\overline{\alpha})/h'(\overline{\alpha})p^{\delta-i}) \bmod p$: $h(\overline{\alpha}+p^{\delta-i}x_0) \equiv 0 \bmod p^{\delta+1}$. This follows from the Taylor expansion and since $2(\delta-i) > \delta$.

So, $\overline{\alpha} - p^{\delta-i}(h(\overline{\alpha})/h'(\overline{\alpha})p^{\delta-i}) \bmod p^{\delta+1}$ is a lift, of $\overline{\alpha} \bmod p^{\delta}$. By similar reasoning, it can be lifted further to arbitrarily high powers $p^{\delta+j}$. This proves $h(x)$ has a $\mathbb{Z}_p$-root, which is a contradiction. □

The following lemma is perhaps the most important one. It associates every root $\overline{\alpha}$ of $f(x) \bmod p^k$ to a unique $\mathbb{Z}_p$-root of f. Recall the notation from Section 2.2.

Lemma 15 (unique association). *Let $k > d(\Delta+1)$ and $\overline{\alpha} \in \mathbb{Z}_p$ be a root of $f(x) \bmod p^k$. There exists a unique α_i such that $v_p(\overline{\alpha}-\alpha_i) > \Delta+1$ and thus, $v_p(\overline{\alpha}-\alpha_i) > v_p(\alpha_i-\alpha_j)$, for all $j \neq i$, $j \in [n]$.*

Proof. Let us first prove that there exists some $i \in [n]$, given $\overline{\alpha}$, such that $v_p(\overline{\alpha}-\alpha_i) > \Delta+1$. For the sake of contradiction, assume that $v_p(\overline{\alpha}-\alpha_i) \leq \Delta+1$ for all $i \in [n]$. Then, by Definition 8, $v_p(f(\overline{\alpha})) = \sum_{i=1}^{n} e_i \cdot v_p(\overline{\alpha}-\alpha_i) + \sum_{j=1}^{m} t_j \cdot v_p(g_j(\overline{\alpha})) \leq (\Delta+1) \cdot \sum_{i=1}^{n} e_i + \sum_{j=1}^{m} t_j \cdot v_p(g_j(\overline{\alpha}))$.

Since g_j has no $\mathbb{Z}_p$-root, for all $j \in [m]$, by Lemma 14, $v_p(g_j(\overline{\alpha})) \leq v_p(D(g_j))$. By the properties given in Section 2.2 we get $v_p(D(g_j)) \leq v_p(D(\mathrm{rad}(f))) = \Delta$, proving that $v_p(g_j(\overline{\alpha})) \leq \Delta$.

Going back, $v_p(f(\overline{\alpha})) \leq (\Delta+1) \cdot \left(\sum_{i=1}^{n} e_i + \sum_{j=1}^{m} t_j\right) \leq d(\Delta+1) < k$. It implies that $f(\overline{\alpha}) \not\equiv 0 \bmod p^k$, which contradicts the hypothesis that $\overline{\alpha}$ is a root of $f \bmod p^k$.

Thus, there exists $i \in [n]$ such that $v_p(\overline{\alpha}-\alpha_i) > \Delta+1$. The uniqueness of i follows from Claim 13. □

Having seen that every root $\overline{\alpha}$ of $f \bmod p^k$ is associated (or close) to a unique $\mathbb{Z}_p$-root α_i, the following lemma tells us that the valuation of the α_i-free part of f (resp. factors of f with no $\mathbb{Z}_p$-root) is the same on any $\overline{\alpha}$ close to α_i. This unique valuation is important in getting an expression for $N_k(f)$.

Lemma 16 (unique valuation). *Fix $i \in [n]$. Fix $\overline{\alpha} \in \mathbb{Z}_p$ such that $v_p(\overline{\alpha}-\alpha_i) > \Delta$. Recall $g_j(x)$, f_i from Section 2.2. Then,*

(1) $v_p(g_j(\overline{\alpha})) = v_p(g_j(\alpha_i))$, *for all* $j \in [m]$,

(2) $v_p(f_i(\overline{\alpha})) = v_p(f_i(\alpha_i))$.

In other words, the valuation with respect to p of $f_i = f(x)/(x-\alpha_i)^{e_i}$, on $x \mapsto \overline{\alpha}$, is fixed uniquely to $v_i := v_p(f_i(\alpha_i))$, for any "close" approximation $\overline{\alpha} \in \mathbb{Z}_p$ of α_i.

Proof. Since $g_j \mid \mathrm{rad}(f_i)$ and $\mathrm{rad}(f_i) \mid \mathrm{rad}(f)$, we have by the properties of discriminants (Section 2.2) that $v_p(g_j(\alpha_i)) \leq v_p(\mathrm{rad}(f_i)(\alpha_i)) \leq \Delta$, for all $j \in [m]$.

Since $v_p(\overline{\alpha}-\alpha_i) > \Delta$, we deduce $v_p(g_j(\overline{\alpha}) - g_j(\alpha_i)) > \Delta$. Furthermore, $v_p(g_j(\alpha_i)) \leq \Delta$ implies $v_p(g_j(\overline{\alpha})) = v_p(g_j(\alpha_i))$. This proves the first part.

By Claim 13, $v_p(\overline{\alpha}-\alpha_u) = v_p(\alpha_i-\alpha_u)$, for all $u \neq i$, $u \in [n]$. Also, by the first part, $v_p(g_w(\overline{\alpha})) = v_p(g_w(\alpha_i))$, for all $w \in [m]$. Consequently, $v_p(f_i(\overline{\alpha})) = \sum_{u=1, u\neq i}^{n} e_u \cdot v_p(\alpha_i-\alpha_u) + \sum_{w=1}^{m} t_w \cdot v_p(g_w(\alpha_i)) = v_p(f_i(\alpha_i))$. This proves the second part. □

3.2. ***Representative roots versus neighborhoods.*** We now connect the $\mathbb{Z}_p$-roots of f to the representative roots (defined in Section 2.1) of $f \bmod p^k$. Later we characterize each representative root as a "neighborhood" in Theorem 19.

Lemma 17 (perturb a root). *Let $k > d(\Delta+1)$ and let $\overline{\alpha}$ be a root of $f(x) \bmod p^k$ with $l := v_p(\alpha_i - \overline{\alpha}) > \Delta+1$, for some $i \in [n]$ (as in Lemma 15). Then, every $\overline{\beta} \in \overline{\alpha} + p^l *$ is also a root of $f(x) \bmod p^k$.*

Proof. Since $f(\overline{\alpha}) \equiv 0 \bmod p^k$, we have $v_p(f(\overline{\alpha})) \geq k$. Using Lemma 16 we have $v_p(f_i(\overline{\alpha})) = v_p(f_i(\alpha_i)) = \nu_i$. Thus, $v_p(f(\overline{\alpha})) = v_p(\alpha_i - \overline{\alpha}) \cdot e_i + v_p(f_i(\overline{\alpha})) = v_p(\alpha_i - \overline{\alpha}) \cdot e_i + \nu_i \geq k$.

Similarly, $v_p(f(\overline{\beta})) = v_p(\alpha_i - \overline{\beta}) \cdot e_i + v_p(f_i(\overline{\beta})) = v_p(\alpha_i - \overline{\beta}) \cdot e_i + \nu_i \geq v_p(\alpha_i - \overline{\alpha}) \cdot e_i + \nu_i$. The last inequality follows from $v_p(\alpha_i - \overline{\beta}) \geq l = v_p(\alpha_i - \overline{\alpha})$.

From the above two paragraphs we get $v_p(f(\overline{\beta})) \geq k$. Hence, $f(\overline{\beta}) \equiv 0 \bmod p^k$. □

Now we define a notion of "neighborhood" of a $\mathbb{Z}_p$-root of f.

Definition 18 (neighborhood). For $i \in [n]$, $k > d(\Delta+1)$, we define the *neighborhood $S_{k,i}$* of $\alpha_i \bmod p^k$ to be the set of all those roots of $f \bmod p^k$ which are close to the $\mathbb{Z}_p$-root α_i of f. Formally,

$$S_{k,i} := \{\overline{\alpha} \in \mathbb{Z}/\langle p^k \rangle \mid v_p(\overline{\alpha} - \alpha_i) > \Delta+1,\ f(\overline{\alpha}) \equiv 0 \bmod p^k\}.$$

The notion of representative root was first given in [25]. Below we discover its new properties which will lead us to an understanding of *length* of a representative root, which in turn will give us the size of a neighborhood contributing to $N_k(f)$.

Theorem 19 (representative root is a neighborhood). *Let $k > d(\Delta+1)$ and let*

$$\boldsymbol{a} := a_0 + pa_1 + p^2 a_2 + \cdots + p^{l-1} a_{l-1} + p^l *$$

be a representative root of $f(x) \bmod p^k$. Define the $\mathbb{Z}_p$-root reduction $\overline{\alpha}_i := \alpha_i \bmod p^k$, for all $i \in [n]$. Fix an $i \in [n]$, then:

(1) *The length of $\boldsymbol{a}$ is* large. *Formally, $l > \Delta+1$.*

(2) *If $\overline{\alpha}_i \in \boldsymbol{a}$, then $\overline{\alpha}_j \notin \boldsymbol{a}$ for all $j \neq i$, $j \in [n]$. (This means, using Lemma 15, $\boldsymbol{a}$ has a uniquely associated $\mathbb{Z}_p$-root.)*

(3) *If $\boldsymbol{a}$ contains $\overline{\alpha}_i$ then it also contains the respective* neighborhood. *In fact, if $\overline{\alpha}_i \in \boldsymbol{a}$, then $S_{k,i} = \boldsymbol{a}$.*

Proof. (1) Consider $\overline{\alpha} := a_0 + pa_1 + \cdots + p^{l-1} a_{l-1}$. By Lemma 15, there exists a unique $s \in [n]$ such that $v_p(\overline{\alpha} - \alpha_s) > \Delta+1$. Suppose $l \leq \Delta+1$. Then, $v_p(\overline{\alpha} + p^{\Delta+1} - \alpha_s) = \Delta+1$. As, $\overline{\alpha}' := (\overline{\alpha} + p^{\Delta+1})$ is also in $\boldsymbol{a}$, it again has to be close to a unique α_t, with $s \neq t \in [n]$ such that $v_p(\overline{\alpha}' - \alpha_t) > \Delta+1$. In other words, $\alpha_s + p^{\Delta+1} \equiv \overline{\alpha} + p^{\Delta+1} \equiv \alpha_t \bmod p^{\Delta+2}$. Thus, $v_p(\alpha_s - \alpha_t) = \Delta+1 > \Delta/2$, contradicting Fact 12. This proves $l > \Delta+1$.

(2) Consider distinct $\overline{\alpha}_i, \overline{\alpha}_j \in \boldsymbol{a}$. Then, by the definition of $\boldsymbol{a}$, we have $v_p(\overline{\alpha}_i - \overline{\alpha}_j) \geq l > \Delta+1 > \Delta/2$, contradicting Fact 12. Thus, there is a unique i.

(3) Suppose there exists a neighborhood element $\overline{\beta} \notin \boldsymbol{a}$, satisfying the conditions $v_p(\alpha_i - \overline{\beta}) > \Delta + 1$ and $f(\overline{\beta}) \equiv 0 \bmod p^k$. Let j be the index of the first coordinate where $\overline{\beta}$ and $\boldsymbol{a}$ differ; so, $j < l$ since $\overline{\beta} \notin \boldsymbol{a}$. Clearly, $j > \Delta + 1$; otherwise, since $\overline{\alpha}_i \in \boldsymbol{a}$ and $\overline{\beta} \notin \boldsymbol{a}$, we deduce $v_p(\alpha_i - \overline{\beta}) = j \leq \Delta + 1$, which is a contradiction.

By $v_p(\alpha_i - \overline{\beta}) = j > \Delta + 1$ and Lemma 17, we get that every element in $\overline{\beta} + p^j *$ is a root of $f(x) \bmod p^k$, and consequently each element in $a_0 + pa_1 + p^2 a_2 + \cdots + p^{j-1} a_{j-1} + p^j *$ is a root of $f(x) \bmod p^k$, which contradicts that $\boldsymbol{a}$ is a representative root (because $j < l$; see Definition 4). Thus, $\overline{\beta} \in \boldsymbol{a}$, implying $S_{k,i} \subseteq \boldsymbol{a}$.

Conversely, consider $\overline{\alpha} \in \boldsymbol{a}$. Then, as before, $v_p(\overline{\alpha}_i - \overline{\alpha}) \geq l > \Delta + 1$, implying $\overline{\alpha} \in S_{k,i}$. So, $S_{k,i} \supseteq \boldsymbol{a}$. □

Next, we get the expression for the length of a representative root.

Theorem 20. *For $k > d(\Delta + 1)$, the representative roots of $f(x) \bmod p^k$ are in a one-to-one correspondence with $\mathbb{Z}_p$-roots of f. Moreover, the length of the representative root $\boldsymbol{a}$, corresponding to α_i, is $l_{i,k} := \lceil (k - \nu_i)/e_i \rceil$.*

Proof. By Proposition 3, every root of $f \bmod p^k$ is in exactly one of the representative roots. So each reduced $\mathbb{Z}_p$-root $\overline{\alpha}_i := \alpha_i \bmod p^k$ is in a unique representative root. Thus, by parts (2) and (3) of Theorem 19, we get the one-to-one correspondence as claimed.

Consider a p-adic integer $\overline{\alpha}$ with $v_p(\overline{\alpha} - \alpha_i) =: l_{\overline{\alpha}} > \Delta$. We have the following equivalences:

$$\begin{aligned} \overline{\alpha} \in \boldsymbol{a} &\iff v_p(f(\overline{\alpha})) \geq k \iff v_p((\overline{\alpha} - \alpha_i)^{e_i} \cdot f_i(\overline{\alpha})) \geq k \iff e_i l_{\overline{\alpha}} + \nu_i \geq k \quad \text{(by Lemma 16)} \\ &\iff l_{\overline{\alpha}} \geq \lceil (k - \nu_i)/e_i \rceil = l_{i,k}. \end{aligned}$$

Write the representative root corresponding to α_i as $\boldsymbol{a} =: a_0 + pa_1 + p^2 a_2 + \cdots + p^{l-1} a_{l-1} + p^l *$. Clearly, $l = \min\{l_{\overline{\alpha}} \mid \overline{\alpha} \in \boldsymbol{a}\} \geq l_{i,k}$. Note that if $l > l_{i,k}$ then by the equivalences we could reduce the length l of the representative root $\boldsymbol{a}$, which is a contradiction. Thus, $l = l_{i,k}$. □

3.3. ***Formula for $N_k(f)$ — Proof of Corollary 2.*** For large enough k, the previous section gives us an easy way to count the roots. In fact, we have the following simple formula for $N_k(f)$.

Theorem 21 (roots mod p^k). *For $k > d(\Delta + 1)$, $N_k(f) = \sum_{i \in [n]} p^{k - \lceil (k - \nu_i)/e_i \rceil}$, where clearly ν_i, e_i and n (as in Section 2.2) are independent of k.*

Proof. Fix $i \in [n]$ and $k > d(\Delta + 1)$. By Theorem 20 we get that in the unique representative root $\boldsymbol{a}$, corresponding to $\alpha_i \bmod p^k$, the $(k - \lceil (k - \nu_i)/e_i \rceil)$-many higher-precision coordinates could be set arbitrarily from $[0, \ldots, p-1]$ (while the rest, the lower-precision ones, are fixed). That gives us the count via contribution for each $i \in [n]$. Moreover, the sum over neighborhoods, for each $i \in [n]$, gives us exactly $N_k(f)$.

Also, note that if $n = 0$ then the count $N_k(f)$ is equal to 0. □

Proof of Corollary 2. Theorem 21 gives a closed form expression for $N_k(f)$, when

$$k \geq k_0 := d(\Delta + 1) + 1 \leq d(2d - 1)(\log_p C + \log_p d) + 1.$$

For the other part, note the discriminant $D(f)$ is not equal to 0 if and only if f is squarefree. In the squarefree case $e_i = 1$, for all $i \in [n]$. By Theorem 21, $N_k(f) = \sum_{i \in [n]} p^{\nu_i}$, which is independent of k. $\square$

3.4. ***Computing Poincaré series — Proof of Theorem 1.*** Building upon the ideas of the previous sections, we will show how to deterministically compute Poincaré series $P(t) = \sum_{k=0}^{\infty} N_k(f)(p^{-1}t)^k$ associated to the input $f(x)$ efficiently, thereby proving Theorem 1. Before that, we need some notation:

Set $k_0 := d(\Delta + 1) + 1$ so we know by Theorem 21 that for $k \geq k_0$, $N_k(f) = \sum_{i=1}^{n} N_{k,i}(f)$, where $N_{k,i}(f) := p^{k - \lceil (k - \nu_i)/e_i \rceil}$. For each $i \in [n]$, define k_i to be the least integer such that $k_i \geq k_0$ and $(k_i - \nu_i)/e_i$ is an integer. Then, Poincaré series $P(t)$ can be partitioned into finite and infinite sums as

$$P(t) = P_0(t) + \sum_{i=1}^{n} P_i(t),$$

where

$$P_i(t) := \sum_{k=k_i}^{\infty} N_{k,i}(f) \cdot (p^{-1}t)^k \quad \text{and} \quad P_0(t) := \left(\sum_{k=0}^{k_0 - 1} N_k(f) \cdot (p^{-1}t)^k \right) + \sum_{i=1}^{n} \sum_{k=k_0}^{k_i - 1} N_{k,i}(f) \cdot (p^{-1}t)^k.$$

We now compute the multiplicity e_i by viewing it as the *step* that increments the length of the representative root associated to α_i as k keeps growing above k_0.

Lemma 22 (compute e_i). *We can compute the number of $\mathbb{Z}_p$-roots n of f as well as k_i, ν_i and e_i, for each $i \in [n]$, in deterministic poly$(d, \log C + \log p)$-time.*

Proof. By Theorem 7, we get all representative roots of $f \bmod p^k$ implicitly in the form of maximal split ideals (for brevity, we call these split ideals). By Lemma 6, the length of a split ideal is also the length of all representative roots represented by it and the degree is the number of representative roots represented by it. Since, by Theorem 20, n is also the number of representative roots of $f \bmod p^k$ for $k \geq k_0$, we run the algorithm of Theorem 7 for $k = k_0$ and sum up the degree of all split ideals obtained, to get n.

Suppose the split ideal I we find contains a representative root $\boldsymbol{a}$ of $f \bmod p^k$ corresponding to α_i, with k_i as defined before. How do we compute k_i? By Theorem 20, the length of $\boldsymbol{a}$, when $k = k_i$, is $l_{i,k_i} = (k_i - \nu_i)/e_i$. Now, for all $k = k_i + 1, k_i + 2, \ldots, k_i + e_i$, the length $l_{i,k}$ remains equal to $l_{i,k_i} + 1$, while for the next $k = k_i + e_i + 1$, $l_{i,k}$ increments by one.

So we run the algorithm of Theorem 7 for several $k \geq k_0$. When we find the length incrementing by one, namely, at the two values $k = k_i + 1$ and $k = k_i' := k_i + 1 + e_i$, then we have found e_i (and k_i). From the equation, $k_i - \nu_i = e_i \cdot l_{i,k_i}$, we also find ν_i.

Suppose the split ideal I we find contains *two* representative roots $\boldsymbol{a}$ and $\boldsymbol{b}$ mod p^k, corresponding to $\mathbb{Z}_p$-roots α_i and α_j respectively, such that $e_i \neq e_j$ (without loss of generality, say, $e_i < e_j$). In this case, even if $\boldsymbol{a}$ and $\boldsymbol{b}$ have the same length, when $k = k_i$, they will evolve to different length representative roots when we go to a "higher-precision" arithmetic mod $p^{k_i + 1 + e_i}$ (by the formula in Theorem 20). So $\boldsymbol{a}, \boldsymbol{b}$ must lie in different length split ideals, say, I_a and I_b respectively.

Now, for another representative root $\boldsymbol{c}$ in I_a, say corresponding to α_s, we have $e_i = e_s$ and hence $\nu_i = \nu_s$. By computing e_i and ν_i as before, now using the length of I and I_a, we compute e_s and ν_s

(and k_s) for every $\boldsymbol{c}$ in I_a. Since, by Lemma 6, the degree of I_a is the number of such representative roots in I_a, we can compute n; moreover, we get k_i, ν_i, e_i for all $i \in [n]$.

Clearly, we need to run the algorithm of Theorem 7 at most $2\max_{i\in[n]}\{e_i\} = O(d)$ times, to study the evolution of split ideals (implicitly, that of the underlying representative roots). Also Δ is the logarithm (to base p) of the determinant of a Sylvester matrix which gives $\Delta = O(d \cdot (\log_p C + \log_p d))$. So, the algorithm runs in polynomial time as claimed. $\square$

Now we prove that the infinite sums $P_i(t)$ are formally equal to rational functions of $t = p^{-s}$.

Lemma 23 (infinite sums are rational). *For each $i \in [n]$, the series $P_i(t)$ is a rational function of t as*

$$P_i(t) = \frac{t^{k_i} \cdot (p - t(p-1) - t^{e_i})}{p^{(k_i-\nu_i)/e_i} \cdot (1-t) \cdot (p - t^{e_i})}.$$

Proof. Recall that $P_i(t) = \sum_{k=k_i}^{\infty} N_{k,i}(f) \cdot (p^{-1}t)^k$. For simplicity write $T := p^{-1}t$ and define an integer $\delta_i := k_i - (k_i - \nu_i)/e_i$. Now P_i can be rewritten using residues mod e_i as

$$P_i(t) = \sum_{l=k_i}^{k_i+e_i-1} \sum_{k=0}^{\infty} N_{l+ke_i,i}(f) \cdot T^{l+ke_i}.$$

For simplicity take $l = k_i$ and consider the sum, $\sum_{k=0}^{\infty} N_{k_i+ke_i,i}(f) \cdot T^{k_i+ke_i}$. We find that $N_{k_i,i}(f) = p^{\delta_i}$, $N_{k_i+e_i,i}(f) = p^{\delta_i+e_i-1}$, $N_{k_i+2e_i,i}(f) = p^{\delta_i+2(e_i-1)}$, and so on. Hence, $\sum_{k=0}^{\infty} N_{k_i+ke_i,i}(f) \cdot T^{k_i+ke_i} = p^{\delta_i}T^{k_i} \cdot [1 + p^{e_i-1}T^{e_i} + (p^{e_i-1}T^{e_i})^2 + \cdots] = p^{\delta_i} \cdot T^{k_i}/(1 - p^{e_i-1}T^{e_i})$. So

$$\begin{aligned} P_i(t) &= \frac{p^{\delta_i}T^{k_i}}{1-p^{e_i-1}T^{e_i}} + \frac{p^{\delta_i}T^{k_i+1}}{1-p^{e_i-1}T^{e_i}} + \frac{p^{\delta_i+1}T^{k_i+2}}{1-p^{e_i-1}T^{e_i}} + \cdots + \frac{p^{\delta_i+e_i-2}T^{k_i+e_i-1}}{1-p^{e_i-1}T^{e_i}} \\ &= \frac{p^{\delta_i}T^{k_i}}{1-p^{e_i-1}T^{e_i}} + \frac{p^{\delta_i}T^{k_i+1}}{1-p^{e_i-1}T^{e_i}} \cdot (1 + pT + (pT)^2 + \cdots + (pT)^{e_i-2}) \\ &= \frac{p^{\delta_i}T^{k_i}}{1-p^{e_i-1}T^{e_i}} \cdot \left(1 + T \cdot \frac{1-(pT)^{e_i-1}}{1-pT}\right). \end{aligned}$$

Putting $T = t/p$ and $\delta_i = k_i - (k_i - \nu_i)/e_i$ we get

$$P_i(t) = \frac{t^{k_i}(p - t(p-1) - t^{e_i})}{p^{(k_i-\nu_i)/e_i}(1-t)(p-t^{e_i})}. \qquad \square$$

Now we are in a position to prove our main theorem.

Proof of Theorem 1. Recall $P(t) = P_0(t) + \sum_{i=1}^{n} P_i(t)$. We first compute $P_0(t)$, which is the sum of two polynomials in t, namely,

$$Q_1(t) := \sum_{j=0}^{k_0-1} N_j(f)(p^{-1}t)^j \quad \text{and} \quad Q_2(t) = \sum_{i=1}^{n}\sum_{l=k_0}^{k_i-1} N_{l,i}(f)(p^{-1}t)^l,$$

both of degree $O(d\Delta)$. By a standard determinant or Sylvester matrix calculation one shows $d\Delta \leq O(d^2 \cdot (\log_p C + \log_p d))$.

We can compute the polynomial $Q_1(t)$ in deterministic poly(d, $\log C + \log p$)-time by calling the root-counting algorithm of [24] (Theorem 7) $k_0 - 1$ times, getting each $N_j(f)$, for $j = 1, \dots, k_0 - 1$ (note: $N_0(f) := 1$).

Polynomial $Q_2(t)$ is a sum of $n \le d$ polynomials, each with $k_i - k_0 \le d$ many simple terms. Using Lemma 22, we can compute each ν_i, e_i, hence, $N_{l,i}(f)$. So, computation of Q_2 again takes time poly(d, $\log C + \log p$).

Lemma 23 gives us the rational form expression for $P_i(t)$, for each $i \in [n]$. So, using Lemma 22 we can compute the Poincaré series

$$P(t) = P_0(t) + \sum_{i=1}^{n} \frac{t^{k_i}(p - t(p-1) - t^{e_i})}{p^{(k_i - \nu_i)/e_i}(1-t)(p - t^{e_i})}$$

in deterministic poly(d, $\log C + \log p$)-time.

By inspecting the above expression, the degree of the denominator $B(t)$ is $1 + \sum_{i=1}^{n} e_i = O(d)$. The degree of the numerator $A(t)$ is $\le k_0 + 2d \le O(d^2 \cdot (\log_p C + \log_p d))$. $\square$

4. Conclusion and open questions

We presented the first complete solution to the problem of computing Igusa's local zeta function for any given integral univariate polynomial and a prime p. Indeed, our methods work for given $f \in \mathbb{Z}_p[x]$ (with f having computable representation) as our proof for integral f goes via considering its factorization over $\mathbb{Z}_p$ (Section 2.2).

We also found an explicit closed-form expression for $N_k(f)$ and efficiently computed the explicit parameters involved therein, which could be used to compute Greenberg's constants associated with a univariate f and a prime p. Greenberg's constants appear in a classical theorem of Greenberg [29, Theorem 1] which is a generalization of Hensel's lemma to several n-variate polynomials. We hope that our methods for the one variable case could be generalized to compute Greenberg's constants for the n variable case to give an effective version of Greenberg's theorem.

We also hope that our methods extend computing Igusa's local zeta function from characteristic zero ($\mathbb{Z}_p$) to positive characteristic ($\mathbb{F}_p[[T]]$) at least if some standard restrictions are imposed on the characteristic, for example, p is "large enough". This is supported by the fact that the root counting algorithm of [24] also extends to $\mathbb{F}[[T]]$ for a field $\mathbb{F}$.

The following important open questions need to be addressed:

(1) A natural question to study is whether we could generalize our method to compute Igusa's local zeta function for n-variate integral polynomials (say, $n = 2$?). Note that for growing n this problem is at least #P-hard [26].

(2) A related problem is of counting roots of n-variate polynomials mod prime power p^k. We know an efficient quantum algorithm mod p for $n = 2$ due to Kedlaya [37]. Kedlaya further asks, if we can reduce the problem of counting points mod p^k to counting points mod p for fixed k and $n = 2$. This question has affirmative answer known only for variable-separated curves due to Robelle et al. [55].

(3) Following up the problem of point counting on curves for constant k, we ask another important related open question — how to find a single point on curves mod p^k efficiently. It has an application in factoring a univariate $f(x)$ mod p^k [25]. Can we efficiently reduce finding a single point mod p^k to finding a single point mod p, even for fixed k and $n = 2$?

Acknowledgements

We thank anonymous reviewers for their helpful comments and pointing out relevant references to improve the draft of the paper. In particular we thank them for their suggestion which greatly improved the conclusion section and for pointing out a connection to Greenberg's work. We thank Kiran Kedlaya for pointing out some minor corrections and asking a relevant open question (Section 4, open question (2)) during the conference ANTS '20. Nitin Saxena thanks the funding support from DST (DST/SJF/MSA-01/2013-14) and N. Rama Rao Chair.

References

[1] V Albis and WA Zúñiga-Galindo, *An elementary introduction to the theory of Igusa local zeta functions*, Lect. Mat **20** (1999), no. 1, 5–33.

[2] Michael Anshel and Dorian Goldfeld, *Zeta functions, one-way functions, and pseudorandom number generators*, Duke Math. J. **88** (1997), no. 2, 371–390.

[3] Michael Anshel and Dorian Goldfeld, *Multi-purpose high speed cryptographically secure sequence generator based on zeta-one-way functions*, May 12 1998, US Patent 5,751,808.

[4] Jérémy 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** (2013), no. 6, 413–443, https://link.springer.com/article/10.1007/s00200-013-0200-5.

[5] Manjul Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, Journal für die Reine und Angewandte Mathematik **490** (1997), 101–128.

[6] Edward Bierstone, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Inventiones mathematicae **128** (1997), no. 2, 207–302.

[7] Edward Bierstone, Dima Grigoriev, Pierre Milman, and Jarosław Włodarczyk, *Effective Hironaka resolution and its complexity*, Asian Journal of Mathematics **15** (2011), no. 2, 193–228.

[8] Gábor Bodnár and Josef Schicho, *Automated resolution of singularities for hypersurfaces*, Journal of Symbolic Computation **30** (2000), no. 4, 401–428.

[9] Gábor Bodnár and Josef Schicho, *A computer program for the resolution of singularities*, Resolution of singularities, Springer, 2000, pp. 231–238.

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

[11] Edwin León Cardenal, *An algorithm for computing the local zeta function of an hyperelliptic curve*.

[12] Qi Cheng, Shuhong Gao, J Maurice Rojas, and Daqing Wan, *Counting roots of polynomials over prime power rings*, Thirteenth Algorithmic Number Theory Symposium, ANTS-XIII, Mathematical Sciences Publishers, 2018, arXiv:1711.01355.

[13] AL Chistov, *Efficient factorization of polynomials over local fields*, Dokl. Akad. Nauk SSSR **293** (1987), no. 5, 1073–1077.

[14] AL Chistov, *Algorithm of polynomial complexity for factoring polynomials over local fields*, Journal of mathematical sciences **70** (1994), no. 4, 1912–1933.

[15] M Chojnacka-Pniewska, *Sur les congruences aux racines données*, Annales Polonici Mathematici, vol. 3, Instytut Matematyczny Polskiej Akademii Nauk, 1956, pp. 9–12.

[16] J Brian Conrey, *The riemann hypothesis*, Notices of the AMS **50** (2003), no. 3, 341–353.

[17] Raemeon A Cowan, Daniel J Katz, and Lauren M White, *A new generating function for calculating the Igusa local zeta function*, Advances in Mathematics **304** (2017), 355–420.

[18] Bruce Dearden and Jerry Metzger, *Roots of polynomials modulo prime powers*, European Journal of Combinatorics **18** (1997), no. 6, 601–606.

[19] Pierre Deligne, *La conjecture de Weil. I*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **43** (1974), no. 1, 273–307.

[20] Jan Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Inventiones mathematicae **77** (1984), no. 1, 1–23.

[21] Jan Denef et al., *Local zeta functions and Euler characteristics*, Duke Mathematical Journal **63** (1991), no. 3, 713–721.

[22] Jan Denef and Kathleen Hoornaert, *Newton polyhedra and Igusa's local zeta function*, Journal of number Theory **89** (2001), no. 1, 31–64.

[23] Marcus PF du Sautoy and Fritz Grunewald, *Analytic properties of zeta functions and subgroup growth*, Ann. of Math.(2) **152** (2000), no. 3, 793–833.

[24] Ashish Dwivedi, Rajat Mittal, and Nitin Saxena, *Counting basic-irreducible factors mod p^k in deterministic poly-time and p-adic applications*, Computational Complexity Conference (2019), https://www.cse.iitk.ac.in/users/nitin/papers/basic-irred-mod-pk.pdf.

[25] Ashish Dwivedi, Rajat Mittal, and Nitin Saxena, *Efficiently factoring polynomials modulo p^4*, The 44th International Symposium on Symbolic and Algebraic Computation (ISSAC) (2019), https://www.cse.iitk.ac.in/users/nitin/papers/factor-mod-p4.pdf.

[26] Andrzej Ehrenfeucht and Marek Karpinski, *The Computational Complexity of (XOR, AND)-Counting Problems*, International Computer Science Inst., 1990.

[27] Emilio Elizalde, *Applications of zeta function regularization in QFT*, Quantum Field Theory Under the Influence of External Conditions, Springer, 1996, pp. 122–130.

[28] Michael R Garey and David S Johnson, *Computers and intractability*, vol. 174, freeman San Francisco, 1979.

[29] Marvin J Greenberg, *Rational points in henselian discrete valuation rings*, Publications Mathématiques de l'IHÉS **31** (1966), 59–64.

[30] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki **9** (1964), 41–55.

[31] Stephen W Hawking, *Zeta function regularization of path integrals in curved spacetime*, Communications in Mathematical Physics **55** (1977), no. 2, 133–148.

[32] Denis Ibadula, *On the plane cubics over $\mathbb{Q}_p$ and the associated igusa zeta function*, Bull. Math. Soc. Sci. Math. Roumanie (NS) **49** (2005), no. 97, 3.

[33] Jun-ichi Igusa, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, American Mathematical Society, Providence, RI; International Press, Cambridge, MA.

[34] Jun-ichi Igusa, *Complex powers and asymptotic expansions. I. Functions of certain types.*, Journal für die reine und angewandte Mathematik **268** (1974), 110–130.

[35] Jun-ichi Igusa, *Complex powers and asymptotic expansions. II.*, Journal für die reine und angewandte Mathematik **278** (1975), 307–321.

[36] Jun-ichi Igusa and S Raghavan, *Lectures on forms of higher degree*, vol. 59, Springer Berlin-Heidelberg-New York, 1978.

[37] Kiran S Kedlaya, *Quantum computation of zeta functions of curves*, computational complexity **15** (2006), no. 1, 1–19.

[38] Adam Klivans, *Factoring polynomials modulo composites*, tech. report, Carnegie-Mellon Univ, Pittsburgh PA, Dept of CS, 1997.

[39] Benjamin Klopsch and Christopher Voll, *Igusa-type functions associated to finite formed spaces and their functional equations*, Transactions of the American Mathematical Society **361** (2009), no. 8, 4405–4436.

[40] Benjamin Klopsch and Christopher Voll, *Zeta functions of three-dimensional p-adic Lie algebras*, Mathematische Zeitschrift **263** (2009), no. 1, 195–210.

[41] Neal Koblitz, *P-adic numbers*, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer, 1977, pp. 1–20.

[42] Leann Kopp, Natalie Randall, Joseph Rojas, and Yuyu Zhu, *Randomized polynomial-time root counting in prime power rings*, Mathematics of Computation (2019).

[43] Alan GB Lauder, *Counting solutions to equations in many variables over finite fields*, Foundations of Computational Mathematics **4** (2004), no. 3, 221–267.

[44] Edwin León-Cardenal and WA Zúñiga-Galindo, *An introduction to the theory of local zeta functions from scratch*, Revista Integración **37** (2019), no. 1, 45–76.

[45] Xiangdong Li and M Anshel, *Application of zeta function to quantum cryptography*, Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, IEEE, 2005, pp. 430–431.

[46] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge university press, 1994.

[47] Shaowei Lin, *Ideal-theoretic strategies for asymptotic approximation of marginal likelihood integrals.*, Journal of Algebraic Statistics **8** (2017), no. 1.

[48] Benjamin D Marko, Jeffrey M Riedl, et al., *Igusa local zeta function of the polynomial* $f(x) = x_1^m + x_2^m + \cdots + x_m^m$, (2005).

[49] Davesh Maulik, *Root sets of polynomials modulo prime powers*, Journal of Combinatorial Theory, Series A **93** (2001), no. 1, 125–140.

[50] Diane Meuser, *A survey of Igusa's local zeta function*, American Journal of Mathematics **138** (2016), no. 1, 149–179.

[51] Joseph Polchinski, *String theory: Volume 1, an introduction to the bosonic string*, Cambridge university press, 1998.

[52] H Reichardt, *SI Borewicz und IR Safarevic, Zahlentheorie.(Mathematische Reihe, Band 32). 468 S. Basel/Stuttgart 1966. Birkhäuser Verlag. Preis geb. sFr. 56,-*, Zeitschrift Angewandte Mathematik und Mechanik **49** (1969), 187–187.

[53] Nicolai Reshetikhin and Boris Vertman, *Combinatorial quantum field theory and gluing formula for determinants*, Letters in Mathematical Physics **105** (2015), no. 3, 309–340.

[54] Bernhard Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grosse*, Ges. Math. Werke und Wissenschaft. Nachlaß **2** (1859), 145–155.

[55] Caleb Robelle, J Maurice Rojas, and Yuyu Zhu, *Sub-linear point counting for variable separated curves over prime power rings*, manuscript, https://www.math.tamu.edu/ rojas/curve.pdf.

[56] Margaret M Robinson, *The Igusa local zeta function associated with the singular cases of the determinant and the Pfaffian*, Journal of number theory **57** (1996), no. 2, 385–408.

[57] Barry Robson, *Clinical and pharmacogenomic data mining: 3. Zeta theory as a general tactic for clinical bioinformatics*, Journal of proteome research **4** (2005), no. 2, 445–455.

[58] M Saia and WA Zúñiga-Galindo, *Local zeta function for curves, non-degeneracy conditions and Newton polygons*, Transactions of the American Mathematical Society **357** (2005), no. 1, 59–88.

[59] Yiannis Sakellaridis, *On the unramified spectrum of spherical varieties over p-adic fields*, Compositio Mathematica **144** (2008), no. 4, 978–1016.

[60] Ana Sălăgean, *Factoring polynomials over* $\mathbb{Z}_4$ *and over certain Galois rings*, Finite fields and their applications **11** (2005), no. 1, 56–70.

[61] Dirk Segers and WA Zúñiga-Galindo, *Exponential sums and polynomial congruences along p-adic submanifolds*, Finite Fields and Their Applications **17** (2011), no. 4, 303–316.

[62] Wacław Sierpiński, *Remarques sur les racines d'une congruence*, Annales Polonici Mathematici **1** (1955), no. 1, 89–90.

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

[64] Edward Charles Titchmarsh and DR Heath-Brown, *The theory of the Riemann zeta-function*, Oxford University Press, 1986.

[65] John Jaime Rodrıguez Vega, *The Igusa local zeta function for $x^q - a$*, Lecturas Matemáticas **26** (2005), no. 2, 173–176.

[66] Willem Veys, *Zeta functions for curves and log canonical models*, Proceedings of the London Mathematical Society **74** (1997), no. 2, 360–378.

[67] Orlando Villamayor, *Constructiveness of Hironaka's resolution*, Annales scientifiques de l'École Normale Supérieure, vol. 22, 1989, pp. 1–32.

[68] Christopher Voll, *Functional equations for zeta functions of groups and rings*, Annals of mathematics (2010), 1181–1218.

[69] Joachim Von Zur Gathen and Jürgen Gerhard, *Modern computer algebra*, Cambridge university press, 2013.

[70] Joachim von zur Gathen and Silke Hartlieb, *Factorization of polynomials modulo small prime powers*, tech. report, Paderborn Univ, 1996.

[71] Joachim von zur Gathen and Silke Hartlieb, *Factoring modular polynomials*, Journal of Symbolic Computation **26** (1998), no. 5, 583–606, (Conference version in ISSAC'96).

[72] Sumio Watanabe, *Algebraic geometry and statistical learning theory*, vol. 25, Cambridge University Press, 2009.

[73] André Weil, *Variétés abéliennes et courbes algébriques*, Paris: Hermann, 1948.

[74] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc **55** (1949), no. 5, 497–508.

[75] André Weil, *Sur certains groupes d'opérateurs unitaires*, Acta mathematica **111** (1964), no. 143-211, 14.

[76] André Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*, Acta mathematica **113** (1965), 1–87.

[77] Keith R Willison, *An intracellular calcium frequency code model extended to the Riemann zeta function*, arXiv:1903.07394 (2019).

[78] Yuyu Zhu, *Trees, point counting beyond fields, and root separation*, Ph.D. thesis, Texas A&M University, 2020.

[79] WA Zúñiga-Galindo, *Igusa's local zeta functions of semiquasihomogeneous polynomials*, Transactions of the American Mathematical Society **353** (2001), no. 8, 3193–3207.

[80] WA Zúñiga-Galindo, *Computing Igusa's local zeta functions of univariate polynomials, and linear feedback shift registers*, Journal of Integer Sequences **6** (2003), no. 2, 3.

[81] WA Zúñiga-Galindo, *Local zeta functions and Newton polyhedra*, Nagoya Mathematical Journal **172** (2003), 31–58.

[82] WA Zúñiga-Galindo, *Pseudo-differential equations connected with p-adic forms and local zeta functions*, Bulletin of the Australian Mathematical Society **70** (2004), no. 1, 73–86.

[83] WA Zúñiga-Galindo, *Decay of solutions of wave-type pseudo-differential equations over p-adic fields*, Publications of the Research Institute for Mathematical Sciences **42** (2006), no. 2, 461–479.

[84] WA Zúñiga-Galindo, *Local zeta functions supported on analytic submanifolds and Newton polyhedra*, International Mathematics Research Notices **2009** (2009), no. 15, 2855–2898.

[85] WA Zúñiga-Galindo, *Local zeta functions and fundamental solutions for pseudo-differential operators over p-adic fields*, p-adic Numbers, Ultrametric Analysis, and Applications **3** (2011), no. 4, 344–358.

Received 22 Feb 2020. Revised 24 Feb 2020.

ASHISH DWIVEDI: ashish@cse.iitk.ac.in
Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, India

NITIN SAXENA: nitin@cse.iitk.ac.in
Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, India

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS