

roots of bivariables mod p^n and the related Igusa's local zeta function

Sayak Chakrabarti

Joint work with Nitin Saxena (IIT Kanpur)

International Symposium of Symbolic and Algebraic Computations
Tromsø, Norway, 2023

Algebra over $\mathbb{Z} / p^k \mathbb{Z}$

- Ring: $\text{mod } p^k$.
- Operations: $a + b = a + b \text{ mod } p^k$; $a \times b = a \cdot b \text{ mod } p^k$.
- Elements: $a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}$; $a_i \in \{0, \dots, p-1\}$.
- $(\mathbb{F}_p, \mathbb{F}_p, \dots, \mathbb{F}_p)$.

Algebra over $\mathbb{Z}/p^k\mathbb{Z}$

- $f(x) = x^2 + px \bmod p^2$.
- How many factors?
- Roots: $0, p, 2p, \dots, (p-1) \cdot p$.
- $(x - i \cdot p) \mid (x^2 + px) \bmod p^2$.
- $x^2 + px = (x + 0)(x + 1 \cdot p) = \dots = (x + i \cdot p)(x + (p - i + 1) \cdot p)$.
- Not Unique Factorization Domain (UFD).

Algebra over $\mathbb{Z}/p^k\mathbb{Z}$

- Find roots modulo p^k
- Root-finding over any commutative ring: NP-complete
- Given $f(\mathbf{x}) \in \mathbf{R}[\mathbf{x}]$, find a root of $f(\mathbf{x})$ over $\mathbf{R}$.
- Over $\mathbb{F}_p$: [HW99,LPTWY17].
- Difficult over $\mathbb{Z}/p^k\mathbb{Z}$: **Lifting**.

Notations

- Effective polynomial: Polynomial modulo p .
- Effective degree: Degree of effective polynomial.
E.g., $f(x) = x^2 + px^3$ has effective polynomial x^2 and effective degree 2.
- Valuation: $v_p(a) = v$ such that $p^v | a$ but $p^{v+1} \nmid a$.
- Val-multiplicity: $v_p(f(a + px))$.

Lifting of roots

- Elements: $a_0 + a_1p + \cdots + a_{k-1}p^{k-1}$; $a_i \in \{0, \dots, p-1\}$
- Roots mod p^k  roots mod p^{k-1} .
- Roots mod p^{k-1}  ?? roots mod p^k .

Lifting of roots

- Roots mod p^{k-1}  ?? roots mod p^k .
- Elements: $a_0 + a_1p + \cdots + a_{k-1}p^{k-1}$; $a_i \in \{0, \dots, p-1\}$
- Find each $\mathbb{F}_p$ -coordinate separately.
- $f(x) \bmod p$  root a_0 .
Let $\tilde{f}(x) := p^{-v}f(a_0 + px)$  root a_1 .
- Root: $(a_0 + a_1p)$ of $f(x) \bmod p^2$.

Lifting
of roots

Lifting of roots

Example:

- Let $f(x) = x^3 - x^2 + p \bmod p^2$.
- $f(x) \bmod p = x^3 - x^2 \longrightarrow$ roots $\{0, 1\}$.

Lifting of roots

- First coordinate: 0
 - Roots of $x^3 - x^2 + p \bmod p^2$ of the form: $0 + px$.
 - Roots of $(0 + px)^3 - (0 + px)^2 + p \bmod p^2$.
 - Roots of $p(p^2x^3 - px^2 + 1) \bmod p^2$.
 - Roots of $(p^2x^3 - px^2 + 1) \bmod p$.
 - None exist (0 does not lift)!

Lifting of roots

- First coordinate: 1
 - Roots of $x^3 - x^2 + p \bmod p^2$ of the form: $1 + px$.
 - Roots of $(1 + px)^3 - (1 + px)^2 + p \bmod p^2$.
 - Roots of $p(p^2x^3 + 2px^2 + x + 1) \bmod p^2$.
 - Roots of $(p^2x^3 + 2px^2 + x + 1) \bmod p$.
 - Root exists (1 does lift)!
 - Required root $1 + (p - 1)p$.

Univariate root-finding [BLQ13]

- Algorithm $\text{root-find}(f(x), p^k)$:
 1. If $k = 0$, return $*$.
 2. If $\deg(f) = 1$, return the root.
 3. Factorize $f(x) \bmod p$. Root set $=: S$.
 4. For each $a \in S$:
 1. Find roots of $\text{root-find}(p^{-v}f(a + px), p^{k-v})$.
- Representative roots:
 - Roots of above algorithm of the form $a_0 + a_1p + \dots + a_{k_1}p^{k_1} + p^{k_1+1} *$.
 - p^{k-k_1-1} many roots.

Lifting of roots: Hensel's lifting

Theorem: Effective polynomial is linear $\Rightarrow$ roots mod p^k exist for every k .

Example: $f(x_1, x_2) = \ell x_1 + m x_2 + n + p \cdot g(x_1, x_2)$ has root (a_1, a_2) .

Lifting: $\ell a_1 + m a_2 + n + p \ell x_1 + p n x_2 + p g(a_1 + p x_1, a_2 + p x_2)$.

Divisible by p

val-mult = 1

$p \cdot C + p^2 \cdot h(x_1, x_2)$

Continues to stay linear!

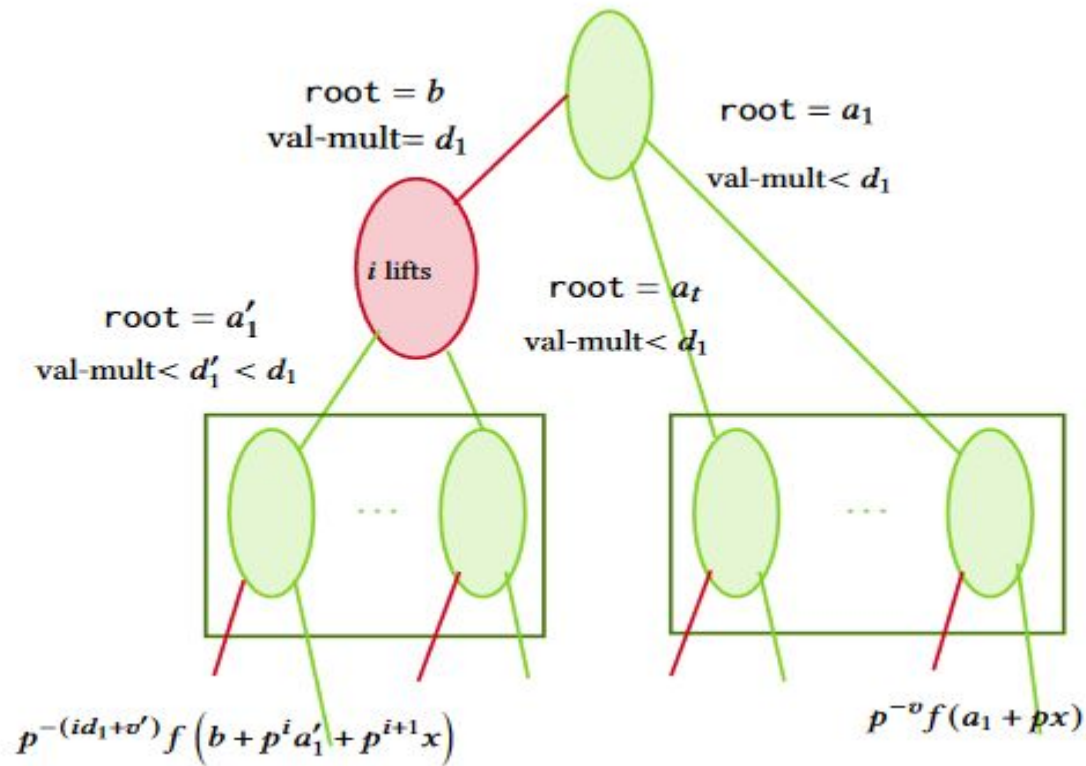
Linear-representative
roots

Structure of polynomial after lifting

- Effective degree change?
- $f(x_1, x_2) \rightarrow \tilde{f}(x_1, x_2) := p^{-v} f(a_1 + px_1, a_2 + px_2)$.
- Effective degree of $f(x_1, x_2) \rightarrow d_1$.
Effective degree of $\tilde{f}(x_1, x_2) \rightarrow d_2$.
- **Theorem:** Effective degree reduces with lifting: $d_2 \leq v \leq d_1$.
- **Goal:** Reduce to linear representative roots **OR** achieve power of p .
$$v^{(1)} + \dots + v^{(t)} \geq k$$

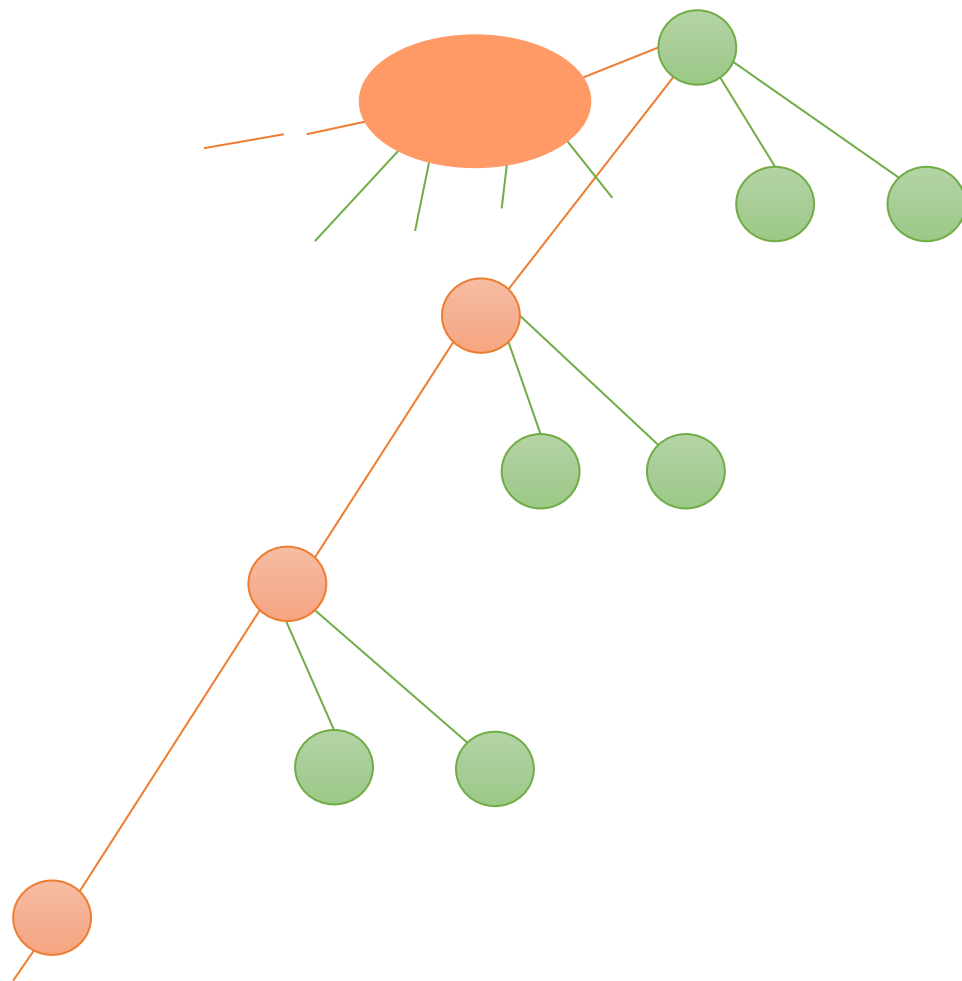
Search for roots

- Degree reduction case
- Constant degree case



Poly in p^d ?

Search for roots



Constant degree case

- Val-multiplicity d_1 roots:
 - Unique val-multiplicity d_1 roots
 d_1 -nonpower form: $\langle x_1 - a_1, x_2 - a_2 \rangle^{d_1}$.
 - Multiple val-multiplicity d_1 roots
 d_1 -power: $(a_1 x_2 - a_2 x_1)^{d_1}$.

Reduction to univariates

- For d_1 -nonpower form:
 - Only one branch exists.
- For d_1 -power:
 - Required structure $(a_2x_1 - a_1x_2)^{d_1}$ at each of i_1 -steps.
 - Let $g(L, x_2) = f(x_1, x_2)$.
 - Write $g(L, x_2)$ as $L^{d_1} + L^{d_1-1} \cdot u_1(x_2) + L^{d_1-2} \cdot \frac{u_2(x_2)}{p} + \dots + \frac{u_{d_1}(x_2)}{p^{d_1-1}}$.
 - Require $\left(L + \frac{u_1(x_2)}{d_1}\right)^{d_1} \bmod p$ to lift using d_1 -power again.
 - System of equations $u_j(x_2) = p^{j-1} \cdot d_1 C_j \cdot \left(\frac{u_1(x_2)}{d_1}\right)^j \bmod p^j$.

Chain of val-mult= d_1 roots

- Contiguous chain of ' i_1 ' d_1 -powers and ' i_3 ' d_1 -nonpower forms .
- $i_1 + i_3 \leq k/d_1$.
- Iterate over all possible i_1, i_3 .

Moving to p -adics

- $\mathbb{Z} / p^k \mathbb{Z}$ where $k \rightarrow \infty$.
- Elements: $a_0 + a_1 p + a_2 p^2 + \dots$; $a_i \in \{0, \dots, p - 1\}$.
- Different from integers?
- Not countable.
- $f(x) = x^2 + 1$, $p = 2$.
- Root over $\mathbb{Z}_2$ but not $\mathbb{Z}$.

Moving to p -adics

- $k \rightarrow$ how large?
- Roots over $\mathbb{Z}_p$ from:
 - Linear representative roots.
 - Blowing up of 0: homogeneous polynomial, e.g., $x_1^2 + (p + 1)x_1x_2$.
- $k_0 = O(d^{10}\log M)$.

Igusa's local zeta function

- Given $f(\mathbf{x}) \in \mathbb{Z}_p[x_1, \dots, x_n]$.
- Define IZF: $Z_{f,p}(s) := \int_{\mathbb{Z}_p^n} |f(\mathbf{x})|_p^s \cdot |d\mathbf{x}|$.
where $s \in \mathbb{C}$ and $\operatorname{Re}(s) > 0$.
- Poincare series: $P_{f,p}(t) := \sum_{i=0}^{\infty} N_{p^i}(f) \cdot (p^{-n} t)^i$,
where $t \in \mathbb{C}$ with $|t| < 1$, $N_{p^i}(f) := \# \text{ roots of } f \text{ mod } p^i$.
- $P(t) = \frac{1 - t \cdot Z_{f,p}(s)}{1 - t}$
where $t = p^{-s}$.

Igusa's local zeta function

- Hardness: $\#$ -P hard.
- Proof of rationality: [Igu74,Igu77,Den84].
- Efficient algorithms for computing IZF: [ZG03,DS20] (univariates).

Igusa's LZF: Counting roots modulo every p^k

- Constant $k \rightarrow N_k(f)$ is constant.
- Non-constant?
- $N_k(f)$ for all $k < k_0$.
- $N_k(f)$ for $k > k_0$:
 1. Linear-representative roots mod $p^{k_0} \rightarrow p^{k-k_0}$.
 2. Blowing up of zero roots after $k_0 \rightarrow (k - k_0)p^{k-k_0}$.

Thank you!

Summary

- ▶ Roots: Linear-rep. roots/ non-linear rep. roots
- ▶ Root finding: Degree reduction
- ▶ Constant degree: Reduction to univariates
- ▶ k_0 : Gap between $\mathbb{Z}_p$ and mod p^k
- ▶ $\mathbb{Z}_p$ roots
- ▶ Rationality of IZF for bivariate

Future work

- ▶ n-variables
- ▶ Root finding in $\text{polylog}(p)$
(d, n const)