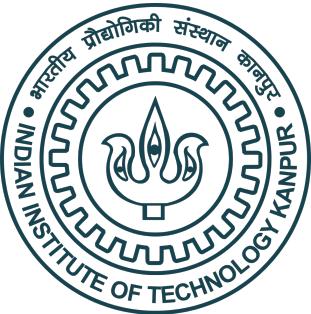


# Efficiently computing Igusa's local-zeta function

Nitin Saxena (CSE@IIT Kanpur, India)

(ANTS-XIV'20 ; with Ashish Dwivedi)

Indo-European Maths Conference  
Jan 2026, SPPU & IISER Pune



# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- Compute Poincaré Series
- Conclusion

# Zeta functions

E.g. Ramanujan *tau-function*  
 $t \cdot \prod_{m \geq 1} (1-t^m)^{24}$

- For function  $N_k$  there's **generating-function**  $G(t) := \sum_{k \geq 0} N_k t^k$ .
  - This carries comprehensive information about  $N_k$ .
  - Eg. the **growth** of  $N_k$  decides how the **power-series** converges.
- **Riemann zeta-fn**:  $\zeta(s) = \sum_{k \geq 1} 1/k^s$ .
  - What's it encoding?
- Inspired many other *zeta functions*:
  - **Selberg** zeta fn of a manifold
  - **Ruelle** zeta fn of a dynamical system
  - **Ihara** zeta fn of a graph
- **Local-zeta** functions (based on a prime  $p$ ):
  - **Hasse-Weil** zeta fn
  - **Igusa** local-zeta fn

PRIMES



Riemann 1826-66

Cycles  
Geodesics, Orbits,

◦ ◦ ◦

To count points

Galois field vs ring  
 $Z/p^kZ$

# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- Compute Poincaré Series
- Conclusion

# Igusa's local-zeta function

- Let  $\mathbb{Z}_p$  denote  $p$ -adic integers.
  - Elements are  $\sum_{i \geq 0} a_i p^i$  ( $a_i \in [0, p-1]$ ) .
- Let  $f = f(x_1, \dots, x_n)$  be  $n$ -variate integral polynomial.

infinite sum



- Defn. 1: Igusa's local-zeta fn  $Z_{f,p}(s) = \int_{(\mathbb{Z}_p)^n} |f(\mathbf{x})|_p^s \cdot |\mathbf{d}\mathbf{x}|$ .
  - Integrate using  $p$ -adic metric and Haar measure.
- This converges to a rational function in  $\mathbb{Q}(p^s)$ .
  - (Igusa'74) by resolving singularities.
  - (Denef'84) by  $p$ -adic cell decomposition.
- Counts roots  $f(\mathbf{x}) \bmod p^k$  & 'multiplies' by  $p^{-ks}$ .
- So, we can give an easier definition:

For all  $k$

# Igusa's local-zeta function

Two Defns: Analytic  
vs Discrete

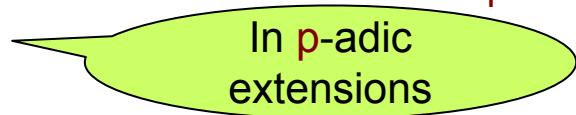
- Define  $N_k(f) := \# \text{ roots of } f(x) \bmod p^k$ .
- Defn.2: Poincaré Series  $P_{f,p}(t) = \sum_{k \geq 0} N_k(f)/p^{nk} \cdot t^k$ .
  - Eg.  $P_{0,p}(t) = \sum_{k \geq 0} t^k = 1/(1-t)$ .
  - (Igusa'74) connected them at  $t=p^{-s}$  :  $P(t) \cdot (1-t) = 1 - t \cdot Z(s)$ .
- (Igusa'74)  $P_{f,p}(t)$  converges to a rational function in  $Q(t)$ .
- This means that  $N_k(f)$  is rather *special* !
  - Generally, power-series don't converge in  $Q(t)$ .
  - Eg.  $\sum_{k \geq 0} (1/k!) \cdot t^k$  is *irrational* !
- Convergence proofs are quite *non-explicit*.
  - What do we learn about  $N_k(f)$  , for small  $k$  ?

# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- Compute Poincaré Series
- Conclusion

# Algorithmic questions

- **Qn:** Could  $N_k(f)$  be computed efficiently?
- Trivially, in  $p^{kn}$  time.
  - Much faster *unlikely*.
  - It's *NP-hard*; even Permanent-hard !
- Could  $N_k(f)$  be computed efficiently, for **univariate**  $f(x)$ ?
  - **Qn:** In  $\text{poly}(\deg(f), \log p^k)$  time?
- Or, try to compute the analytic-integral defining  $Z_{f,p}(s)$ .
- (Chistov'87) gave a *randomized* algorithm to factor  $f(x)$  over  $Z_p$ .
  - Using this one could factor  $f$  into roots,
  - and attempt the integration ...?
- **Qn:** But, a *deterministic poly*-time algorithm for  $N_k(f)$  ?



In  $p$ -adic extensions

# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- Compute Poincaré Series
- Conclusion

# Root-finding mod $p^k$

- Instead of integration, we take the route of roots mod  $p^k$ .
- Let  $f \bmod p^k$  be degree  $d$  univariate polynomial.
- (Berthomieu,Lecerf,Quintin'13) Roots of  $f \bmod p^k$  arrange as **representative-roots**:
  - $a =: \sum_{0 \leq i < \ell} a_i p^i + *p^\ell$  ( $a_i \in [0, p-1]$  ,  $* \in \mathbb{Z}$ ) .
  - $a$  is *minimal* &  $f(a) = 0 \bmod p^k$  .
  - At most  $d$  rep.roots.
- Proof is *inductive*, based on the **transformation**:
  - $g(x) := f(\sum_{0 \leq i < m} a_i p^i + x \cdot p^m) / p^v \bmod p^{k-v}$  .
  - Root of  $g(x) \bmod p$  gives  $a_m$  .
  - Continue with  $\sum_{0 \leq i \leq m} a_i \cdot p^i$  .

Reduces char  
 $p^k$  to  $p$

Many  $a_m$ 's  $\Rightarrow$   
slower  
growth of  $m$ .

Why are rep.roots  
**a few?**

# Root-finding mod $p^k$

- Rep.roots are few, but roots may be *exponentially* many!
  - Eg.  $f := px \bmod p^2$  has  $p$  roots,
  - but just one rep.root  $a =: 0 + *p$  !
- (BLQ'13) yields *fast randomized* algorithm to find roots  $\bmod p^k$ .
  - Counting is easy, as rep.root  $a$  means  $p^{k-\ell}$  roots.
  - $a = \sum_{0 \leq i < \ell} a_i \cdot p^i + *p^\ell$ .
  - Summing up over rep.roots, gives **all roots**.
- How to make it *deterministic* poly-time?
- Rep.roots yield  $N_k(f) = \sum_i p^{k-\ell_i}$ .
  - What does it say about *Poincaré* series  $P_{f,p}(t)$  ?

$\ell_i$  depends on  
 $i, k$

# Root-finding mod $p^k$

- (Dwivedi,Mittal,S '19) gave fast **deterministic** algorithm to **implicitly** find roots mod  $p^k$ .
- Idea: Store rep.roots  $\mathbf{a} = \sum_{0 \leq i < \ell} a_i \cdot p^i + *p^\ell$  in **maximal split ideals**.
  - $\mathbf{I} = \langle h_0(x_0), h_1(x_0, x_1), \dots, h_{\ell-1}(x_0, \dots, x_{\ell-1}) \rangle$  .
  - Each zero of  $\mathbf{I}$  in  $\mathbb{F}_p^\ell$  defines a rep.root.
  - Essentially, run (BLQ'13) mod  $\mathbf{I}$  (*without* randomization!).
  - Keep 'growing'  $\mathbf{I}$ .
- (DMS'19) yields *fast deterministic* algorithm to **count** roots  $f$  mod  $p^k$ .

Yet  $N_k(f)$  remains a *mystery* !

# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- Compute Poincaré Series
- Conclusion

# Root-counting mod $p^k$

- Intuitively,  $N_k(f) = \sum_i p^{k - \ell_i}$  should behave better for **large  $k$** .
  - Since, large  $k$  is like **studying roots in  $Z_p$** .
- We show, for large  $k$  :  $\ell_i$  is *linear* in  $k$ .

## Details:

- $k > k_0 := \deg(f) \cdot \text{val}_p(\text{disc}(\text{rad}(f)))$ .
- $\ell_i = \lceil (k - \text{val}_p(f_i(\alpha_i))) / \text{mult}(\alpha_i) \rceil$ .
  - Where,  $\alpha_i$  are all  **$p$ -adic integer roots** of  $f(x)$ .

Constant  $(k - \ell_i)/k$   
=:  $u_i$

Roots  
*uniquely*  
lift as  
 $k$  grows.

Curiously, **squarefree  $f$  & large  $k$**   $\Rightarrow N_k(f)$  *independent* of  $k$ .

# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- **Compute Poincaré Series**
- Conclusion

# Compute Poincaré Series

- Got :  $N_k(f) = \sum_i p^{k \cdot u_i}$  for  $k > k_0$  .
- So,  $P(t) = \sum_{k \geq 0} N_k(f) / p^k \cdot t^k$  ,  
 $=: P_0(t) + \sum_{k \geq k_0} N_k(f) / p^k \cdot t^k$  ,  
 $= P_0(t) + \sum_{k \geq k_0} \sum_i p^{k \cdot (u_i - 1)} \cdot t^k$  .
- The infinite sum converges to a *rational*, in  $Q(t)$ .
- Thus,  $P(t)$  is a *rational function*.
- Our algorithm computes  $N_k(f)$  function;  
hence, both  $P_0(t)$  and the infinite sum are *known*.
  - In  $\text{poly}(|f|, \log p)$  time.

# Contents

- Zeta functions
- Igusa's local-zeta fn
- Algorithmic questions
- Root finding mod  $p^k$
- Root counting mod  $p^k$
- Compute Poincaré Series
- Conclusion

# At the end ...

- *Det.poly-time* algorithm for Igusa's local-zeta function.
  - For *univariate* polynomial  $f$ .
- Could we do this for **bivariate** polynomial  $f(x_1, x_2)$  ?
- Relevant Questions:
  1. Estimating the count  $N_k(f(x_1, x_2)) = ?$  (Chakrabarti, S., ISSAC'23)
  2. Counting **factors** of  $f(x) \bmod p^k$ ?
    - Irreducibility-testing of  $f(x) \bmod p^5$  ? (Mahapatra, S., WIP)
    - GCD of  $f(x), g(x) \bmod p^5$  ?
  3. Hasse-Weil Zeta fn of a *variety*  $\bmod p$ ? (S., Madhavan V., WIP)



Thank you!