Efficiently computing Igusa's local-zeta function

Nitin Saxena (CSE@IIT Kanpur, India)

(appeared in ANTS-XIV'20 ; with Ashish Dwivedi)

Oberseminar

Nov 2021, Univ. Bayreuth (virtually)

Contents

Zeta functions

Eg. Ramanujan *tau-function*

- 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? PRIMES

Riemann 1826-66

- 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

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

Igusa 1924-2013

- Let Z_p denote p-adic integers.

infinite sum

  - Elements are $\sum_{i\geq 0} a_i p^i$ ($a_i \in [0,p-1]$) .
- Let $f = f(x_1,\ldots,x_n)$ be n-variate integral polynomial.
- Defn.1: Igusa's local-zeta fn $Z_{f,p}(s) = \int_{(Z\_p)^n} |f(\mathbf{x})|_p{}^s.|d\mathbf{x}|$.
  - Integrate using *p-adic metric* & *Haar measure*.
- This converges to a rational function in $Q(p^s)$.
  - (Igusa'74) by resolving singularities.
  - (Denef'84) by p-adic cell decomposition.

For all k

- Counts roots $f(\mathbf{x}) \bmod p^k$ & `multiplies' by p^{-ks}.
- So, we can give another definition:

Igusa's local-zeta function

Defns: Analytic vs *Discrete*

- Define $N_k(f) := \#$ roots of $f(\mathbf{x}) \bmod p^k$.
- Defn.2: Poincaré Series $P_{f,p}(t) = \sum_{k\geq 0} N_k(f)/p^{nk} . t^k$.
  - Eg. $P_{0,p}(t) = \sum_{k\geq 0} t^k = 1/(1-t)$.
  - (Igusa'74) connected them at $t=p^{-s}$: $P(t).(1-t) = 1 - t.Z(s)$.
- (Igusa'74) $P_{f,p}(t)$ converges to a <u>rational</u> function in $Q(t)$.
- This means that $N_k(f)$ is rather *special*!
  - Generally, power-series don't converge in $Q(t)$.
  - Eg. $\sum_{k\geq 0} (1/k!) .t^k$ 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 *un*likely.
  - It's *NP-hard*; even Permanent-hard !
- Could $N_k(f)$ be computed efficiently, for univariate $f(x)$?
  - Qn: In poly($deg(f)$, $\log p$, k) time?
- Or, try to compute the integral in $Z_{f,p}(s)$.
- (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 ...?

In p-adic extensions

- **Qn:** But, a *deterministic poly*-time algorithm for $N_k(f)$?

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:
  - $\mathbf{a} =: \sum_{0\le i<l} a_i p^i + {*}p^l$ ($a_i \in [0,p-1]$, $* \in Z$) .
  - $\mathbf{a}$ is *minimal* & $f(\mathbf{a}) = 0 \bmod p^k$.
  - At most d rep.roots.
- Proof is *inductive*, based on the transformation:
  - $g(x) := f(\sum_{0\le i<m} a_i p^i + x.p^m) / p^v \ \bmod p^{k-v}$.
  - Root of $g(x) \bmod p$ gives a_m .
  - Continue with $\sum_{0\le i\le m} a_i p^i$.

Reduces char p^k to p

Why are rep.roots *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 $\mathbf{a} =: 0 + {*}p$!
- (BLQ'13) yields *fast randomized* algorithm to find roots $\bmod\ p^k$.
  - Counting is easy, as rep.root $\mathbf{a}$ means p^{k-l} roots.
  - $\mathbf{a} = \sum_{0\le i<l} a_i p^i + {*}p^l$.
  - Summing up over rep.roots, gives all roots.
- How to make it *deterministic* poly-time?
- Rep.roots yield $N_k(f) = \sum_i p^{k-l\_i}$.
  - What does it say about *Poincaré series* $P_{f,p}(t)$?

l_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 $\mathbf{a} = \sum_{0\le i<l} a_i p^i + {*}p^l$ in maximal split ideals.
  - $\mathbf{I} = \langle h_0(x_0) , h_1(x_0,x_1) ,\ldots, h_{l-1}(x_0,\ldots,x_{l-1})\rangle$.
  - Each zero of $\mathbf{I}$ in $\mathbb{F}_p^{\,l}$ 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, $N_k(f) = \sum_i p^{k - l_i}$ should behave better for large k .
  - Since, large k is like studying roots in Z_p .

- We show, for large k : l_i is *linear* in k.

Constant $(k-l_i)/k =: u_i$

<u>Details</u>:

- $k > k_0 := \deg(f) * \mathrm{val}_p(\mathrm{disc}(\ \mathrm{rad}(f)\ ))$.

- $l_i = \lceil\ (\ k - \mathrm{val}_p(f_i(\alpha_i))\ )\ /\ \mathrm{mult}(\alpha_i)\ \rceil$.
  - Where, α_i are all p-adic integer roots of $f(x)$.

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 : $N_k(f) = \sum_i p^{k.u\_i}$ for $k > k_0$.
- So, $P(t) = \sum_{k\geq 0} N_k(f)/p^k .t^k$,
  $= P_0(t) + \sum_{k\geq k\_0} N_k(f)/p^k .t^k$,
  $= P_0(t) + \sum_{k\geq k\_0} \sum_i p^{k.(u\_i-1)} .t^k$.
- The infinite sum converges to a *rational,* in $Q(t)$.
- Thus, $P(t)$ is a rational function.
- Our algorithm computes $N_k(f)$; hence, both $P_0(t)$ and the infinite sum are *known*.
  - In 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 Qns:

1. Estimating the count $N_k(f(x_1, x_2)) =$?

2. Counting factors of $f(x) \bmod p^k$?
   - Irreducibility-testing of $f(x) \bmod p^5$?

Thank you!