Faster Root Counting Over $\mathbb{Z}/(p^k)$

J. Maurice Rojas
July 19, 2018

This is joint work with...

Leann Kopp Natalie Randall Yuyu Zhu

This is joint work with...

Leann Kopp Natalie Randall Yuyu Zhu

...and is heavily based on the joint work with Qi Cheng, Shuhong Gao, and Daqing Wan just presented here!

Main Result

...simpler, faster randomized version of our root counting algorithm from earlier today!

Main Result

...simpler, faster randomized version of our root counting algorithm from earlier today!: For counting roots in $\mathbb{Z}/(p^k)$ of a polynomial, we get a speed-up exponential in k.

Background: $k = \infty \implies p$-adic rationals

- Relative to the *sparse* input size...

Background: $k = \infty \implies p$-adic rationals

- Relative to the *sparse* input size...
  - Detecting roots in $\mathbb{Z}/(p)$ is **NP**-hard... [Bi, Cheng, Rojas, 2014]. (Complements [Kipnis, Shamir, 1999] result over $\mathbb{F}_{2^k}$...

Background: $k = \infty \implies p$-adic rationals

- Relative to the *sparse* input size...
  - Detecting roots in $\mathbb{Z}/(p)$ is **NP**-hard... [Bi, Cheng, Rojas, 2014]. (Complements [Kipnis, Shamir, 1999] result over $\mathbb{F}_{2^k}$...
  - Counting roots in $(\mathbb{Z}/(p))^2$ is #**P**-hard... [von zur Gathen, Karpinski, Shparlinski, 1996]

Background: $k = \infty \implies p$-adic rationals

- Relative to the *sparse* input size...
    - Detecting roots in $\mathbb{Z}/(p)$ is **NP**-hard... [Bi, Cheng, Rojas, 2014]. (Complements [Kipnis, Shamir, 1999] result over $\mathbb{F}_{2^k}$...
    - Counting roots in $(\mathbb{Z}/(p))^2$ is #**P**-hard... [von zur Gathen, Karpinski, Shparlinski, 1996]
- For any fixed k, detecting roots in $\mathbb{Z}/(p^k)$ is **NP**-hard...

Background: $k = \infty \implies p$-adic rationals

- Relative to the *sparse* input size...
  - Detecting roots in $\mathbb{Z}/(p)$ is **NP**-hard... [Bi, Cheng, Rojas, 2014]. (Complements [Kipnis, Shamir, 1999] result over $\mathbb{F}_{2^k}$...
  - Counting roots in $(\mathbb{Z}/(p))^2$ is #**P**-hard... [von zur Gathen, Karpinski, Shparlinski, 1996]
- For any fixed k, detecting roots in $\mathbb{Z}/(p^k)$ is **NP**-hard...
- Detecting roots in $\mathbb{Q}_p$ for an input $(f, p) \in \mathbb{Z}[x_1] \times \{2, 3, 5, \ldots\}$ is **NP**-hard with respect to **ZPP** reductions [Avendaño, Ibrahim, Rojas, Rusek, 2011].

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$,

Key Reduction for Recursion

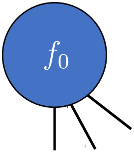
We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

Example of Recursion

To count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...

Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



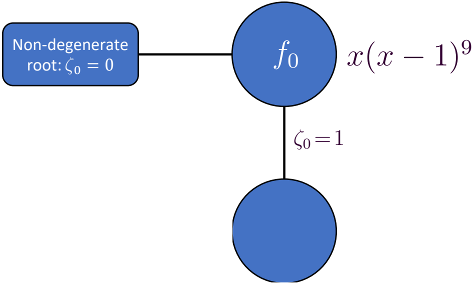
Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...

f_0 $\quad x(x-1)^9 \qquad (= f(x) \bmod 3)$

Example of Recursion

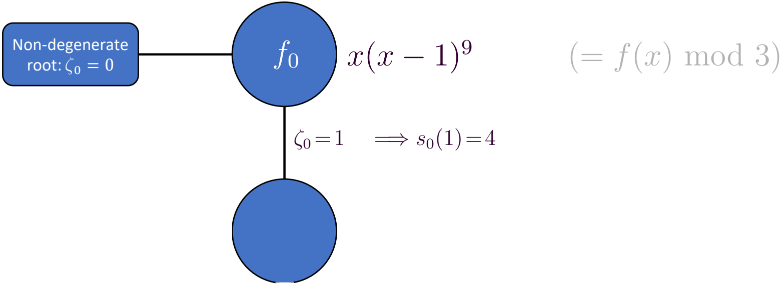
To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



$(= f(x) \bmod 3)$

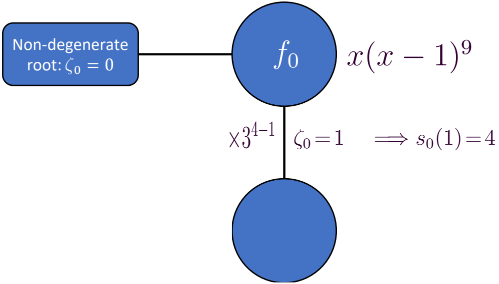
Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



Example of Recursion

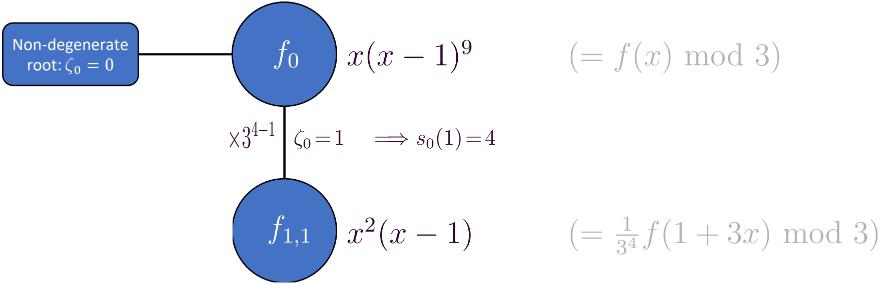
To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



$(= f(x) \bmod 3)$

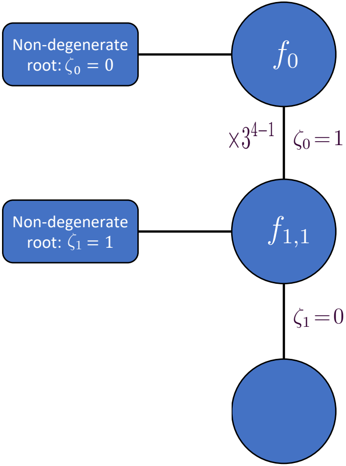
Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)\ldots$



Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



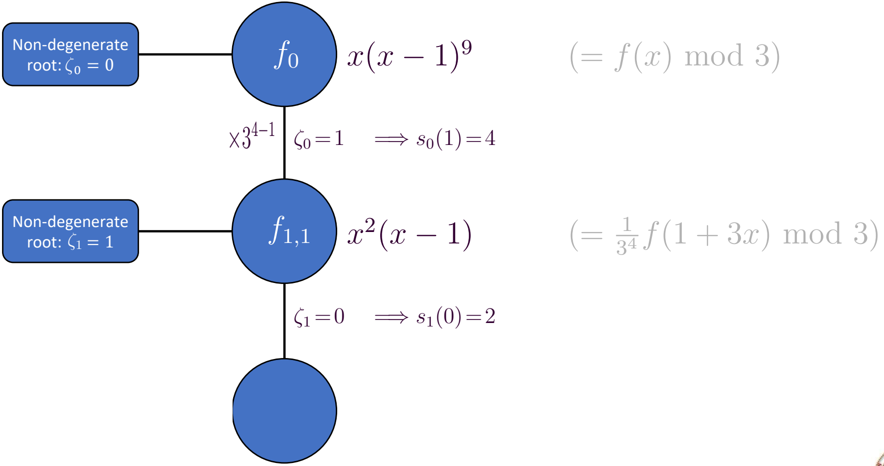
$x(x-1)^9$ $\quad (= f(x) \bmod 3)$

$\Longrightarrow s_0(1) = 4$

$x^2(x-1)$ $\quad (= \frac{1}{3^4} f(1+3x) \bmod 3)$

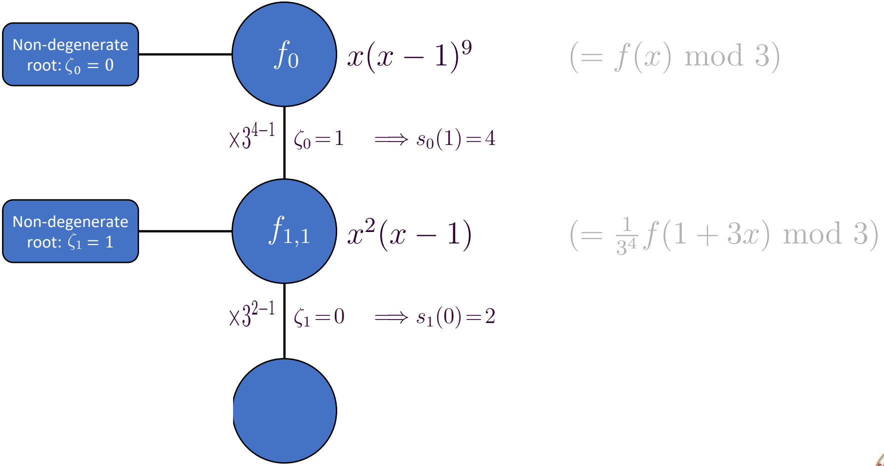
Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)\ldots$

Non-degenerate root: $\zeta_0 = 0$ — f_0: $x(x-1)^9$ $\quad (= f(x) \bmod 3)$

$\times 3^{4-1}$ $\quad \zeta_0 = 1 \implies s_0(1) = 4$

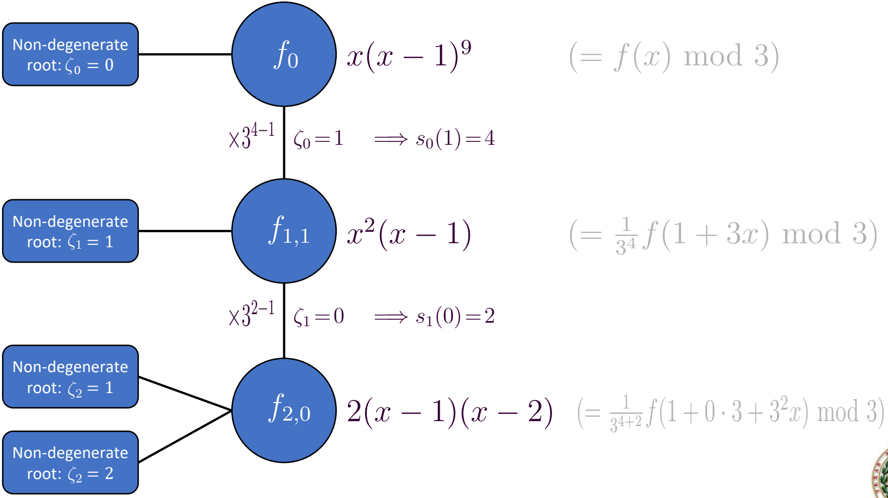
Non-degenerate root: $\zeta_1 = 1$ — $f_{1,1}$: $x^2(x-1)$ $\quad (= \frac{1}{3^4} f(1+3x) \bmod 3)$

$\times 3^{2-1}$ $\quad \zeta_1 = 0 \implies s_1(0) = 2$

$f_{2,0}$: $2(x-1)(x-2)$ $\quad (= \frac{1}{3^{4+2}} f(1 + 0 \cdot 3 + 3^2 x) \bmod 3)$

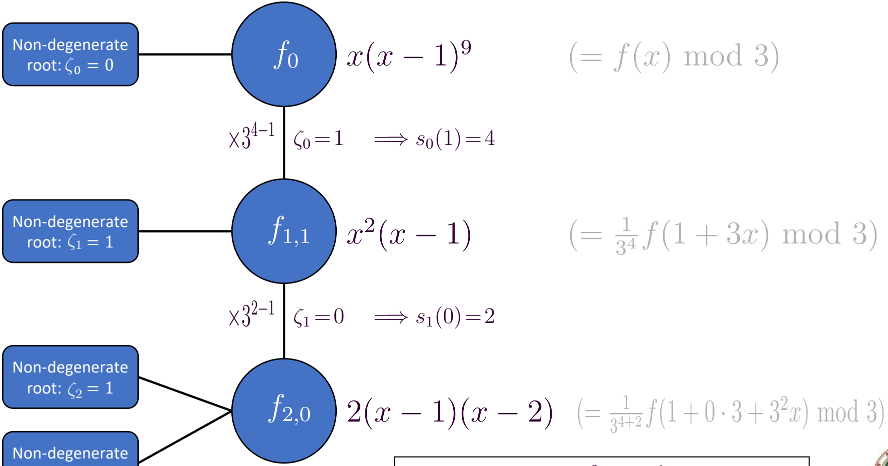
Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)$...



Example of Recursion

To ~~find~~ count the roots of $f(x) := x^{10} - 10x + 738$ in $\mathbb{Z}/(3^7)\ldots$



Final Count $= 1 + 3^3(1 + 3^1(1+1)) = 190.$

Las Vegas Complexity Bound

Maximizing number of nodes,

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$,

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

$$d^{1.5+o(1)}(\log p)^{2+o(1)}1.12^k.$$

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

$$d^{1.5+o(1)}(\log p)^{2+o(1)}1.12^k.$$

...and for $p=2$, we get major speed-ups for $k \geq 10$,

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

$$d^{1.5+o(1)}(\log p)^{2+o(1)}1.12^k.$$

...and for $p=2$, we get major speed-ups for $k \geq 10$, e.g., for degree 100, our algorithm takes milliseconds, vs. half a second for brute-force

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

$$d^{1.5+o(1)}(\log p)^{2+o(1)}1.12^k.$$

...and for $p=2$, we get major speed-ups for $k\geq 10$, e.g., for degree 100, our algorithm takes milliseconds, vs. half a second for brute-force (in `Maple`

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

$$d^{1.5+o(1)}(\log p)^{2+o(1)}1.12^k.$$

...and for $p=2$, we get major speed-ups for $k \geq 10$, e.g., for degree 100, our algorithm takes milliseconds, vs. half a second for brute-force (in `Maple` on a Dell Desktop

Las Vegas Complexity Bound

Maximizing number of nodes, and noting that each node computation is dominated by factorization over $\mathbb{F}_p$, we obtain complexity no worse than:

$$d^{1.5+o(1)}(\log p)^{2+o(1)}1.12^k.$$

...and for $p=2$, we get major speed-ups for $k \geq 10$, e.g., for degree 100, our algorithm takes milliseconds, vs. half a second for brute-force (in `Maple` on a Dell Desktop with an Intel Core i7-4770 and 4Gb RAM).

♡ Thank you for your attention!

See www.math.tamu.edu/~rojas for preprints and further info...

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically 0 mod p,

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min \Big\{ \mathrm{ord}_p(f(\zeta_0)),$

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min \Big\{ \mathrm{ord}_p(f(\zeta_0)), \mathrm{ord}_p(f'(\zeta_0)p),$

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min \left\{ \mathrm{ord}_p(f(\zeta_0)), \mathrm{ord}_p(f'(\zeta_0)p), \ldots, \right.$

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically 0 mod p, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the f mod p.
- Let $s_0(\zeta_0) := \min\left\{\mathrm{ord}_p(f(\zeta_0)), \mathrm{ord}_p(f'(\zeta_0)p), \ldots, \mathrm{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically 0 mod p, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the f mod p.
- Let $s_0(\zeta_0) := \min\left\{\operatorname{ord}_p(f(\zeta_0)), \operatorname{ord}_p(f'(\zeta_0)p), \ldots, \operatorname{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.
- Let $f_1(x) := \frac{1}{p^{s_0(\zeta_0)}} f(\zeta_0 + px)$.

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min\left\{\mathrm{ord}_p(f(\zeta_0)), \mathrm{ord}_p(f'(\zeta_0)p), \ldots, \mathrm{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.
- Let $f_1(x) := \frac{1}{p^{s_0(\zeta_0)}} f(\zeta_0 + px)$. You now need only count the roots of f_1 in $\mathbb{Z}/\left(p^{k-s_0(\zeta_0)}\right)$!

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically 0 mod p, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the f mod p.
- Let $s_0(\zeta_0) := \min\left\{\text{ord}_p(f(\zeta_0)), \text{ord}_p(f'(\zeta_0)p), \ldots, \text{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.
- Let $f_1(x) := \frac{1}{p^{s_0(\zeta_0)}} f(\zeta_0 + px)$. You now need only count the roots of f_1 in $\mathbb{Z}\,/\left(p^{k-s_0(\zeta_0)}\right)$!
- Hensel's Lemma implies the $s_0(\zeta_0) = 1$ case is easy.

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min\left\{\mathrm{ord}_p(f(\zeta_0)), \mathrm{ord}_p(f'(\zeta_0)p), \ldots, \mathrm{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.
- Let $f_1(x) := \frac{1}{p^{s_0(\zeta_0)}} f(\zeta_0 + px)$. You now need only count the roots of f_1 in $\mathbb{Z}/\left(p^{k-s_0(\zeta_0)}\right)$!
- Hensel's Lemma implies the $s_0(\zeta_0) = 1$ case is easy. The case $s_0(\zeta_0) = k$ implies ζ_0 has exactly p^{k-1} lifts.

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min\left\{\mathrm{ord}_p(f(\zeta_0)), \mathrm{ord}_p(f'(\zeta_0)p), \ldots, \mathrm{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.
- Let $f_1(x) := \frac{1}{p^{s_0(\zeta_0)}} f(\zeta_0 + px)$. You now need only count the roots of f_1 in $\mathbb{Z}/\left(p^{k-s_0(\zeta_0)}\right)$!
- Hensel's Lemma implies the $s_0(\zeta_0) = 1$ case is easy. The case $s_0(\zeta_0) = k$ implies ζ_0 has exactly p^{k-1} lifts.
- We may thus assume $s_0(\zeta) \in \{2, \ldots, k-1\}$.

Key Reduction for Recursion

We'll *count* $\zeta = \zeta_0 + p\zeta_1 + \cdots + p^{k-1}\zeta_{k-1} \in \mathbb{Z}/(p^k)$ by first *finding* possible $\zeta_0 \in \{0, \ldots, p-1\}$, then *counting* the remaining base-p digits via an algebraically defined recursion...

- If $f \in \mathbb{Z}[x]$ is not identically $0 \bmod p$, let $\zeta_0 \in \{0, \ldots, p-1\}$ be any root of the $f \bmod p$.
- Let $s_0(\zeta_0) := \min\left\{\text{ord}_p(f(\zeta_0)), \text{ord}_p(f'(\zeta_0)p), \ldots, \text{ord}_p\left(\frac{f^{(k-1)}(\zeta_0)}{(k-1)!}p^{k-1}\right)\right\}$.
- Let $f_1(x) := \frac{1}{p^{s_0(\zeta_0)}} f(\zeta_0 + px)$. You now need only count the roots of f_1 in $\mathbb{Z}/\left(p^{k-s_0(\zeta_0)}\right)$!
- Hensel's Lemma implies the $s_0(\zeta_0) = 1$ case is easy. The case $s_0(\zeta_0) = k$ implies ζ_0 has exactly p^{k-1} lifts.
- We may thus assume $s_0(\zeta) \in \{2, \ldots, k-1\}$.
- Proceed recursively!