Counting Roots for Polynomials Modulo Prime Powers

Qi Cheng

School of Computer Science
University of Oklahoma

July 2018
ANTS

This is a joint work with Shuhong Gao, Maurice Rojas and Daqing Wan.

Given a prime p, and a polynomial $f \in \mathbf{Z}[x]$ of degree d with coefficients of absolute value $< p^t$, it is a basic problem to count the roots of f in $\mathbf{Z}/(p^t)$.

- Aside from its natural cryptological relevance, counting roots in $\mathbf{Z}/(p^t)$ is closely related to factoring polynomials over the p-adic rationals $\mathbf{Q}_p$
- and the latter problem is fundamental in polynomial-time factoring over the rationals
- the study of prime ideals in number fields
- the computation of zeta functions and the detection of rational points on curves.

Outline

- Introduction: $t = 1$
- Complications arise for $t > 1$
- $t = 2, 3, 4$
- General t
- Open problems

Factoring polynomials over finite fields

- By root rationality: $\gcd(f(x), x^p - x)$
- By root multiplicities: $\gcd(f(x), \frac{\mathrm{d}f}{\mathrm{d}x}(x))$
-
$$f(x) = f_1(x) f_2^2(x) f_3^3(x) ... f_l^l(x) F(x) \pmod{p}, \tag{1}$$
where each f_i is a monic polynomial over $\mathbf{F}_p$ that can be split into a product of distinct linear factors over $\mathbf{F}_p$, and the f_i are pairwise relatively prime, and $F(x)$ is free of linear factors in $\mathbf{F}_p[x]$.

- Further factorization is not known to be in deterministic polynomial time.
- Use random r_1 and r_2 , can split further:

$$\gcd(f(r_1(x + r_2)), x^{(p-1)/2} - 1)$$

Hensel lifting

$$
\begin{aligned}
x^2 &= 2 \\
x_1^2 &= 2 \pmod{7} \\
x_1 &= 3 \\
(3 + 7x_2)^2 &= 2 \pmod{7^2} \\
9 + 42x_2 &= 2 \pmod{7^2} \\
7 + 42x_2 &= 0 \pmod{7^2} \\
1 + 6x_2 &= 0 \pmod{7} \\
x_2 &= 1 \\
x &= 10 \pmod{7^2} \\
&\vdots
\end{aligned}
$$

Hensel lifting

$$\begin{aligned}
x^2 &= 2 \\
x_1^2 &= 2 \pmod 7 \\
x_1 &= 3 \\
(3 + 7x_2)^2 &= 2 \pmod{7^2} \\
9 + 42x_2 &= 2 \pmod{7^2} \\
7 + 42x_2 &= 0 \pmod{7^2} \\
1 + 6x_2 &= 0 \pmod 7 \\
x_2 &= 1 \\
x &= 10 \pmod{7^2} \\
&\vdots
\end{aligned}$$

A simple root of f (roots of $f_1(x)$) in $\mathbf{Z}/(p)$ can be lifted uniquely to a root in $\mathbf{Z}/(p^t)$, according to the classical Hensel's lemma

$$\begin{aligned}
&f(x_1 + px_2) \\
=&f(x_1) + px_2 \frac{\mathrm{d}f}{\mathrm{d}x}(x_1) \pmod{p^2} \\
&f(x_1 + p^{t-1}x_2) \\
=&f(x_1) + p^{t-1}x_2 \frac{\mathrm{d}f}{\mathrm{d}x}(x_1) \pmod{p^t}
\end{aligned}$$

When roots have multiplicities

- A root over $\mathbf{F}_p$ can be lifted to *exponentially* many roots: The quadratic polynomial
$$x^2 = 0,$$
which has roots $0, p, 2p, \cdots, (p-1)p$ in $\mathbf{Z}/(p^2)$, is such an example.
- A root over $\mathbf{F}_p$ can be lifted to no root in $\mathbf{Z}/p^2\mathbf{Z}$:
$$x^2 + p = 0$$
has no roots mod p^2, even though it has a root mod p.
- There is surprisingly little written about root counting in $\mathbf{Z}/(p^t)$ for $t \geq 2$: The cases $t \geq 3$, which we solve here, appeared to be completely open.

More Complications

- One complication with $t \geq 2$ is that polynomials in $(\mathbf{Z}/(p^t))[x]$ do not have unique factorization, thus obstructing a simple use of polynomial gcd.
- It is still an open problem whether there exists a deterministic polynomial time algorithm for finding roots of polynomials modulo p.

Igusa zeta function

- Let $N_t(f)$ denote the number of roots of f in $\mathbf{Z}/(p^t)$ (setting $N_0(f) := 1$). The *Poincare series for f* is

$$P(x) := \sum_{t=0}^{\infty} N_t(f) x^t$$

- Example: $x^2 = 0$

t	0	1	2	3	$\cdots$	i
# of roots mod p^t	1	1	p	p	$\cdots$	$p^{\lfloor i/2 \rfloor}$

- $\sum p^i x^{2i} + \sum p^i x^{2i+1} = \frac{1+x}{1-px^2}$

- Assuming $P(x)$ is a rational function in x, one can reasonably recover $N_t(f)$ for any t via standard generating function techniques.
- That $P(x)$ is in fact a rational function in x was first proved in 1974 by Igusa (in the course of deriving a new class of zeta functions), applying resolution of singularities.
- Denef found a new proof (using p-adic cell decomposition leading to more algorithmic approaches later).
- While this in principle gives us a way to compute $N_t(f)$, there are few papers studying the computational complexity of Igusa zeta functions.

Main result

Theorem

There is a deterministic algorithm that computes the number, $N_t(f)$, of roots in $\mathbf{Z}/(p^t)$ of f in time $(d + \log(p) + 2^t)^{O(1)}$.

Note that Theorem 1 implies that if $t = O(\log \log p)$ then there is a deterministic $(d + \log p)^{O(1)}$ algorithm to count the roots of f in $\mathbf{Z}/(p^t)$.

Main techniques I

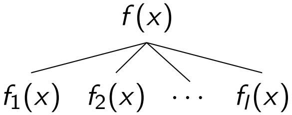
- We use (triangular) ideals in the ring $\mathbf{Z}_p[x_1, x_2, \ldots]$ of multivariate polynomials over the p-adic integers to keep track of the roots of f in $\mathbf{Z}/(p^t)$. More precisely, if $(x_1, x_2, \cdots, x_i) \in \mathbf{Z}_p^i$ is a zero of $I \subseteq \mathbf{Z}_p[x_1, x_2, \cdots, x_i]$, then

$$f(x_1 + px_2 + \cdots + p^{i-1}x_i) = 0 \pmod{p^s}.$$

- We can decompose the ideals according to multiplicity type and rationality of their roots, so that the ideals have only rational roots and are radical over $\mathbf{F}_p$.
- This process produces a tree of ideals which will ultimately encode the summands making up our final count of roots.

Main techniques II

We manage to keep most of our computation within $\mathbf{Z}/(p) = \mathbf{F}_p$, and maintain uniformity for the roots of our intermediate ideals, by using Teichmuller lifting. Namely, if $(x_1, x_2, \cdots, x_i) \in \mathbf{Z}_p^i$ is a zero of $I \subseteq \mathbf{Z}_p[x_1, x_2, \cdots, x_i]$, then x_j is the Teichmuller lift of some number in $\mathbf{F}_p$.

- The core of our algorithm counts how many roots of f in $\mathbf{Z}/(p^t)$ are lifts of roots of f_i in $\mathbf{F}_p$.
- 

- For f_1, by Hensel's lifting lemma, the answer should be $\deg f_1$ for all t.

Algorithm

- For other f_i, however, Hensel's lemma will not apply, so we run our algorithm on the pair (f, m), where m is the lift of f_i to $\mathbf{Z}[x]$, for each $i \in \{2, \ldots, l\}$, to see how many lifts (to roots of f in $\mathbf{Z}/(p^t)$) are produced by the roots of f_i in $\mathbf{Z}/(p)$. The final count will be the summation of the results over all the f_i, since the roots of f in $\mathbf{Z}/(p^t)$ are partitioned by the roots of the f_i.
- If randomness is allowed, $m(x)$ has degree one.

Since $m|f$ (in fact $m^2|f$) over $\mathbf{F}_p[x]$, we have $f(x) = 0 \pmod{(m(x), p)}$, and over $\mathbf{Z}[x_1, x_2]$,

$$f(x_1 + px_2) = 0 \pmod{(m(x_1), p)}.$$

If $f(x_1 + px_2) = 0 \pmod{(m(x_1), p^t)}$, then each root of m in $\mathbf{F}_p$ lifts to p^{t-1} roots of f in $\mathbf{Z}/(p^t)$, and the counting problem for (f, m) is solved.

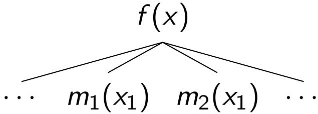
Otherwise we can find efficiently an integer $1 \le s < t$ and $g \in \mathbf{Z}[x_1, x_2]$ such that

$$f(x_1 + px_2) = p^s g(x_1, x_2) \pmod{(m(x_1), p^t)}, \qquad (2)$$

where $\deg_{x_2} g \le t - 1$, $\deg_{x_1} g < \deg m$ and $g(x_1, x_2) \ne 0 \pmod{p, m(x_1)}$.

Normalization

- Let
$$g(x_1, x_2) = \sum_{0 \le j < t} g_j(x_1) x_2^j.$$
Assume that the leading coefficient is invertible in $\mathbf{F}_p[x]/(m(x_1))$, so the polynomial can be made monic.
- Otherwise,



$s = 1$

Since $m^2|f$ over $\mathbf{F}_p$, we must have

$$f(x_1 + px_2) = pg_0(x_1) \pmod{m(x_1), p^2}.$$

Since $\gcd(m, g_0) = 1$ over $\mathbf{F}_p$, none of the roots of m in $\mathbf{F}_p$ can be lifted to $\mathbf{Z}/p^2$. So for now on we assume that $1 < s < t$.

$t = 3$

The only interesting case is when $s = 2$. We have $f(x_1 + px_2) = p^2 g(x_1, x_2) \pmod{m(x_1), p^3}$.

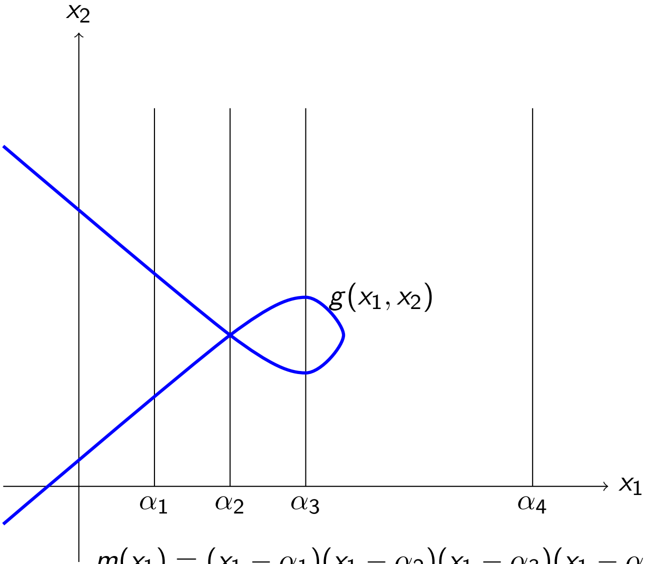
Theorem

The number of roots in $\mathbf{Z}/(p^3)$ of f that are lifts of roots of $m \pmod{p}$ is equal to p times the number of roots in $\mathbf{F}_p^2$ of the 2×2 polynomial system below:

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \qquad (3)$$

which can be calculated in deterministic polynomial time.

The $\mathbf{F}_p$-points of $m(x_1) = 0 \cap g(x_1, x_2) = 0$



$$m(x_1) = (x_1 - \alpha_1)(x_1 - \alpha_2)(x_1 - \alpha_3)(x_1 - \alpha_4)$$

- Run the Euclidean algorithm on

$$g(x_1, x_2)(= x_2^{n_2} + m_2(x_1, x_2)), x_2^p - x_2$$

  over $\mathbf{F}_p[x_1]/(m(x_1)) = \mathbf{F}_p \oplus \mathbf{F}_p \cdots \mathbf{F}_p$
- If a zero divisor in $\mathbf{F}_p[x_1]/(m(x_1))$ is found, factor $m(x_1)$ and rerun the algorithm.
- Let n_2' be the degree of the gcd.
- The number of $\mathbf{F}_p$ solutions is $n_2' \deg(m)$.

A theorem for a general t

Theorem

The number of roots in $\mathbf{Z}/(p^t)$ of f that are lifts of the roots of $m \pmod{p}$ is equal to p^{s-1} times the number of solutions in $(\mathbf{Z}/(p^{t-s}))^2$ of the 2×2 polynomial system (in the variables (x_1, x_2)) below:

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \tag{4}$$

A dichotomy

Theorem

If $m^2 | f$ in $\mathbf{F}_p[x]$, and $t \geq 2$, then any root of m in $\mathbf{F}_p$ is either not liftable to a root in $\mathbf{Z}/(p^t)$ of f, or can be lifted to at least p roots of f in $\mathbf{Z}/(p^t)$.

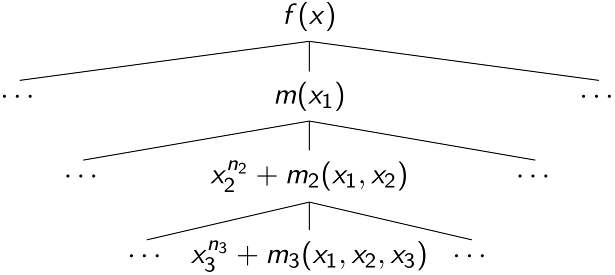
t=4

- $I_1 = (m(x_1)) \subseteq \mathbf{Z}_p[x_1]$
- $f(x_1 + px_2) = p^2(x_2^{n_2} + m_2(x_1, x_2)) \pmod{m_1(x_1), p^3}$
- $I_2 = (m(x_1), x_2^{n_2} + m_2(x_1, x_2)) \subseteq \mathbf{Z}_p[x_1, x_2]$
- Computer the gcd of $x_2^{n_2} + m_2(x_1, x_2)$ and $x_2^p - x_2$ over $\mathbf{F}_p[x_1]/(m(x_1))$

t=4

- $I_1 = (m(x_1)) \subseteq \mathbf{Z}_p[x_1]$
- $f(x_1 + px_2) = p^2(x_2^{n_2} + m_2(x_1, x_2)) \pmod{m_1(x_1), p^3}$
- $I_2 = (m(x_1), x_2^{n_2} + m_2(x_1, x_2)) \subseteq \mathbf{Z}_p[x_1, x_2]$
- Computer the gcd of $x_2^{n_2} + m_2(x_1, x_2)$ and $x_2^p - x_2$ over $\mathbf{F}_p[x_1]/(m(x_1))$
- Now assume that I_2 is zero dimensional and all roots are rational in $\mathbf{Z}_p$, and $I_2 \pmod{p}$ is radical in $\mathbf{F}_p[x_1, x_2]$.
- $f(x_1 + px_2 + p^2x_3) = p^3(x_3^{n_3} + m_3(x_1, x_2, x_3)) \pmod{I_2, p^4}$
- $I_3 = (I_2, x_3^{n_3} + m_3(x_1, x_2, x_3))$
- Computer the gcd of $x_3^{n_3} + m_3(x_1, x_2, x_3)$ and $x_3^p - x_3$ over $\mathbf{F}_p[x_1, x_2]/(I_2)$

Triangular ideals



The need for uniformity

When we split $m(x) \in \mathbf{Z}[x]$ over $\mathbf{F}_p$, and lift naively back to $\mathbf{Z}$, we keep the first digit of $\mathbf{Z}_p$-root of $m(x)$, but lose the information about the other digits.

Teichmuller lift

- $$\mathbf{Z} \hookrightarrow \mathbf{Z}_p \twoheadrightarrow \cdots \mathbf{Z}/(p^{n+1})\mathbf{Z} \twoheadrightarrow \mathbf{Z}/(p^n\mathbf{Z}) \twoheadrightarrow \cdots \mathbf{Z}/p\mathbf{Z}$$
- The Teichmuller lift of $a \in \mathbf{Z}/p\mathbf{Z}$ to $\mathbf{Z}/(p^n)\mathbf{Z}$ is a^{p^n}.
- Example: The naive lift of $3 \in \mathbf{Z}/5$ to $\mathbf{Z}/125$ is 3. The Teichmuller lift is
$$3^{125} = 3 + 3 * 5 + 2 * 5^2 \pmod{125}.$$
- The lift is independent of the representation of a in $\mathbf{Z}/p\mathbf{Z}$ because
$$(a + bp)^{p^i} = a^{p^i} \pmod{p^i}$$

Techmuller lift of polynomial roots

If $m(x) \in \mathbf{Z}[x]$ is a monic polynomial of degree $d > 0$ such that $m(x) \mod p$ splits as a product of distinct linear factors

$$m(x) \equiv \prod_{i=1}^{d}(x - \alpha_i) \mod p, \ \alpha_i \in \mathbf{Z}/p\mathbf{Z},$$

then the Teichmuller lifting of $m(x)$ mod p is defined to be the unique monic p-adic polynomial $\hat{m}(x) \in \mathbf{Z}_p[x]$ of degree d such that the p-adic roots of $\hat{m}(x)$ are exactly the Teichmuller lifting of the roots of $m(x) \mod p$. That is,

$$\hat{m}(x) = \prod_{i=1}^{d}(x - w(\alpha_i)) \in \mathbf{Z}_p[x].$$

The Teichmuller lifting $\hat{m}(x)$ can be computed without factoring $m(x) \mod p$. Using the coefficients of $m(x)$, one forms a $d \times d$ companion matrix M with integer entries such that $m(x) = \det(xI_d - M)$. Then, one can show that

$$\hat{m}(x) = \lim_{k \to \infty} \det(xI_d - M^{p^k}),\ \hat{m}(x) \equiv \det(xI_d - M^{p^t}) \mod p^t.$$

Consistency from Teichmuller lift

The roots of $\hat{I}$ over $\mathbf{Z}/p^t\mathbf{Z}$ are precisely the Teichmuller liftings mod p^t of the roots of I over $\mathbf{F}_p$. Each point $(r_1, \cdots, r_k)$ over $\mathbf{Z}/p^t\mathbf{Z}$ of $\hat{I}$ satisfies the condition $r_i^p \equiv r_i \mod p^t$.

- For any ideal I_i in the tree, there exists an integer $s \in \{i, \dots, t\}$, and if $(r_1, \dots, r_i)$ is a solution of I_i in $(\mathbf{Z}/(p^t))^i$, then $r_1 + pr_2 + \cdots + p^{i-1} r_i + p^i r$ is a solution of $f(x) \pmod{p^s}$ for any integer r. Denote the maximum such s by $s(I_i)$.
- If r is a root of $f \pmod{p^t}$, then there exists a terminal leaf I_k in the tree such that

  $$r \equiv r_1 + pr_2 + \cdots + p^{k-1} r_k \pmod{p^k}$$

  for some root $(r_1, \dots, r_k)$ of I_k.
- The root sets of ideals from distinct leaves are disjoint.

Termination conditions I

If $s(I_k) = t$ then each root of I_k in $\mathbf{Z}_p^k$ produces exactly p^{t-k} roots of f in $\mathbf{Z}/(p^t)$. We can count the number of roots in $\mathbf{F}_p^k$ of I_k, multiply it by p^{t-k}, output the number, and terminate the branch.

Termination conditions II

Let g be the polynomial satisfying

$$f(x_1 + px_2 + p^2x_3 + \cdots + p^{k-1}x_k + p^k x_{k+1})$$
$$\equiv p^{s(I_k)} g(x_1, \ldots, x_{k+1}) \pmod{I_k}.$$

If $g \pmod{p}$ is a constant polynomial in x_{k+1}, and its constant is an invertible element $\pmod{I_k, p}$, then the count on this leaf is zero.

Complexity analysis

$$
\begin{aligned}
& f(x_1 + px_2 + p^2x_3 + p^3x_4 + \cdots) \\
=& g_1(x_1) + pg_2(x_1, x_2) + p^2g_3(x_1, x_2, x_3) + \cdots \pmod{p^t}
\end{aligned}
$$

- The degree of x_2 in g_2 is less than t
- The degree of x_3 in g_3 is less than $t/2$
- The degree of x_i in g_i is less than $t/(i-1)$

The proof

- The number of children that an ideal with distance k from the root can have for is bounded from above by t/k, the degree of g.
- The complexity is determined by the size of the tree, which is bounded from above by $d \prod_{1 \leq k \leq t}(t/k) < de^t$.
- We need to compute in the ring $\mathbf{F}_p[x_1, \ldots, x_k]/I_k$. The ring is a linear space over $\mathbf{F}_p$ with dimension at most $d \prod_{1 \leq k \leq t}(t/k) < de^t$.

Open problem

- Complexity from $(d + \log p + 2^t)^{O(1)}$ to $(d + \log p + t)^{O(1)}$.

The end

Thank you !