ROOT COUNTING FOR ARBITRARY CURVES OVER PRIME POWER RINGS

CALEB ROBELLE, J. MAURICE ROJAS, AND YUYU ZHU

Abstract. Let $k, p \in \mathbb{N}$ with p prime and $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial in n variables with degree d. Counting the roots of f over $(\mathbb{Z}/\langle p^k \rangle)^n$ has applications in cryptography, integer factorization, and coding theory. We extend an algorithm for counting the number of roots of a univariate polynomial over $\mathbb{Z}/\langle p^k \rangle$ to polynomials in n variables over $(\mathbb{Z}/\langle p^k \rangle)^n$. We prove a complexity of $O(dkp^{2n})$ for our algorithm.

1. Introduction

Let $k, p \in \mathbb{N}$ with p prime and $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial in n variables with non-zero degree d. Computing the number of roots of f over $(\mathbb{Z}/\langle p^k \rangle)^n$, denoted by $N_{p,k}(f)$, has applications in cryptography, integer factorization, and coding theory. Previous work has resulted in an algorithm that can compute the number of roots of a univariate polynomial with non-zero degree over $\mathbb{Z}/\langle p^k \rangle$ in time $kd^3(k \log p)^1 + o(1) + (dk \log^2 p)^{1+o(1)}$ [1]. Less is know regarding algorithms for counting roots of multivariate polynomials over prime power rings. We extend the algorithm from [1] to arbitrary polynomials in n variables.

Theorem 1.1. *Let $f(x)(x) \in \mathbb{Z}[x_1, \ldots, x_n]$, d is the degree of f, and $k, p \in \mathbb{N}$ with p prime. Then one can compute $\#\{(x_1, \ldots, x_n) \in (\mathbb{Z}/\langle p^k \rangle)^n \mid f(x_1, \ldots, x_n) = 0\}$ in time $O(d\,k\,p^{2n})$.*

Our algorithm reduces counting over $(\mathbb{Z}/\langle p^k \rangle)^n$ to repeated counting over $(\mathbb{Z}/\langle p \rangle)^n$. We establish a bound on the number of times we have to count over $(\mathbb{Z}/\langle p \rangle)^n$ which leads to the complexity given in theorem 1.1. We will now introduce some definitions that will be necessary in our proofs later on. Let $x := (x_1, \ldots, x_n)$ denote an n-tuple, and Let $f(x) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial in n variables over the integers. Then, for $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{Z}^n$ the multi-dimensional Taylor expansion of f at ζ is

$$f(x) = \sum_{i_1, \ldots, i_n} D^{i_1 \cdots i_n} f(\zeta)(x_1 - \zeta_1)^{i_1} \ldots (x_n - \zeta_n)^{i_n}$$

where $i_1 \ldots, i_n$ are non-negative integers, and $D^{i_1 \cdots i_n} f(x)$ denotes the multi-dimensional Hasse derivative, defined as

$$D^{i_1 \cdots i_n}\left(\sum_{j_1, \ldots, j_n} c_{j_1, \ldots j_n} x_1^{j_1} \ldots x_n^{j_n}\right) := \sum_{j_1, \ldots, j_n} c_{j_1, \ldots j_n} \binom{j_1}{i_1} \ldots \binom{j_n}{i_n} x_1^{j_1 - i_1} \ldots x_n^{j_n - i_n}$$

For a prime p, $\tilde{f}$ denotes the mod p reduction of f. Let $\zeta \in (\mathbb{Z}/\langle p \rangle)^n$ be a root of $\tilde{f}$. We say that ζ is of multiplicity m if $m \geq 1$ is the largest integer such that $D^{i_1 \cdots i_n} f(\zeta) = 0 \mod p$ for all $i_1 + \ldots + i_n < m$. We call ζ a *nondegenerate root* of $\tilde{f}$ if $m = 1$, and call it a *degenerate root* otherwise. As an observation, it is immediate by definition that $m < max_i\, d_i$

Definition 1.2. *Let $f(x) \in \mathbb{Z}[x_1, \ldots, x_n]$ and fix a prime p. Let $ord_p : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ denote the usual p-adic valuation with $ord_p(p) = 1$. Then for any degenerate root $\zeta_0 \in (\mathbb{F}_p)^n$ of $\tilde{f}$ we define $s(f, \zeta_0) := ord_p(f(\zeta_0 + px))$, the largest power of p dividing $f(\zeta_0 + px)$. Next, we inductively define a set $T_{p,k}(f)$ of pairs $(f_{i,\zeta}, k_{i,\zeta})$ as follows: Set $(f_{0,0}, k_{0,0}) := (f, k)$. For $i \geq 1$ with $(f_{i-1,\mu}, k_{i-1,\mu}) \in T_{p,k}(f)$ and any degenerate root $\zeta_{i-1} \in (\mathbb{Z}/\langle p \rangle)^n$ of $\tilde{f}_{i-1,\mu}$*

Partially supported by NSF REU grant DMS-1757872.
Partially supported by NSF grants CCF-1900881 and DMS-1757872.
Partially supported by NSF grant CCF-1900881.

with $s_{i-1} := s(f_{i-1,\mu}, \zeta_{i-1}) \in \{2, \ldots, k_{i-1,\mu}\}$. $\zeta = \mu + p^{i-1}\zeta_{i-1}$ $k_{i,\zeta} = k_{i-1,\mu} - s_{i-1}$ $f_{i,\zeta}(x) := \left[\frac{1}{p^{s_{i-1}}} f_{i-1,\mu}(\zeta_{i-1} + px)\right]$ *mod* $p^{k_{i,\zeta}}$

The elements of the set $T_{p,k}(f)$ can be associated with the nodes of a finite, rooted directed tree which will assist us in performing our complexity analysis. Next, we prove the following multivariate-version of Hensel's lemma.

Lemma 1.3. *Let* $f(x) \in \mathbb{Z}[x_1, \ldots, x_n]$*. If* $f(\zeta_0) = 0$ *mod* p^j *for some* $j \geq 1$ *and* ζ_0 *mod* p *is a nondegenerate root of* $\tilde{f}$*, then there are exactly* p^{n-1} *many* $t \in (\mathbb{Z}/\langle p \rangle)^n$ *such that* $f(\zeta_0 + pt) = 0$ *mod* p^{j+1}*.*

Proof. Consider the taylor expansion of f at ζ_0 by $p^j x$,

$$f(\zeta_0 + p^j x) = f(\zeta_0) + p^j \left(\frac{\partial f}{\partial x_1}(\zeta_0) + \ldots \frac{\partial f}{\partial x_n}(\zeta_0) \right) + \sum_{i_1 + \ldots + i + n \geq 2} p^{j(i_1 + \ldots + i_n)} D^{i_1 \ldots i_n} f(\zeta_0) x_1^{i_1} \ldots x_n^{i_n}$$
$$= f(\zeta_0) + p^j \left(\frac{\partial f}{\partial x_1}(\zeta_0) + \ldots \frac{\partial f}{\partial x_n}(\zeta_0) \right) \text{ mod } p^{j+1},$$

as $j(i_1 + \ldots + i_n) \geq j + 1$ for all $i_1 + \ldots + i_n \geq 2$. Then $t := (t_1, \ldots t_n)$ is such that $(\zeta_0 + tp^j)$ is a root of f mod p^{j+1} if and only if

$$\frac{\partial f}{\partial x_1}(\zeta_0)t_1 + \ldots + \frac{\partial f}{\partial x_n}(\zeta_0)t_n = \frac{-f(\zeta_0)}{p^j} \text{ mod } p \tag{1}$$

As ζ_0 mod p is a non-degenerate root of $\tilde{f}$, then there exists an i such that $\frac{\partial f}{\partial x_i} \neq 0$ mod p. The left hand side of (1) does not vanish identically, and thus defines a nontrivial linear relation in $(\mathbb{Z}/\langle p \rangle)^n$. Fixing ζ_0, there are exactly p^{n-1} many $t \in (\mathbb{Z}/\langle p \rangle)^n$ satisfying (1). ■
For any root ζ_0 of f mod p^j and $k \geq j$ we call $\zeta \in (\mathbb{Z}/\langle p^k \rangle)^n$ a lift of ζ_0, if $f(\zeta) = 0$ mod p^k and $\zeta_0 = \zeta$ mod p^j. By inductively applying Lemma 1.3 we can obtain:

Proposition 1.4. *Let* $f(x) \in \mathbb{Z}[x_1, \ldots, x_n]$*, and* $k \geq j \geq 1$*. If* $f(\zeta_0) = 0$ *mod* p^j *and* ζ_0 *mod* p *is a non-degenerate root of* $\tilde{f}$*, then* ζ_0 *lifts to exactly* $p^{(n-1)(k-j)}$ *roots of* f *mod* p^k*.*

Lemma 1.5. *Following the notations above, suppose that* $\zeta_0 \in (\mathbb{Z}/\langle p \rangle)^n$ *is a root of* $\tilde{f}$ *of finite multiplicity* $m \geq 2$ *and that there is a* $\zeta \in (\mathbb{Z}/\langle p^k \rangle)^n$ *with* $\zeta_0 = \zeta$ *mod* p *and* $f(\zeta) = 0$ *mod* p^k*. Then* $s(f, \zeta_0) \in 2, \ldots m$*.*

Proof. Since ζ_0 is a degenerate root of $\tilde{f}$, $\frac{\partial f}{\partial x_i}(\zeta_0) = 0$ mod p for every $i \in 1 \ldots n$. Then for $\zeta = \zeta_0 + p\sigma \in (\mathbb{Z}/\langle p^k \rangle)^n$ with $\sigma := (\sigma_1, \ldots \sigma_n)$,

$$f(\zeta) = f(\zeta_0) + p\left(\frac{\partial f}{\partial x_1}(\zeta_0)\sigma_1 + \ldots + \frac{\partial f}{\partial x_n}(\zeta_0)\sigma_n \right) + \sum_{i_1 + \ldots + i + n \geq 2} p^{i_1 + \ldots + i_n} D^{i_1 \ldots i_n} f(\zeta_0) \sigma_1^{i_1} \ldots \sigma_n^{i_n} \tag{2}$$

to have solutions mod p^k we need $f(\zeta_0) = 0$ mod p^2, as the second and the third summand in equation (2) has order at least 2. Now, as ζ_0 is a degenerate root of multiplicity m, there exists and m-th Hasse derivative: $j_1 + \ldots + j_n = m$, and $D^{j_1 \cdots j_n} f(\zeta_0) \neq 0$ mod p. So $s(f, \zeta_0) \leq ord_p(p^{j_1 + \ldots + j_n} D^{j_1 \cdots j_n}) = m$. ■

2. Algorithm

We will now introduce a recurrence relation on f which counts the number of roots of f over $(\mathbb{Z}/\langle p^k\rangle)^n$.

Lemma 2.1. *Let $n_p(f)$ denote the number of non-degenerate roots of $\tilde{f}$ over $\mathbb{Z}/\langle p\rangle$. Then, provided $k \geq 2$ and $\tilde{f}$ is not identically zero mod p, we have*

$$N_{p,k}(f) = p^{(k-1)(n-1)} n_p(f) + \left(\sum_{\substack{\zeta_0 \in (\mathbb{F}_p)^n \\ s(f,\zeta_0) \geq k}} p^{n(k-1)} \right) + \sum_{\substack{\zeta_0 \in (\mathbb{F}_p)^n \\ s(f,\zeta_0) \in \{2,\ldots,k-1\}}} p^{n(s(f,\zeta_0)-1)} N_{p,k-s(f,\zeta_0)}(f_{1,\zeta_0})$$

Proof. The lifting of the non-degenerate roots of $\tilde{f}$ follows from Proposition 1.4. Now assume that $\zeta_0 \in (\mathbb{Z}/\langle p\rangle)^n$ is a degenerate root of $\tilde{f}$. Write $\zeta = \zeta_0 + p\sigma$ for $\sigma := \zeta_1 + p\zeta_2 + \ldots + p^{k-2}\zeta_{k-1} \in (\mathbb{Z}/\langle p\rangle)^n$, and let $s := s(f, \zeta_0)$. Note that by Lemma 1.5, $s \geq 2$. Then by definition, $f(\zeta) = p^s f_{1,\zeta_0}(\sigma) = 0 \bmod p^k$ regardless of choice of σ. So there are exactly $p^{n(k-1)}$ values of $\zeta \in (\mathbb{Z}/\langle p^k\rangle)^n$ such that $\zeta_0 = \zeta \bmod p$ and $f(\zeta) = 0 \bmod p^k$. If $s \leq k-1$, then ζ is a root of f if and only if

$$f_{1,\zeta_0}(\sigma) = 0 \bmod p^{k-s}. \tag{3}$$

But then $\sigma = \zeta_1 + p\zeta_2 + \ldots + p^{k-s-1}\zeta_{k-s} \bmod p^{k-s}$, i.e the rest of the base p digits $\zeta_{k-s-+1}, \ldots, \zeta_{k-1}$ do not appear in equation (3). So the number of possible lifts ζ of ζ_0 is exactly $p^{n(s-1)}$ times the number of roots $(\zeta_1 + p\zeta_2 + \ldots + p^{k-s-1}\zeta_{k-s}) \in (\mathbb{Z}/\langle p^{k-s}\rangle)^n$ of f_{1,ζ_0}. This accounts for the third summand in our formula. ∎

Below is a pseudo-code implementation of our algorithm. f is the polynomial whose roots we are counting, p is a prime number, k is a natural number, and n is the number of variables in f.

Algorithm 1 Count the number of roots of f over $\mathbb{Z}/\left\langle p^k \right\rangle$

```
countpkMult(f,p,k,n)
stack ← roots of f over F_p
while stack is not empty do
    z ← stack.pop
    g ← f(z + px)
    s ← s(f, z)
    if s = 1 and z is not degenerate then
        count ← count + p^((n−1)(k−1))
    else if s ≥ k then
        count ← count + p^(n(k−1))
    else if s ≠ 0 then
        newf ← g/p^s
        count ← count + p^(n(s−1))countpkMult(newf,p,k-s,n)
    end if
end while
return count
```

In order to count the roots of $\tilde{f}$ over $(\mathbb{Z}/\langle p\rangle)^n$ we perform a brute force search over $(\mathbb{Z}/\langle p\rangle)^n$. In the next section we will determine a bound for the number of times that we will have to search over $(\mathbb{Z}/\langle p\rangle)^n$ which will lead to the complexity stated in theorem 1.1.

3. Complexity

In order to prove the complexity given in Theorem 1.1, we introduce a tree structure on $T_{p,k}(f)$.

Definition 3.1. *We can identify the elements of $T_{p,k}(f)$ with the nodes of a labled rooted directed tree $\mathcal{T}_{p,k}(f)$ defined inductively as follows:*

1. *We set $f_{0,0} := f$, $k_{0,0} := k$ and let $(f_{0,0}, k_{0,0})$ be the label of the root node of $\mathcal{T}_{p,k}(f)$*
2. *The non-root nodes of $\mathcal{T}_{p,k}(f)$ are uniquely labelled by each $(f_{i,\zeta}, k_{i,\zeta}) \in T_{p,k}(f)$ with $i \geq 1$*
3. *There is ans edge from the node $(f_{i,\zeta}, k_{i,\zeta})$ to the node $(f_{j,\mu}, k_{j,\mu})$ if and only if $i = j-1$ and there is a degenerate root $\zeta_i \in (\mathbb{Z}/\langle p\rangle)^n$ of $\tilde{f}_{i,\zeta}$ with $s(f_{i,\zeta}, \zeta_i \in 2, \ldots, k-1)$ and $\mu = \zeta + p^j\zeta_i \in (\mathbb{Z}/\langle p^i\rangle)^n$*
4. *The label of a directed edge from node $(f_{i,\zeta}, k_{i,\zeta})$ to node $(f_{j,\mu}, k_{j,\mu})$ is $p^{s(f_{i,\zeta},(\mu-\zeta)/p^i)-1}$*

The edges of the tree are labled by powers of p in the set $p^1, \ldots, p^{k-2}$ and the labels of the nodes lie in $\mathbb{Z}[x] \times \mathbb{N}$

For any root ζ of $\tilde{f}$, let $m(\zeta)$ denote its multiplicity as previously defined.

Lemma 3.2. *(Schwartz-Zippel Lemma with Multiplicity). Fix a prime p and let $n \geq 1$, $d \geq 0$. Suppose $\tilde{f}$ has degree at most d. if $\tilde{f}$ does not vanish entirely, then we have*

$$\sum_{\zeta \in (\mathbb{Z}/\langle p\rangle)^n} m(\zeta) \leq dp^{n-1}$$

This enhanced version of the Schwartz-Zippel Lemma can be proved by induction. The complete proof can be found in [2] and [3].

Lemma 3.3. *Following the notation in definition 3.1 we claim that the following statements are true:*

1. *The depth of $\mathcal{T}_{p,k}(f)$ is at most $\lfloor \frac{k-1}{2} \rfloor$.*
2. *The degree of the root node of $\mathcal{T}_{p,k}(f)$ is at most $\lfloor \frac{dp^{n-1}}{2} \rfloor$*
3. *The degree of any non-root node of $\mathcal{T}_{p,k}(f)$ labelled $(f_{j,\mu}, k_{j,\mu})$ with parent $(f_{i,\zeta}, k_{i,\zeta})$ and $\zeta_i := (\mu-\zeta)/p^i$, is at most $\lfloor s(f_{i,\zeta}, \zeta_i)p^{n-1}/2 \rfloor$. In particular, deg $\tilde{f}_{i,\zeta} \leq s(f_{i,\zeta}, \zeta_i) \leq k_{i,\zeta} - 1 \leq k$ and $\sum_{\substack{\text{children of} \\ (f_{i,\zeta}, k_{i,\zeta})}} s((f_{i,\zeta}, \zeta_i) \leq$ deg $\tilde{f}_{i,\zeta} p^{n-1}$*
4. *$\mathcal{T}_{p,k}(f)$ has at most $\lfloor \frac{dp^{n-1}}{2} \rfloor$ nodes at depth $i \geq 1$ and thus a total of no more than $\lfloor \frac{dp^{n-1}}{2} \rfloor \lfloor \frac{k-1}{2} \rfloor + 1$ nodes.*

Proof. **Assertion (1):** By definitions 1.2 and 3.1, each $(f_{j,\mu}, k_{j,\mu})$ whose parent node is $(f_{i,\zeta}, k_{i,\zeta})$ must satisfy $2 \leq k_{i,\zeta} - k_{j,\mu} \leq k_{i,\zeta} - 1$, and $1 \leq k_{j,\mu} \leq k-2$ for all $i \geq 1$. So, considering any root to leaf path in $\mathcal{T}_{p,k}(f)$, it is clear that the depth of $\mathcal{T}_{p,k}(f)$ can be no greater than $1 + \lfloor (k-2-1)/2 \rfloor = \lfloor \frac{k-1}{2} \rfloor$.

Assertion (2): Since the multiplicity of any degenerate root of $\tilde{f}$ is at least two, by Lemma 3.2, the number of degenerate roots that $\tilde{f}$ can have is bounded above by $\lfloor dp^{n-1} \rfloor$. Every edge leaving the root node of $\mathcal{T}_{p,k}(f)$ corresponds uniquely to a degenerate root ζ_0 of $\tilde{f}$ with $s(f, \zeta_0) \in \{2, \ldots, k\}$. Therefore the root can have at most degree $\lfloor dp^{n-1} \rfloor$.
Assertion (3): Let $s := (f_{i,\zeta}, \zeta_i)$, then the degree greater than s part of the Taylor expansion $f_{i,\zeta}(\zeta_0 + px)$:

$$\sum_{i_1+\ldots+i_n>s} p^{i_1+\ldots+i_n} D^{i_1\ldots i_n} f_{i,\zeta}(\zeta_0) x_1^{i_1} \ldots x_n^{i_n}$$

has valuation greater then s. In other words, the coefficients of all the x^i terms with $|i| \geq s+1$, must be divisible by p. Thus $deg\, \tilde{f_{i,\zeta}} \leq s$. The inequality $s \leq k_{i,\zeta} - 1 \leq k - 1$ follows directly from the definition. As in Lemma 1.5, each $s(f_{i,\zeta}, \zeta_i)$ is at most the multiplicity of of the root ζ_i of $\tilde{f}_{i,\zeta}$, the final bound is obvious by again applying Lemma 7.
Assertion (4): This is immediate from Assertion (1) and Assertion (3). ■

At each node of $\mathcal{T}_{p,k}(f)$ we perform a brute force search for roots of a polynomial over $(\mathbb{Z}/\langle p \rangle)^n$ which dominates the complexity of our algorithm. Each search takes time $O(p^n)$ and number of searches we do is bounded above by $\lfloor \frac{dp^{n-1}}{2} \rfloor \lfloor \frac{k-1}{2} \rfloor + 1$ which gives our algorithm a complexity of $O(dkp^{2n})$.

4. Acknowledgements

I would like to thank Dr. Maurice Rojas for his constant support and guidance throughout my involvement in this project. I would also like to thank Joan Coronado for helping me clear several hurdles when I first began working on the project.

References

[1] Leann Kopp; Natalie Randall; J. Maurice Rojas; and Yuyu Zhu, *"Randomized Polynomial-Time Root Counting in Prime Power Rings,"* Mathematics of Computation, to appear. DOI: https://doi.org/10.1090/mcom/3431
[2] Zeev Dvir; Swastik Kopparty; Shubhangi Saraf; and Madhu Sudan, *"Extensions to the Method of Multiplicities, with applications to Kakeya Sets and Mergers,"* SIAM Journal on Computing, vol. 42, no. 6, pp. 2305-2328.
[3] Terrance Tao, *"Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory,"* EMS Surveys in Mathematical Sciences 1.1 (2014): 1-46.
[4] David Harvey, *"Computing zeta functions of arithmetic schemes,"* Proceedings of the London Mathematical Society, Volume 111, Issue 6, December 2015, Pages 1379-1401

E-mail address: `carobel1@umbc.edu`

Department of Mathematics, University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250

E-mail address: `rojas@math.tamu.edu`

Department of Mathematics, Texas A&M University, TAMU 3368, College Station, TX 77843-3368

E-mail address: `zhuyuyu@math.tamu.edu`

Department of Mathematics, Texas A&M University, TAMU 3368, College Station, TX 77843-3368