COUNTING ROOTS FOR POLYNOMIALS MODULO PRIME POWERS

QI CHENG, SHUHONG GAO, J. MAURICE ROJAS, AND DAQING WAN

Abstract. Suppose p is a prime, t is a positive integer, and $f \in \mathbb{Z}[x]$ is a univariate polynomial of degree d with coefficients of absolute value $< p^t$. We show that for any *fixed* t, we can compute the number of roots in $\mathbb{Z}/(p^t)$ of f in deterministic time $(d \log p)^{O(1)}$. This fixed parameter tractability appears to be new for $t \geq 3$. A consequence for arithmetic geometry is that we can efficiently compute Igusa zeta functions Z, for univariate polynomials, assuming the degree of Z is fixed.

1. Introduction

Given a prime p, and a univariate polynomial $f \in \mathbb{Z}[x]$ of degree d with coefficients of absolute value $< p^t$, it is a basic problem to count the roots of f in $\mathbb{Z}/(p^t)$. Aside from its natural number theoretic relevance, counting roots in $\mathbb{Z}/(p^t)$ is closely related to error correcting codes [3] and factoring polynomials over the p-adic rationals $\mathbb{Q}_p$ [8, 4, 17], and the latter problem is fundamental in polynomial-time factoring over the rationals $\mathbb{Q}$ [24], the study of prime ideals in number fields [9, Ch. 4 & 6], elliptic curve cryptography [22], the computation of zeta functions [5, 23, 30, 6], and the detection of rational points on curves [28].

There is surprisingly little written about root counting in $\mathbb{Z}/(p^t)$ for $t \geq 2$: While an algorithm for counting roots of f in $\mathbb{Z}/(p^t)$ in time polynomial in $d \log p$ has been known in the case $t = 1$ for many decades (just compute the degree of $\gcd(x^p - x, f)$ in $\mathbb{F}_p[x]$), the case $t = 2$ was just solved in 2017 by some of our students [18]. The cases $t \geq 3$, which we solve here, appeared to be completely open (see also [29, 27, 14] for further background). One complication with $t \geq 2$ is that polynomials in $(\mathbb{Z}/(p^t))[x]$ do not have unique factorization, thus obstructing a simple use of polynomial gcd.

However, certain basic facts can be established quickly. For instance, the number of roots can be exponential in $\log p$. (It is natural to use $\log p$, among other parameters, to measure the size of a polynomial since it takes $O(dt \log p)$ bits to write down f.) The quadratic polynomial $x^2 = 0$, which has roots $0, p, 2p, \ldots, (p-1)p$ in $\mathbb{Z}/(p^2)$, is such an example. This is why we focus on computing the number of roots of f, instead of listing or searching for the roots in $\mathbb{Z}/(p^t)$.

Let $N_t(f)$ denote the number of roots of f in $\mathbb{Z}/(p^t)$ (setting $N_0(f) := 1$). The *Poincare series for* f is $P_f(x) := \sum_{t=0}^{\infty} N_t(f) x^t$. Assuming $P_f(x)$ is a rational function in x, one can reasonably recover $N_t(f)$ for any t via standard generating function techniques. That $P_f(x)$ is in fact a rational function of x (even for multivariate f) was first proved in 1974 by Igusa (in the course of deriving a new class of zeta functions [19]), applying resolution of singularities. Denef found a new proof (using p-adic cell decomposition [10]) 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 [31]. Our work here thus also contributes in the direction of arithmetic geometry by significantly improving [31], where P_f is computed in the special case where f is univariate and splits completely over $\mathbb{Q}$.

To better describe our results, let us start with a naive description of the first key idea: How do roots in $\mathbb{F}_p$ lift to roots in $\mathbb{Z}/(p^t)$? A simple root of f in $\mathbb{F}_p$ can be lifted uniquely to a root in $\mathbb{Z}/(p^t)$, according to the classical Hensel's lemma (see, e.g., [15]). But a root with multiplicity ≥ 2 in $\mathbb{F}_p$ can potentially be the image (under mod p reduction) of many roots in $\mathbb{Z}/(p^t)$, as illustrated by our earlier example $f(x) = x^2$. Or a root may not be liftable at all, e.g., $x^2 + p = 0$ has no roots mod p^2, even though it has a root mod p. More to the point, if one wants a fast deterministic algorithm, one can not assume that one has access to individual roots. This is because it is still an open problem to find the roots of univariate polynomials modulo p in deterministic polynomial time (see, e.g., [11, 16]).

Partially supported by NSF grant CCF-1409020, the American Institute of Mathematics, and MSRI (through REU grant DMS-1659138).

Nevertheless, we have overcome this difficulty and found a way to keep track of how to correctly lift roots of any multiplicity.

Theorem 1.1. *There is a deterministic algorithm that computes the number of roots of f in $\mathbb{Z}/(p^t)$ in time $(d\log(p)+2^t)^{O(1)}$, where the implied constant in the big O notation is absolute.*

We prove Theorem 1.1 in Section 5. Note that Theorem 1.1 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 $\mathbb{Z}/(p^t)$. We are unaware of any earlier algorithm achieving this complexity bound, even if randomness is allowed. (A few weeks after our work here was presented at ANTS XIII, an improved complexity bound was obtained in the preprint [20].) It is worth noting that further speed-ups in terms of sparsity (e.g., polynomials with a fixed number of monomial terms) may be difficult to derive: Merely deciding the existence of roots in $\mathbb{F}_p$ or $\mathbb{Q}_p$ is already **NP**-hard (under **BPP**-reductions) with respect to the sparse encoding [1, 7]. An interesting open problem in this direction is then the following: If $c_1, c_2, c_3, a, b \in \{1, \ldots, p^2-1\}$ with $a < b < p^2 - p$, can one decide if $c_1 + c_2x^a + c_3x^b$ has a root in $\mathbb{Z}/(p^2)$ in time polynomial in $\log p$?

Our main technical innovations are the following:

- We use ideals in the ring $\mathbb{Z}_p[x_1, \ldots, x_k]$ of multivariate polynomials over the p-adic integers to keep track of the roots of f in $\mathbb{Z}/(p^t)$. More precisely, from the expansion
$$f(x_1 + px_2 + \cdots + p^k x_{k-1}) = g_1(x_1) + pg_2(x_1, x_2) + p^2 g_3(x_1, x_2, x_3) + \cdots$$
we build a collection of ideals in $\mathbb{Z}_p[x_1, \ldots, x_k]$, starting from $(g_1(x_1))$. We then decompose the ideals according to multiplicity type and rationality. This process produces a tree of ideals which ultimately encode the summands making up our final root count.
- The expansion above is not unique. (For example, adding p to g_1 and subtracting 1 from g_2 gives us another expansion.) However, we manage to keep most of our computations within $\mathbb{F}_p$, and maintain uniformity for the roots of our intermediate ideals, by using Teichmüller lifting (described in Section 4).

2. Overview of Our Approach

To count the number of roots in $\mathbb{Z}/(p^t)$ of $f \in \mathbb{Z}[x]$, our algorithm follows a divide-and-conquer strategy. First, partially factor f over $\mathbb{F}_p$ according to multiplicity and rationality as follows:

$$f = f_1 f_2^2 f_3^3 \cdots f_l^l F \pmod{p}, \tag{1}$$

where each $f_i \in \mathbb{F}_p[x]$ is monic and splits completely into a product of distinct linear factors over $\mathbb{F}_p$, the f_i are pairwise relatively prime, and F is free of linear factors in $\mathbb{F}_p[x]$. Such a factorization is classically known to be doable in deterministic polynomial-time (see, e.g., [2, pp. 170–171]). For an element $\alpha \in \mathbb{F}_p$, we call any element of its inverse image under the natural map $\mathbb{Z} \to \mathbb{F}_p$ a *lift* of α to $\mathbb{Z}$. Similarly, we can define a lift of α to $\mathbb{Z}_p$ or to $\mathbb{Z}/(p^t)$, and we can naturally extend this concept to polynomials in $\mathbb{F}_p[x]$ as well. The core of our algorithm counts how many roots of f in $\mathbb{Z}/(p^t)$ are lifts of roots of f_i in $\mathbb{F}_p$, for each i. For f_1, by Hensel's lifting lemma, the answer should be $\deg f_1$ for all t. 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 (a factor of) f_i to $\mathbb{Z}[x]$[1], for each $i \in \{2, \ldots, l\}$, to see how many lifts (to roots of f in $\mathbb{Z}/(p^t)$) are produced by the roots of the f_i in $\mathbb{F}_p$. The final count is then the summation of the results over all the f_i, since the roots of f in $\mathbb{Z}/(p^t)$ are partitioned by the roots of the f_i.

Remark 2.1. *If one instead uses a randomized factorization algorithm (e.g., [21]) to find roots of f in $\mathbb{F}_p$ in polynomial time then one may assume $\deg m = 1$, and greatly simplify the analysis of our algorithm.*

[1] All factors of all f_i are ultimately exhausted.

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

$$f(x_1 + px_2) \in (m(x_1), p).$$

If we have the refined containment $f(x_1 + px_2) \in (m(x_1), p^t)$ then for any root r_1 of m in $\mathbb{Z}/(p^t)$, and any integer $0 \le r_2 < p^{t-1}$, $f(r_1 + pr_2) = 0 \pmod{p^t}$. Thus each root of m in $\mathbb{F}_p$ lifts to exactly p^{t-1} roots of f in $\mathbb{Z}/(p^t)$, and the counting problem for (f, m) is solved. Otherwise we can efficiently find an integer $s \in \{1, \ldots, t-1\}$ and a $g \in \mathbb{Z}[x_1, x_2]$ such that

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

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

$$g(x_1, x_2) = \sum_{0 \le j < t} g_j(x_1) x_2^j.$$

Then either $g_j = 0 \pmod p$ or $\gcd(m(x_1), g_j(x_1)) = 1$ over $\mathbb{F}_p$. (Otherwise, we apply the algorithm to the pairs $(f, \gcd(m, g_j))$ and $(f, m/\gcd(m, g_j))$.)

If $s = 1$ then, since $m^2|f$ over $\mathbb{F}_p$, 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 $\mathbb{F}_p$, none of the roots of m in $\mathbb{F}_p$ can be lifted to $\mathbb{Z}/p^2$. So from now on we assume that $1 < s < t$.

2.1. The algorithm for $t = 3$.

The only interesting case is when $s = 2$.

Theorem 2.2. *The number of roots in $\mathbb{Z}/(p^3)$ of f that are lifts of roots of $m \pmod p$ is equal to p times the number of roots in $\mathbb{F}_p^2$ of the 2×2 polynomial system below:*

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

and thus the number of roots can be calculated in deterministic polynomial time.

Proof. To calculate the number of the roots, we run the Euclidean algorithm to compute the gcd of two polynomials:

$$g(x_1, x_2) \text{ and } x_2^p - x_2,$$

viewed as polynomials in x_2 over $\mathbb{F}_p[x_1]/(m(x_1))$. If we encounter a zero divisor of $\mathbb{F}_p[x_1]/(m(x_1))$ during the computation, then we have a nontrivial factorization of $m(x_1) = m_1 m_2$. We recursively count the $\mathbb{F}_p$ solutions of the equation system $m_1(x_1) = 0$ and $g(x_1, x_2) = 0$, and the system $m_2(x_1) = 0$ and $g(x_1, x_2) = 0$, output the sum of these two numbers.

Otherwise assume that the degree of the gcd (a monic polynomial in x_2) is n_2. The number of $\mathbb{F}_p$-roots of (3) equals to $n_2 \deg(m(x))$.

Since $m(x_1)$ has at most $\deg(m(x))$ many factors, and the Euclidean algorithm can be done in deterministic polynomial time, the theorem follows. ■

More details and generalization (to the Gröbner base computation) of the algorithm can be found in Section 6. Note that since $\deg_{x_2} g \le 2$ any root of m in $\mathbb{F}_p$ can be lifted to at most $2p$ roots in $\mathbb{Z}/(p^3)$.

Assume that $f \in \mathbb{Z}[x]$ is not divisible by p. The preceding ideas are formalized in the following algorithm:

Algorithm 1 The case $t = 3$

function COUNT($f(x) \in \mathbb{Z}[x],\ f(x) \neq 0 \pmod{p}$)
  Factor f as in (1).
  $count = \deg f_1$ ▷ Every root of f_1 can be lifted uniquely.
  Push $f_2, f_3, \ldots, f_l$ onto a stack S
  while $S \neq \emptyset$ **do**
    Pop a polynomial from the stack, find its lift to $\mathbb{Z}$ and denote it by m
    if $f(x_1 + px_2) = 0 \pmod{(m(x_1), p^3)}$ **then**
      $count \leftarrow count + p^2 \deg m$
    else
      Find s and g satisfying the conditions in Equation (2)
      if $\deg \gcd(m, g_j) > 0$ for some j **then**
        Push $\gcd(m, g_j)$ and $m/\gcd(m, g_j)$ onto the stack
      else
        if $s = 2$ **then**
          $count \leftarrow$ count $+p\cdot$(the number of the solutions of (3) in $\mathbb{F}_p^2$)
        end if
      end if
    end if
  end while
  return count
end function

2.2. **A Proposition for General t.** Let $r \in \mathbb{F}_p$ be any root of m, r' be the corresponding lifted root of m in $\mathbb{Z}_p$, and $a \in \mathbb{Z}_p$. We then have

$$f(r' + ap) = p^s g(r', a) \pmod{p^t}.$$

So $r' + ap$ is a root in $\mathbb{Z}/(p^t)$ for f if and only if

$$g(r', a) = 0 \pmod{p^{t-s}}.$$

The preceding argument leads us to the following result.

Proposition 2.3. *The number of roots in $\mathbb{Z}/(p^t)$ of f that are lifts of the roots of $m \pmod{p}$ is equal to p^{s-1} times the number of solutions in $(\mathbb{Z}/(p^{t-s}))^2$ of the 2×2 polynomial system (in the variables (x_1, x_2)) below:*

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

Since the root of m is liftable only when $s > 1$ (see the discussion at the beginning of the section), this yields the following dichotomy corollary:

Corollary 2.4. *If $m^2 | f$ in $\mathbb{F}_p[x]$, and $t \geq 2$, then any root of m in $\mathbb{F}_p$ is either not liftable to a root in $\mathbb{Z}/(p^t)$ of f, or can be lifted to at least p roots of f in $\mathbb{Z}/(p^t)$.*

3. From Taylor Series to Ideals

For any univariate polynomial m of degree n let us define

$$T_{m,j}(x, y) = \sum_{1 \leq i \leq j} \frac{y^{i-1}}{i!} \frac{d^i m}{(dx)^i}(x).$$

Note that if $m \in \mathbb{Z}[x]$ then $\frac{1}{i!}\frac{d^i m}{(dx)^i}(x)$, being a Taylor expansion coefficient, also lies in $\mathbb{Z}[x]$. So $T_{m,j}$ is an integral multivariate polynomial for any j. Since $T_{m,1}$ does not depend on y, we abbreviate $T_{m,1}(x,y)$ by $T_m(x)$. The following lemma follows from a simple application of Taylor expansion:

Lemma 3.1. *Let $m \in \mathbb{Z}[x]$ be a polynomial that is irreducible in $\mathbb{Z}[x]$ but splits completely, without repeated factors, into linear factors in $\mathbb{F}_p[x]$. Let $r \in \mathbb{F}_p$ be any root of m and let $r' \in \mathbb{Z}_p$ be the corresponding p-adic integer root of m. Then*

$$m(r'+ap) = apT_m(r) \pmod{p^2}.$$

To put it in another way, we have the following congruence:

$$m(x_1+px_2) \equiv px_2T_m(x_1) \pmod{m(x_1), p^2}$$

in the ring $\mathbb{Z}[x_1,x_2]$.

That one can always associate an $r \in \mathbb{F}_p$ to a root $r' \in \mathbb{Z}_p$ as above is an immediate consequence of the classical Hensel's Lemma [15]. More generally, we have the following stronger result:

Lemma 3.2. *Let $m \in \mathbb{Z}[x]$ be a polynomial that is irreducible in $\mathbb{Z}[x]$ but splits completely, without repeated factors, into linear factors in $\mathbb{F}_p[x]$. Let $r \in \mathbb{F}_p$ be any root of m, and let $r' \in \mathbb{Z}_p$ be the corresponding p-adic integer root of m. Then for any positive integer u,*

$$m(r'+ap) = apT_{m,u-1}(r',ap) \pmod{p^u}.$$

Also, in the ring $\mathbb{Z}[x_1,x_2]$, we have

$$m(x_1+px_2) = x_2pT_{m,\deg(m)}(x_1,px_2) \pmod{m(x_1)}.$$

Proof. By Taylor expansion:

$$\begin{aligned} m(r'+ap) &= m(r') + \sum_{1\le i<u} \frac{(ap)^i}{i!}\frac{d^i m}{(dx)^i}(r') \pmod{p^u} \\ &= \sum_{1\le i<u} \frac{(ap)^i}{i!}\frac{d^i m}{(dx)^i}(r') \pmod{p^u} \\ &= ap\sum_{1\le i<u} \frac{(ap)^{i-1}}{i!}\frac{d^i m}{(dx)^i}(r') \pmod{p^u} \end{aligned}$$

As observed earlier, $\frac{1}{i!}\frac{d^i m}{(dx)^i}(x)$ is an integral polynomial (even when $i > p-1$), so we are done. ■

Note that in the setting of Lemma 3.2, $T_{m,u-1}(r',ap) \equiv T_m(r') \neq 0 \pmod{p}$.

The following theorem is a generalization of the preceding lemmas to ideals.

Theorem 3.3. *Let I be a ideal in $\mathbb{Z}_p[x_1,\ldots,x_{k-1}]$. Assume that $I \pmod{p}$ is a zero-dimensional radical ideal in $\mathbb{F}_p[x_1,\ldots,x_{k-1}]$ whose zero set in $\bar{F}_p^{k-1}$ lies in $\mathbb{F}_p^{k-1}$ and lifts to $\mathbb{Z}_p$. Let $f \in \mathbb{Z}[x_1,\ldots,x_k]$ satisfy $\deg_{x_k} f < p$. If $f(r_1,\ldots,r_k) \equiv 0 \pmod{p^s}$ for every $\mathbb{Z}_p$-root $(r_1,\ldots,r_{k-1})$ of I, and every integer r_k, then there must exist a polynomial $g(x_1,\ldots,x_k)$ such that*

$$f(x_1,\ldots,x_k) \equiv p^s g(x_1,\ldots,x_k) \pmod{I}.$$

Theorem 3.3 can be proved by induction on k. Lemma 3.2 is basically the special case of Theorem 3.3 when $s=1, k=2$, $I=(m(x_1))$ and $f(x_1,x_2)=m(x_1+px_2)$. It is important in Theorem 3.3 that the ideal $I \pmod{p}$ be radical, just like in Lemma 3.2, where m is free of repeated factors over $\mathbb{F}_p$.

4. The Case $t = 4$ and the Need for Teichmüller Lifting.

Here we work on the case $t = 4$. Earlier, we saw that in the course of our algorithm, m is a lift of a factor of f_i to $\mathbb{Z}[x]$. In this section we will show the need for Teichmüller lifting. We start with

$$f(x_1 + px_2) = p^s g(x_1, x_2) \pmod{m(x_1), p^4},$$

where $1 < s < 4$. If $s = 3$ then we have the following root count, thanks to Proposition 2.3:

Theorem 4.1. *The number of roots in $\mathbb{Z}/(p^4)$ of f that are lifts of roots of $m \pmod p$ is equal to p^2 times the number of roots in $\mathbb{F}_p^2$ of the 2×2 polynomial system (in the variables (x_1, x_2)) below:*

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \tag{5}$$

which can be calculated in deterministic polynomial time.

The most interesting subcase is thus $s = 2$. From Equation (3), we first build an ideal

$$(m(x_1), g(x_1, x_2)) \pmod p \subset \mathbb{F}_p[x_1, x_2].$$

The leading coefficient of $g(x_1, x_2)$, viewed as a polynomial in x_2, is assumed to be invertible in $\mathbb{F}_p[x_1]/(m(x_1))$. So g can be made monic (as a polynomial in x_2). So we may assume that the ideal is given as

$$(m(x_1), x_2^{n_2} + f_2(x_1, x_2)),$$

where $n_2 \leq 2$ and $\deg_{x_2} f_2 < n_2$. If (r, r_2) is a root in $\mathbb{F}_p$ of the ideal, and r_1 is the lift of r to the $\mathbb{Z}_p$-root of m, then $r_1 + pr_2$ is a solution of $f \pmod{p^3}$. We compute the rational component of the ideal, and find its radical over $\mathbb{F}_p$. In the process, we may factor m in $\mathbb{F}_p[x]$. If we lift naively a factor m_1 of m over $\mathbb{F}_p$, the p-adic roots of m_1 may not be p-adic roots of m. So how do we keep the information about p-adic roots of m, a polynomial with integer coefficients?

Our solution to this problem is to use Teichmüller lifting: Recall that for an element α in the prime field $\mathbb{F}/p$, the Teichmüller lifting of α is the unique p-adic integer $w(\alpha) \in \mathbb{Z}_p$ such that $w(\alpha) \equiv \alpha \mod p$ and $w(\alpha)^p = w(\alpha)$. If a is any integer representative of α, then the Teichmüller lifting of α can be computed via

$$w(\alpha) = \lim_{k \to \infty} a^{p^k}, \ w(\alpha) \equiv a^{p^t} \mod p^t.$$

Although the full Teichmüller lifting cannot be computed in finite time, we will see momentarliy how its mod p^t reduction can be computed in deterministic polynomial time.

Let us now review how the mod p^t reduction of the Teichmüller lift can be computed in deterministic polynomial time: If $m \in \mathbb{Z}[x]$ is a monic polynomial of degree $d > 0$ such that $m \mod p$ splits as a product of distinct linear factors

$$m(x) \equiv \prod_{i=1}^{d} (x - \alpha_i) \mod p, \ \alpha_i \in \mathbb{F}_p,$$

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

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

The Teichmüller lifting $\hat{m}$ can be computed without factoring $m \mod p$: Using the coefficients of m, 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

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

This construction and computation of Teichmüller lifting of a single polynomial $m(x) \mod p$ can be extended to any triangular zero-dimensional radical ideal with only rational roots as follows.

Let I be a radical ideal of the form

$$I = (g_1(x_1), g_2(x_1, x_2), \dots, g_k(x_1, \dots, x_k)) \subset \mathbb{F}_p[x_1, \dots, x_k],$$

having only rational roots, where $g_i \in \mathbb{Z}[x_1, \dots, x_i]$ is a monic polynomial in x_i of the form

$$g_i(x_1, \dots, x_i) = x_i^{n_i} + f_i(x_1, \dots, x_i),\ n_i \geq 1$$

satisfying $\deg_{x_i} f_i < n_i$. Such a presentation of the ideal I is called *triangular form*. It is clear that such an I is a zero-dimensional complete intersection. Using the companion matrix of a polynomial, we can easily find $n_i \times n_i$ matrices $M_{i-1}(x_1, \dots, x_{i-1})$ whose entries are polynomials with coefficients in $\mathbb{Z}$ such that

$$g_i(x_1, \dots, x_i) \equiv \det(x_i I_{n_i} - M_i(x_1, \dots, x_{i-1})) \mod p,\ 1 \leq i \leq k.$$

Recursively define the polynomial $f_i \in (\mathbb{Z}/(p^t))[x_1, \dots, x_i]$ for $1 \leq i \leq k$ such that

$$f_1(x_1) \equiv \det(x_1 I_{n_1} - M_0^{p^t}) \mod p^t,$$

$$f_2(x_1, x_2) \equiv \det(x_2 I_{n_2} - M_1(x_1)^{p^t}) \mod (p^t, f_1(x_1)),$$

$$\vdots$$

$$f_k(x_1, \dots, x_k) \equiv \det(x_k I_{n_k} - M_{k-1}(x_1, \dots, x_{k-1})^{p^t}) \mod (p^t, f_1, \dots, f_{k-1}).$$

The ideal $\hat{I} = (f_1, \dots, f_k) \in (\mathbb{Z}/(p^t))[x_1, \dots, x_i]$ is called the *Teichmüller lifting mod* p^t *of* I. It is independent of the choice of the auxiliary integral matrices M_i. The roots of $\hat{I}$ over $\mathbb{Z}/p^t\mathbb{Z}$ are precisely the Teichmüller liftings mod p^t of the roots of I over $\mathbb{F}_p$. In particular, each root $(r_1, \dots, r_k)$ over $\mathbb{Z}/(p^t)$ of $\hat{I}$ satisfies the condition $r_i^p \equiv r_i \mod p^t$.

We require that m be the Teichmüller lift of (a factor of) f_i at beginning of the algorithm. Then we compute the Teichmüller lift of the ideal $(m(x_1), x_2^{n_2} + f_2(x_1, x_2))$, which is an ideal in $\mathbb{Z}_p[x_1, x_2]$. We only need it modulo p^4. Denote the ideal by I_2. For every root (r_1, r_2) of I_2, $r_1 + pr_2$ is a solution of $f(x) = 0 \pmod{p^3}$. Namely, for any integer r_3, we have $f(r_1 + pr_2 + p^2 r_3) = 0 \pmod{p^3}$, since $f(x_1 + px_2) = 0 \pmod{I_2, p^3}$.

According to Theorem 3.3, there exists a polynomial $G \in \mathbb{Z}[x_1, x_2, x_3]$ such that

$$f(x_1 + px_2 + p^2 x_3) \equiv p^3 G(x_1, x_2, x_3) \pmod{I_2},$$

since $I_2 \pmod{p}$ is radical. We have

$$f(x_1 + px_2 + p^2 x_3) = g_1(x_1, x_2) p^3 x_3 + g_0(x_1, x_2) p^3 \pmod{(I_2, p^4)}.$$

Hence if (r_1, r_2) is a root of I_2, then $r_1 + pr_2 + p^2 r_3$ is a root of $f \pmod{p^4}$ iff (r_1, r_2, r_3) satisfies

$$g_1(r_1, r_2) r_3 + g_0(r_1, r_2) = 0.$$

Assume that $g_1 \not\equiv 0 \pmod{I_2, p}$. We count the number of rational roots of

$$(I_2, g_1(x_1, x_2) x_3 + g_0(x_1, x_2)) \pmod{p} \subset \mathbb{F}_p[x_1, x_2, x_3].$$

Multiplying the resulting count by p yields the number of roots of f in $\mathbb{Z}/(p^4)$.

5. Generalization to Arbitrary $t \geq 5$

We now generalize the idea for the case of $t = 4$ to counting roots in $\mathbb{Z}/(p^t)$ of $f(x)$ when $t \geq 5$ and f is not identically 0 mod p. (We can of course divide f by p and reduce t by 1 to apply our methods here, should $p|f$.) In the algorithm, we build a tree of ideals. At level k, the ideals belong to the ring $(\mathbb{Z}/(p^t))[x_1, \ldots, x_k]$. The root of the tree (level 0) is $\{0\} \subset \mathbb{Z}/(p^t)$, the zero ideal. At the next level the ideals are of the form $(m(x_1))$, where m is taken to be the Teichmüller lift of f_i in Equation (1). We study how the roots in $\mathbb{Z}_p$ of m can be lifted to roots of f in $\mathbb{Z}/(p^t)$.

Let $I_0, I_1, \ldots, I_k$ be the ideals in a path from the root to a leaf. We require:

- $I_0 = \{0\} \subset \mathbb{Z}/(p^t)$ and $I_i \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_i]$;
- $I_i = I_{i+1} \cap \mathbb{Z}/(p^t)[x_1, \ldots, x_i]$ for all $0 \leq i \leq k-1$;
- The ideal $I_i \pmod p$ in $\mathbb{F}_p[x_1, \ldots, x_i]$ is zero-dimensional, radical, and has only rational roots for all $i \in \{0, \ldots, k\}$; furthermore, I_i can be written in the form
$$(I_{i-1}, x_i^{n_i} + f_i(x_1, \ldots, x_i)) \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_i] \tag{6}$$
where $\deg_{x_i} f_i < n_i$.
- The ideal I_i is the mod p^t reduction of the Teichmüller lift of the mod p reduction of I_i.

The basic strategy of the algorithm is to grow every branch of the tree until we reach a leaf whose ideal allows a trivial count of solutions. (In which case we output the count and terminate the branch.) Once all the branches terminate, we then compute the summation of the numbers on all the leaves as the output of the algorithm. The tree of ideals contains all necessary information about the solutions of $f \pmod{p^t}$ in the following sense:

- For any ideal I_i in the tree, there exists an integer $s \in \{i, \ldots, t\}$, such that if $(r_1, \ldots, r_i)$ is a solution of I_i in $(\mathbb{Z}/(p^t))^i$, 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 $r \in \mathbb{Z}/(p^t)$ 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 $(r_1, \ldots, r_k)(\mathbb{Z}/(p^t))^k$ of I_k.
- The root sets of ideals from distinct leaves are disjoint.

Suppose that at the end of a branch we have an ideal $I_k \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_k]$. The ideal $I_k \pmod p$ is zero-dimensional and radical in $\mathbb{F}_p[x_1, \ldots, x_k]$, with only rational roots. There are two termination conditions:

- If $s(I_k) = t$ then each root of I_k in $\mathbb{Z}_p^k$ produces exactly p^{t-k} roots of f in $\mathbb{Z}/(p^t)$. We can count the number of roots in $\mathbb{F}_p^k$ of I_k, multiply it by p^{t-k}, output the number, and terminate the branch.
- Let g be the polynomial satisfying
$$f(x_1 + px_2 + p^2x_3 + \cdots + p^{k-1}x_k + p^k x_{k+1}) \equiv p^{s(I_k)} g(x_1, \ldots, x_{k+1}) \pmod{I_k}.$$
Such a polynomial exists according to Theorem 3.3. 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.

Example 5.1. *Suppose $t = 2$. For the polynomials $x^2 = 0$ and $x^2 + p = 0$, the ideal (x_1) is a terminal leaf with count p for the former polynomial, and with count 0 for the latter.*

If none of the conditions hold then let
$$g = \sum_{j \leq t/k} g_j(x_1, \ldots, x_k) x_{k+1}^j \pmod p.$$

The degree bound t/k is due to the fact that p^{kj} divides any term in the monomial expansion of $f(x_1+px_2+\cdots+p^{k-1}x_k+p^kx_{k+1})$ that has a factor x_{k+1}^j. If any of g_j vanish at some rational root of I_k in $\mathbb{F}_p^k$ then this allows $I_k \pmod p$ to expressed as an intersection of simpler ideals. Otherwise, for the ideal $(I_k, g) \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_{k+1}]$, we compute its decomposition in $\mathbb{F}_p[x_1, \ldots, x_{k+1}]$ according to multiplicity type, find the radicals of the underlying ideals, and then lift them back to $(\mathbb{Z}/(p^t))[x_1, \ldots, x_{k+1}]$. They become the children of I_k. Note that if (I_k, g) does not have rational roots, it means that none of the roots of I_k can be lifted to solution of $f \pmod{p^{s+1}}$, and thus the branch terminates with count 0.

Proof of Theorem 1.1: If $p \le d$ then factoring polynomials over $\mathbb{F}_p$ can be done in time polynomial in d by brute force, and all the ideals in the tree are maximal. The number of children that an ideal with distance k from the root can have is bounded from above by t/k or the degree of g. (More precisely, number of non-terminal child nodes is bounded from above by $t/(2k)$.) The complexity is determined by the size of the tree, which is bounded from above by $d\prod_{k=1}^t(t/k) = d\frac{t^t}{t!} < de^t$.

If $p > d$ then our upper bound above on the tree size still holds. Since we use Teichmüller lifting during the algorithm, the tree size will never decrease. The algorithm must stop once the tree size approaches the upper bound $\lfloor de^t \rfloor$. For each tree size change, we either create new children, or split a node. We need to compute in the ring $\mathbb{F}_p[x_1, \ldots, x_k]/I_k$. Observe that in (6), we must have $n_i < t/(i-1)$ for $i \ge 2$. So the ring is a vector space over $\mathbb{F}_p$ of dimension at most $d\prod_{i=2}^t n_i = d\frac{t^{t-1}}{(t-1)!} < de^t$. Theorem follows from the fact that each tree size change involves a number of bit operations at most polynomial in $de^t \log p$. ■

6. Computer Algebra Discussion

In this section, we explain how to split ideals over $\mathbb{F}_p$ into triangular form so that the Teichmüller lift to $\mathbb{Z}_p$ can be computed. We start with the one variable case: For any given ideal $I = (f(x)) \subset \mathbb{F}_p[x]$, we can split f into the following form

$$f = g_1^{d_1} \cdots g_t^{d_t} g_0$$

where $d_1 > \cdots > d_t > 0$, the polynomials $g_1, \ldots, g_t \in \mathbb{F}_p[x]$ are separable, pairwise co-prime and each splits completely over $\mathbb{F}_p$, and g_0 has no linear factors in $\mathbb{F}_p[x]$. Such a factorization can be computed deterministically in time polynomial in $\log(p)\deg(f)$. Note that, for $1 \le i \le t$, each root of g_i has multiplicity d_i in I. This means that we can count the number of $\mathbb{F}_p$-rational roots of I, and their multiplicities, in polynomial time. Also, the rational part of I (i.e., excluding the factor g_0) is decomposed into t factors $g_1, \ldots, g_t$.

Now we show how to go from k variables to $k+1$ variables for any $k \ge 1$. Suppose $J = (g_1, \ldots, g_k) \subset \mathbb{F}_p[x_1, \ldots x_k]$ has triangular form:

$$\begin{aligned} g_1 &= x_1^{n_1} + r_1(x_1), \\ g_2 &= x_2^{n_2} + r_2(x_1, x_2), \\ &\vdots \\ g_k &= x_k^{n_k} + r_k(x_1, x_2, \ldots, x_k), \end{aligned}$$

where g_i is monic in x_i (i.e., $\deg_{x_i} r_i < n_i$) for $1 \le i \le k$. We further assume that J is radical and splitting completely over $\mathbb{F}_p$ — that is, J has $n_1 n_2 \cdots n_k$ distinct solutions in $\mathbb{F}_p^k$. In particular, $g_1(x_1)$ has n_1 distinct roots in $\mathbb{F}_p$ and, for each root $a_1 \in \mathbb{F}_p$ of g_1, there are n_2 distinct $a_2 \in \mathbb{F}_2$ such that (a_1, a_2) is a root of $g_2(x_1, x_2)$. In general, for $1 \le i < k$, each root $(a_1, \ldots, a_i) \in \mathbb{F}_p^i$ of $(g_1, \ldots, g_i)$ can be extended to n_{i+1} distinct solutions $(a_1, \ldots, a_i, a_{i+1}) \in \mathbb{F}_p^{i+1}$ of g_{i+1}. For convenience, any ideal with these properties is called a *splitting triangular ideal*.

Let $f \in \mathbb{F}_p[x_1, \ldots, x_k, x_{k+1}]$ be any nonzero polynomial which is monic in x_{k+1}, and let $I = (J, f)$ be the ideal generated by J and f in $\mathbb{F}_p[x_1, \ldots, x_k, x_{k+1}]$. We want to decompose I into splitting triangular ideals, together with their multiplicities. More precisely, we want to decompose I into the following form:

$$I = (J_1, h_1^{d_1}) \cap (J_2, h_2^{d_2}) \cap \cdots \cap (J_m, h_m^{d_m}) \cap (J_0, h_0), \tag{7}$$

where $J = J_1 \cap J_2 \cap \cdots \cap J_m \cap J_0$, $I_0 = (J_0, h_0)$ has no solutions in $\mathbb{F}_p^{k+1}$, and the ideals $I_i = (J_i, h_i) \subset \mathbb{F}_p[x_1, \ldots, x_k, x_{k+1}]$, $1 \le i \le m$, are splitting triangular ideals and are pairwise co-prime (i.e., any pair of distinct I_i have no roots in common).

To get the decomposition (7), we first compute

$$w := x_{k+1}^p - x_{k+1} \bmod G.$$

where $G = \{g_1, g_2, \ldots, g_k, f\}$ is a Gröbner basis under the lexicographical order with $x_{k+1} > x_k > \cdots > x_1$. Via the square-and-multiply method, w can be computed using $\mathrm{O}(\log(p)^3 n^2)$ bit operations where $n = \deg(f) \cdot n_1 \cdots n_k$ is the degree of the ideal I. Next we compute the Gröbner basis B of $\{g_1, g_2, \ldots, g_k, f, w\}$ (under lex order with $x_{k+1} > x_k > \cdots > x_1$), which is radical and completely splitting (hence all of its solutions are in $\mathbb{F}_p^{k+1}$ and are distinct). This mean that we get rid of the nonlinear part (J_0, h_0) in (7). The ideal (B) is now equal to the radical of the rational part of I. To decompose (B) into splitting triangular ideals, we view each polynomial in B as a polynomial in x_{k+1} with coefficient in $\mathbb{F}_p[x_1, \ldots, x_k]$. Let $t_0 = 0 < t_1 < \cdots < t_v$ be the distinct degrees of x_{k+1} among the polynomials in B. For $0 \le i \le v$, let B_i denote the set of the leading coefficient of all $g \in B$ with $\deg(g) \le t_i$. We then have a chain of ideals

$$J \subseteq (B_0) \subset (B_1) \subset \cdots \subset (B_{v-1}) \subset (B_v) = \mathbb{F}_p[x_1, \ldots, x_k]$$

with the following properties:

(i) $1 \in B_v$,
(ii) each B_i $(1 \le i \le v)$ is automatically a Gröbner basis under the lex order with $x_k > \cdots > x_1$ (one can remove some redundant polynomials from B_i),
(iii) for $0 \le i < v$, each solution of B_i that is not a solution of B_{i+1} can be extended to exactly t_{i+1} distinct solutions of I.

We can compute a Gröbner basis C_i for the colon ideal $(B_{i+1}) : (B_i)$ for $0 \le i < v$. These C_i give us the different components of J that have different numbers of solution extensions. Together with B, we get different components of (I, w). These components are completely splitting, but may not be in triangular form (as stated above). We again use the Gröbner basis structure to further decompose them until all are splitting triangular ideals (J_i, h_i). Note that computing Gröbner bases, for arbitrary ideals in $\mathbb{Q}[x_1, \ldots, x_n]$, has exponential worst-case complexity [26]. However, all of our ideals are of a special form, so their Gröbner bases can be computed deterministically in polynomial-time via the incremental method in [12] (see also [13]).

Finally, to get the multiplicity of each component (J_i, h_i), we compute the Gröbner basis for the ideal $(J_i, f, f^{(j)})$ where $f^{(j)}$ denotes the j-th derivative of f for $j = 1, 2, \ldots, \deg(f)$, until the Gröbner basis is 1. These ideals may not be in triangular form, so they may split further, but the total number of components is at most $\deg f$. Hence the total number of bit operations used is still polynomial in $\log(p) \deg(I)$.

Acknowledgements

We thank the anonymous referees for suggestions that helped improve our paper. We also gratefully acknowledge the support of the American Institute of Mathematics.

References

[1] Martíin Avendaño; Ashraf Ibrahim; J. Maurice Rojas; and Korben Rusek, *"Faster p-adic Feasibility for Certain Multivariate Sparse Polynomials,"* Journal of Symbolic Computation, special issue in honor of 60th birthday of Joachim von zur Gathen, vol. 47, no. 4, pp. 454–479 (April 2012).

[2] Eric Bach and Jeff Shallit, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[3] Jérémy Berthomieu; Grégoire Lecerf; and Guillaume Quintin, *"Polynomial root finding over local rings and application to error correcting codes,"* Applicable Algebra in Engineering, Communication, and Computing, December 2013, Volume 24, Issue 6, pp. 413–443.

[4] David G. Cantor and Daniel M. Gordon, *"Factoring polynomials over p-adic fields,"* Algorithmic number theory (Leiden, 2000), pp. 185–208, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[5] Wouter Castryck; Jan Denef; and Frederik Vercauteren, *"Computing Zeta Functions of Nondegenerate Curves,"* International Mathematics Research Papers, vol. 2006, article ID 72017, 2006.

[6] Antoine Chambert-Loir, *"Compter (rapidement) le nombre de solutions d'équations dans les corps finis,"* Séminaire Bourbaki, Vol. 2006/2007, Astérisque No. 317 (2008), Exp. No. 968, vii, pp. 39-90.

[7] Qi Cheng; Shuhong Gao; J. Maurice Rojas; and Daqing Wan, *"Sparse Univariate Polynomials with Many Roots Over a Finite Field,"* Finite Fields and their Applications, Vol. 46, July 2017, pp. 235–246.

[8] Alexander L. Chistov, *"Efficient Factoring [of] Polynomials over Local Fields and its Applications,"* in I. Satake, editor, Proc. 1990 International Congress of Mathematicians, pp. 1509–1519, Springer-Verlag, 1991.

[9] Henri Cohen, *A course in computational algebraic number theory,* Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[10] Jan Denef, *"Report on Igusa's local zeta function,"* Séminaire Bourbaki 1990/1991 (730-744) in Astérisque 201–203 (1991), pp. 359–386.

[11] Shuhong Gao, *"On the deterministic complexity of polynomial factoring"*, *Journal of Symbolic Computation*, 31 (2001), 19–36.

[12] Shuhong Gao, Yinhua Guan, and Frank Volny IV, *"A new incremental algorithm for computing Gröbner bases"*, the 35th International Symposium on Symbolic and Algebraic Computation (ISSAC), pp. 13–19, Munich, July 25–28, 2010.

[13] Shuhong Gao, Frank Volny IV, and Mingsheng Wang, *"A new framework for computing Gröbner bases"*, *Mathematics of Computation*, 85 (2016), no. 297, 449–465.

[14] Joachim von zur Gathen and Silke Hartlieb, *"Factoring Modular Polynomials,"* J. Symbolic Computation (1998) **26**, pp. 583–606.

[15] Fernando Q. Gouveêa, *p-adic Numbers,* Universitext, 2nd ed., Springer-Verlag, 2003.

[16] Bruno Grenet, Joris van der Hoeven and Grégoire Lecerf, *"Deterministic root finding over finite fields using Graeffe transforms,"* Applicable Algebra in Engineering, Communication and Computing, (2016) **27** , pp. 237–257.

[17] Jordi Guàrdia; Enric Nart; Sebastian Pauli, *"Single-factor lifting and factorization of polynomials over local fields,"* Journal of Symbolic Computation 47 (2012), pp. 1318–1346.

[18] Trajan Hammonds; Jeremy Johnson; Angela Patini; and Robert M. Walker, *"Counting Roots of Polynomials Over $\mathbb{Z}/p^2\mathbb{Z}$,"* Houston Journal of Mathematics, to appear. (Also available as Math ArXiv preprint `1708.04713` .)

[19] Jun-Ichi Igusa, *Complex powers and asymptotic expansions I: Functions of certain types*, Journal für die reine und angewandte Mathematik, 1974 (268–269): 110130.

[20] Leann Kopp; Natalie Randall; J. Maurice Rojas; and Yuyu Zhu *"Randomized Polynomial-Time Root Counting in Prime Power Rings",* Arxiv:1808.10531

[21] Kiran Kedlaya and Christopher Umans, *"Fast polynomial factorization and modular composition,"* SIAM J. Comput., 40 (2011), no. 6, pp. 1767–1802.

[22] Alan G. B. Lauder, *"Counting solutions to equations in many variables over finite fields,"* Found. Comput. Math. 4 (2004), no. 3, pp. 221–267.

[23] Alan G. B. Lauder and Daqing Wan, *"Counting points on varieties over finite fields of small characteristic,"* Algorithmic number theory: lattices, number fields, curves and cryptography, pp. 579-612, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

[24] Arjen K. Lenstra; Hendrik W. Lenstra (Jr.); Laszlo Lovász, *"Factoring polynomials with rational coefficients,"* Math. Ann. 261 (1982), no. 4, pp. 515–534.

[25] Michael Maller and Jennifer Whitehead, *"Efficient p-adic cell decomposition for univariate polynomials,"* J. Complexity *15* (1999), pp. 513-525.

[26] E. Mayr and A. Meyer, *"The Complexity of the Word Problem for Commutative Semigroups and Polynomial Ideals,"* Adv. Math. **46**, 305–329, 1982.

[27] Bernard R. McDonald, *Finite Rings with Identity,* Marcel Dekker, Inc., New York, 1974.
[28] Bjorn Poonen, *"Heuristics for the Brauer-Manin Obstruction for Curves,"* Experimental Mathematics, Volume 15, Issue 4 (2006), pp. 415–420.
[29] R. Raghavendran, *"Finite associative rings,"* Compositio Mathematica, tomme 21, no. 2 (1969), pp. 195–229.
[30] Daqing Wan, *"Algorithmic theory of zeta functions over finite fields,"* Algorithmic number theory: lattices, number fields, curves and cryptography, pp. 551–578, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.
[31] W. A. Zuniga-Galindo, *"Computing Igusa's Local Zeta Functions of Univariate Polynomials, and Linear Feedback Shift Registers,"* Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.6.

E-mail address: qcheng@ou.edu

School of Computer Science, University of Oklahoma, Norman, OK 73019

E-mail address: sgao@math.clemson.edu

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975

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

Department of Computer Science and Engineering, TAMU 3368, College Station, TX 77843-3368

E-mail address: dwan@math.uci.edu

Department of Mathematics, University of California, Irvine, CA 92697-3875