COUNTING ROOTS OF POLYNOMIALS OVER PRIME POWER RINGS

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.

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

1. Introduction

Given a prime p, and a 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 cryptological relevance, counting roots in $\mathbb{Z}/(p^t)$ is closely related to factoring polynomials over the p-adic rationals $\mathbb{Q}_p$ [4, 1, 11], and the latter problem is fundamental in polynomial-time factoring over the rationals [17], the study of prime ideals in number fields [5, Ch. 4 & 6], elliptic curve cryptography [15], the computation of zeta functions [2, 16, 20, 3], and the detection of rational points on curves [19].

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 [12]. The cases $t \geq 3$, which we solve here, appeared to be completely open. 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 take $O(t \log p)$ bits to specify a solution in $\mathbb{Z}/(p^t)$.) The quadratic polynomial $x^2 = 0$, which has roots $0, p, 2p, \cdots, (p-1)p$ 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 $P(x) := \sum_{t=0}^{\infty} N_t(f)x^t$. 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 [13]), applying resolution of singularities. Denef found a new proof (using p-adic cell decomposition [6]) 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 [21]. Our work here thus also contributes in the direction of arithmetic geometry by significantly improving [21], where it is assumed that $f(x)$ 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 $\mathbb{Z}/(p)$ lift to roots in $\mathbb{Z}/(p^t)$? A simple root of f in $\mathbb{Z}/(p)$ can be lifted uniquely to a root in $\mathbb{Z}/(p^t)$, according to the classical Hensel's lemma (see, e.g., [7]). But a root with multiplicity ≥ 2 in $\mathbb{Z}/(p)$ 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 whether there exists a deterministic polynomial time algorithm for finding roots of polynomials modulo p, see for example [8, 14].

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, $N_t(f)$, of roots in $\mathbb{Z}/(p^t)$ of f in time $(d + \log(p) + 2^t)^{O(1)}$.*

Theorem 1.1 is proved 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.

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 can then decompose the ideals according to multiplicity type and rationality. This process produces a tree of ideals which will ultimately encode the summands making up our final count of roots.

- 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 computation within $\mathbb{Z}/(p)$, and maintain uniformity for the roots of our intermediate ideals, by using Teichmuller 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, factor f over $\mathbb{F}_p$ as follows:

$$f(x) = f_1(x)f_2^2(x)f_3^3(x)...f_l^l(x)g(x) \pmod{p}, \tag{1}$$

where each f_i is a monic polynomial over $\mathbb{F}_p$ that can be split into a product of distinct linear factors over $\mathbb{F}_p$, and the f_i are pairwise relatively prime, and $g(x)$ is free of linear factors in $\mathbb{F}_p[x]$. For an element $\alpha \in \mathbb{F}_p$, we call its pre-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 $\mathbb{Z}_p$ (the p-adic integers) or to $\mathbb{Z}/(p^t)$. We extend the concept to polynomials in $\mathbb{F}_p[x]$. 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 f_i to $\mathbb{Z}[x]$, 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 f_i in $\mathbb{Z}/(p)$. The final count will be 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.

The first step of the algorithm (when applied to a pair (f, m)) is to find the maximum positive integer s such that there exists a polynomial such that

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

We may assume that

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

and for all j, either $g_j = 0$ or $\gcd(m(x_1), g_j(x_1)) = 1$ over $\mathbb{F}_p$. (Otherwise some f_i can be split further, and we restart the algorithm with new m's of smaller degrees.) Since $m|f$ over $\mathbb{F}_p[x]$, such s and g exist, and can be found efficiently.

If $s \ge t$, then each root of m in $\mathbb{F}_p$ lifts to p^{t-1} roots of f in $\mathbb{Z}/(p^t)$.

If $s < t$, let $r \in \mathbb{F}_p$ be any root of m and let r' be the corresponding lifted root of m 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 2.1. *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:*

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \tag{2}$$

There is a dichotomy corollary from the above proposition.

Corollary 2.2. *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 $\mathbb{Z}/(p^t)$.*

2.1. **The algorithm for $t = 3$.** Recall that our algorithm begins by seeking the maximal positive integer s such that there is a polynomial g satisfying

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

where $m(x) \in \mathbb{Z}[x]$ and $m^2|f$ over $\mathbb{F}_p$. If $s = 1$ then we must have

$$f = g'm^2 + pg$$

for some polynomials g' and g with $\gcd(m, g) = 1$ over $\mathbb{F}_p$. None of the roots of m in $\mathbb{F}_p$ can then be lifted.

If $s = 2$ then we have $f(x_1 + px_2) = p^2 g(x_1, x_2) \pmod{m(x_1), p^3}$.

Corollary 2.3. *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:*

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

which can be calculated in deterministic polynomial time.

Note that since the degree of x_2 in g is at most 2 , any root of m in $\mathbb{Z}/(p)$ can be lifted to at most $2p$ roots in $\mathbb{Z}/(p^3)$.

If $g(x_1, x_2)$ is linear in x_2 , then counting points for (3) is easy. The following theorem covers the other case.

Theorem 2.4. *Assume that $g(x_1, x_2) = x_2^2 + g'(x_1, x_2)$, where the degree of x_2 in g' is less than 2. Let M be the companion matrix of m. Let $X(x_1)$ be the discriminant of the second equation in (3), viewed as a polynomial in x_2. Let $D(x_2)$ be the determinant of the matrix $g(M, x_2)$. Let E be the number of solutions of $D(x_2)$ over $\mathbb{F}_p$, counting multiplicity. The number of solutions of the 2×2 polynomial system (3) is equal to $E - \deg \gcd(m, X)$.*

Proof. Suppose that over $\mathbb{F}_p$

$$m(x) = \prod_{i=1}^{c} (x - \alpha_i).$$

Then $M = V\mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_c)V^{-1}$ for some invertible matrix $V \in \mathbb{F}_p^{c \times c}$, where diag maps a vector into a diagonal matrix in the obvious way. So $g(M, x_2) = V\mathrm{diag}(g(\alpha_i, x_2), \ldots)V^{-1}$. We then have

$$D(x_2) = \prod_{i=1}^{c} g(\alpha_i, x_2).$$

If a_1 is a solution of $D(x_2)$ then there must exist a root α_i of m such that a_1 is a solution of

$$g(\alpha_i, a_1) = 0.$$

If $m|X$, then for every root α_i of m, the above equation has a solution in $\mathbb{F}_p$ with multiplicity two, so the number of solutions of (3) is $E/2(= c)$.

If $\gcd(m, X) = 1$, the equation has two distinct roots (which may not lie in $\mathbb{F}_p$), and the total number solutions of (3) is E. ■

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
$$f(x) = f_1(x)f_2^2(x)f_3^3(x)...f_n^n(x)g(x) \pmod p.$$
  $count = \deg f_1$ ▷ Every roots of f_1 can be lifted uniquely.
  Push $f_2(x), f_3(x), \cdots, f_s(x)$ into a stack
  while $S \neq \emptyset$ **do**
    Pop a polynomial from the stack, find its lift to $\mathbb{Z}$ and denote it by $m(x)$
    Find the maximum s and a polynomial $g(x_1, x_2)$ such that
$$f(x_1 + px_2) = p^s g(x_1, x_2) \pmod{(m(x_1), p^t)}.$$
    if $s = 3$ **then**
      $count \leftarrow count + p^2 \deg m$
    else
      if $s = 2$ **then**
        Let $g'(x_1)$ be the leading coefficient of $g(x_1, x_2)$, viewed as a polynomial in x_2.
        if $\gcd(m, g')$ in $\mathbb{F}_p[x]$ is nontrivial **then**
          Find the nontrivial factorization $m(x) = m_1(x)m_2(x)$ in $\mathbb{F}_p[x]$
          Push m_1 and m_2 into the stack
        else
          $count \leftarrow$ the number of the $\mathbb{F}_p$-points of (3)
        end if
      end if
    end if
  end while
  return count
end function

3. From Taylor Series to Ideals

For any polynomial $m(x)$ of degree n, 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 an irreducible polynomial that splits completely, without repeated factors, into linear factors over $\mathbb{F}_p$. 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:

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

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

That one can always associate an $r \in \mathbb{Z}/(p)$ to a root $r' \in \mathbb{Z}_p$ as above is an immediate consequence of the classical Hensel's Lemma [7]. More generally, we have the following stronger result:

Lemma 3.2. *Let $m \in \mathbb{Z}[x]$ be an irreducible polynomial that splits completely, without repeated factors, into linear factors over $\mathbb{F}_p$. 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,*

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

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

$$m(x_1 + px_2) = x_2 pT_{m,u-1}(x_1, px_2) \pmod{m(x_1), p^u}.$$

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 $\mathbb{Z}_p[x_1, x_2, \cdots, x_{k-1}]$. Assume that $I \pmod{p}$ is a zero dimensional radical ideal in $\mathbb{F}_p[x_1, x_2, \cdots, x_{k-1}]$ with only rational roots. Let $f(x_1, x_2, \cdots, x_k)$ be an integer polynomial whose degree on x_k is less than p. If $f(r_1, r_2, \cdots, r_k) \equiv 0 \pmod{p^s}$ for every $\mathbb{Z}_p$-root $(r_1, r_2, \cdots, r_{k-1})$ of I, and every integer r_k, then there must exist a polynomial $g(x_1, x_2, \cdots, x_k)$ such that*

$$f(x_1, x_2, \cdots, x_k) \equiv p^s g(x_1, x_2, \cdots, x_k) \pmod{I}.$$

The theorem can be proved by induction on s. 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 that the ideal $I \pmod{p}$ need to be radical, just like in Lemma 3.2, $m(x)$ need to be free of repeated factors over $\mathbb{F}_p$.

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

Here we work on the case $t = 4$. Earlier, we saw that $m(x)$ can be taken to be any lift of f_i to $\mathbb{Z}[x]$. In this section we will use Teichmuller lifting to get some uniformity needed by our algorithm. We start with

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

The simplest subcase is $s = 4$. Every root of $m(x)$ can be lift to p^3 many roots of f in $\mathbb{Z}/p^4$.

If $s = 3$, we have

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:*

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

which can be calculated in deterministic polynomial time.

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

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

We can assume that the leading coefficient of $g(x_1, x_2)$, viewed as a polynomial in x_2, is invertible in $\mathbb{F}_p[x_1]/(m(x_1))$, thus the polynomial can be made monic. If not, we can factor $m(x_1)$, and use its factors as new $m(x_1)$'s, and restart the algorithm with $m(x_1)$ of smaller degrees. 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 the degree of x_2 in f_2 is less than 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 $m(x)$ over $\mathbb{F}_p$. But how do we keep the information about p-adic roots of $m(x)$, a polynomial with integer coefficients?

Our solution to this problem is to use Teichmuller lifting: Recall that for an element α in the prime finite field $\mathbb{Z}/p\mathbb{Z}$, the Teichmuller 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 Teichmuller lifting of α can be computed by

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

Although the full Teichmuller lifting cannot be computed in finite time, we will see momentarily 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 Teichmuller lift can be computed in deterministic polynomial time: If $m(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $d > 0$ such that $m(x) \mod p$ splits as a product of distinct linear factors

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

then the Teichmuller lifting of $m(x) \mod p$ is defined to be the unique monic p-adic polynomial $\hat{m}(x) \in \mathbb{Z}_p[x]$ 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,

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

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

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

This construction and computation of Teichmuller 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 with only rational roots of the form

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

where $g_i(x_1, \cdots, x_i)$ is a monic polynomial in x_i of the form

$$g_i(x_1, \cdots, x_i) = x_i^{n_i} + f_i(x_1, x_2, \cdots, x_i), \ n_i \geq 1$$

satisfying that the degree in x_i of f_i is less than n_i. Such a presentation of the ideal I is called *triangular form*. It is clear that I is a zero dimensional complete intersection. Using the companion

matrix of a polynomial, we can easily find $n_i \times n_i$ matrices $M_{i-1}(x_1, ..., x_{i-1})$ whose entries are polynomials with coefficients in $\mathbb{Z}$ such that

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

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

$$f_1(x_1) \equiv \det(x_1 I_{n_1} - M_0^{p^t}) \mod p^t,$$
$$f_2(x_1, x_2) \equiv \det(x_2 I_{n_2} - M_1(x_1)^{p^t}) \mod (p^t, f_1(x_1)),$$
$$\cdots$$
$$f_k(x_1, \cdots, x_k) \equiv \det(x_k I_{n_k} - M_{k-1}(x_1, \cdots, x_{k-1})^{p^t}) \mod (p^t, f_1, \cdots, f_{k-1}).$$

The ideal $\hat{I} = (f_1, \cdots, f_k) \in \mathbb{Z}/p^t\mathbb{Z}[x_1, \cdots, x_i]$ is called the Teichmuller 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 Teichmuller liftings mod p^t of the roots of I over $\mathbb{F}_p$. Each point $(r_1, \cdots, r_k)$ over $\mathbb{Z}/p^t\mathbb{Z}$ of $\hat{I}$ satisfies the condition $r_i^p \equiv r_i \mod p^t$.

We require that $m(x)$ be the Teichmuller lift at beginning of the algorithm. Then we compute the Teichmuller lift of the ideal, 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 $f(r_1 + pr_2 + p^2 r_3) = 0 \pmod{p^3}$.

According to Theorem 3.3, there exists a polynomial $G(x_1, x_2, x_3)$ 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

$$g_1(x_1, x_2)x_3 + g_0(x_1, x_2).$$

Assume that $g_1 \neq 0$ and it does not vanish on any of the roots of $I_2 \pmod p$. We count the 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 number by p gives us the number of $\mathbb{Z}/(p^4)$ roots of f.

5. Generalization to Arbitrary $t \ge 4$

We now generalize the idea for the case of $t = 4$ to counting roots in $\mathbb{Z}/(p^t)$ of $f(x)$ when $t \ge 5$ 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 $\mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_k]$. The root of the tree (level 0) is $\{0\} \subset \mathbb{Z}/(p^t)$, the zero ideal. At the next level the ideals are $(m(x_1))$, where $m(x_1)$ is taken to be the Teichmuller lift of f_i in Equation 1. We study how the roots in $\mathbb{Z}_p$ of $m(x_1)$ can be lifted to solutions of $f(x)$ in $\mathbb{Z}/p^t$.

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

- $I_0 = \{0\} \subset \mathbb{Z}/(p^t)$ and $I_i \subset \mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_i]$;
- $I_i = I_{i+1} \cap \mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_i]$ for all $0 \le i \le k-1$;
- The ideal $I_i \pmod p$ is a zero dimensional and radical ideal with only rational roots in $\mathbb{F}_p[x_1, x_2, \cdots, x_i]$ for all $0 \le i \le k$; Furthermore, I_i can be written as

$$\begin{aligned}&(I_{i-1}, x_i^{n_i} + f_i(x_1, x_2, \cdots, x_i)) \\ &\subset \mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_i]\end{aligned} \tag{5}$$

  where degree of x_i in f_i is less than n_i.
- The ideal I_i is (the mod-p^t part of) the Teichmuller lift of $I_i \pmod p$.

The basic strategy of the algorithm is to grow every branch of the tree until we reach a leaf that whose ideal allows a trivial count of the solutions. (In which case we output the count and terminate the branch.) If all branches terminate then we compute the summation of the numbers on all the leaves as the output of the algorithm. The tree of ideals contains complete 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, such that $i \le s \le t$, and if $(r_1, r_2, \cdots, r_i)$ 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 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 $(r_1, r_2, \cdots, r_k)$ of I_k.

Suppose in the end of one branch we have an ideal $I_k \subset \mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_k]$. The ideal $I_k \pmod{p}$ is zero dimensional and radical in $\mathbb{F}_p$ with only rational roots. There are two termination conditions:

- If $s(I_k) \ge t$, then each root of I_k in $\mathbb{Z}_p^k$ can produce p^{t-k} roots of $f(x)$ 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 $g(x_1, x_2, \cdots, x_{k+1})$ be the polynomial satisfying
$$f(x_1 + px_2 + p^2x_3 + \cdots + p^{k-1}x_k + p^k x_{k+1}) \equiv p^{s(I_k)} g(x_1, x_2, \cdots, x_{k+1}) \pmod{I_k}.$$
Such a polynomial exists according to Theorem 3.3. Let $D(x_1, x_2, \cdots, x_k)$ be the discriminant of g, viewed as a polynomial in x_{k+1}. Another termination condition is that none of the roots of I_k vanishes on D. In this case, the count on this leaf is the number of rational roots of $(I_k, g) \pmod{p} \subset \mathbb{F}_p[x_1, x_2, \cdots, x_{k+1}]$.

Example 5.1. *If $I_1 = (m(x_1))$ where $m(x_1)$ is the lift to $\mathbb{Z}[x]$ of f_1 in Equation 1, then $s(I_1) = 1$, and $g(x_1, x_2) = x_2(df/dx)(x_1) \pmod{p}$ and $gcd((df/dx) \pmod{p}, f \pmod{p}) = 1$. So I_1 is a terminal leaf.* $\diamond$

If none of the conditions holds, let
$$g = \sum_{j \le t/k} g_j(x_1, x_2, \cdots, x_k) x_{k+1}^j.$$
The degree bound t/k is due to the fact that p^{kj} divides any term in the monomial expansion of $f(x_1 + px_2 + \cdots + p^{k-1}x_k + p^k x_{k+1})$ that has a factor x_{k+1}^j. If any of the non-constant g_j vanish at some rational root of I_k in $\mathbb{F}_p^k$ then this allows $I_k \pmod{p}$ to decompose. Otherwise, for the ideal $(I_k, g) \subset \mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_{k+1}]$, we compute its decomposition in $\mathbb{F}_p[x_1, x_2, \cdots, x_{k+1}]$ according to multiplicity type, find the radicals of the underlying ideals, and then lift them back to $\mathbb{Z}/(p^t)[x_1, x_2, \cdots, x_{k+1}]$. 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, and all the ideals in the tree are maximal. The number of children that I_k $(k > 1)$ can have is bounded from above by t/k, the degree of g. (More precisely, number of nonterminal children is bounded from above by $t/(2k)$.) The complexity is determined by the size of the tree, which is bounded from above by $\prod_{1 \le k \le t}(t/k) < e^t$.

If $p > d$ then we need to compute in the ring $\mathbb{F}_p[x_1, x_2, \cdots, x_k]/I_k$. Observe that in (5), we must have $n_i < t/(i-1)$ for $i \ge 2$. So the ring is a linear space over $\mathbb{F}_p$ with dimension $\prod_{2 \le k \le t} n_i < e^t$. ■

6. Computer Algebra Discussion

In this section, we explain how to split ideals over $\mathbb{F}_p$ into triangular form so that the Teichmuller 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 $f(x)$ into the following form

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

where $d_1 > \cdots > d_t > 0$, the polynomials $g_1(x), \cdots, g_t(x) \in \mathbb{F}_p[x]$ are separable, pairwise co-prime and each splits completely over $\mathbb{F}_p$, and $g_0(x)$ has no linear factors in $\mathbb{F}_p[x]$. This can be computed deterministically in time polynomial in $\log(p)\deg(f)$. Note that, for $1 \le i \le t$, each root of $g_i(x)$ 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 part of $g_0(x)$) is decomposed into t parts $g_1(x), \ldots, g_t(x)$.

Now we show how to go from k variables to $k+1$ variables for any $k \ge 1$. Suppose $J = (g_1, g_2, \ldots, g_k) \subset \mathbb{F}_p[x_1, \ldots x_k]$ has a 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., the degree of r_i in x_i is less than $< n_i$) for $1 \le i \le k$. We further assume that J is radical and completely splitting 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 $g_1(x_1)$, there are n_2 distinct $a_2 \in \mathbb{F}_2$ so that (a_1, a_2) is a solution of $g_2(x_1, x_2)$. In general, for $1 \le i < k$, each solution $(a_1, \ldots, a_i) \in \mathbb{F}_p^i$ 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:

$$I = (J_1, h_1^{d_1}) \cap (J_2, h_2^{d_2}) \cdots \cap (J_m, h_m^{d_m}) \cap (J_0, h_0), \tag{6}$$

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 (hence any distinct pair of them have no common solutions).

To get the decomposition (6), 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 (6). 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 denotes the set of the leading coefficient of all $g \in B$ with $\deg(g) \le t_i$. We have the 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's gives us the different components of J that have different number 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 Gröbner basis structure to further decompose them until all are splitting triangular ideals (J_i, h_i). Note that computing Gröbner bases is generally NP-hard. However, all of our ideals are of a special form, and their Gröbner bases can be computed deterministically in polynomial time via the incremental method in [9] (see also [10]).

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 may split further. But the total number of components is at most the degree of f. Hence the total number of bit operations used is still polynomial in $\log(p) \deg(I)$.

References

[1] 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.

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

[3] 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.

[4] 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.

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

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

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

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

[9] 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.

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

[11] 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.

[12] Trajan Hammonds; Jeremy Johnson; Angela Patini; and Robert M. Walker, *"Counting Roots of Polynomials Over $\mathbb{Z}/p^2\mathbb{Z}$,"* Math ArXiv preprint `1708.04713` .

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

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

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

[16] 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.

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

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

[19] Bjorn Poonen, *"Heuristics for the Brauer-Manin Obstruction for Curves,"* Experimental Mathematics, Volume 15, Issue 4 (2006), pp. 415–420.

[20] Daqing Wan, *"Algorithmic theory of zeta functions over finite fields,"* Algorithmic number theory: lattices, number fields, curves and cryptography, pp. 5551-578, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

[21] 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

TAMU 3368, College Station, TX 77843-3368

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

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