COUNTING ROOTS OF POLYNOMIALS OVER $\mathbb{Z}/p^2\mathbb{Z}$

TRAJAN HAMMONDS, JEREMY JOHNSON, ANGELA PATINI, AND ROBERT M. WALKER

Abstract. Until recently, the only known method of finding the roots of polynomials over prime power rings, other than fields, was brute force. One reason for this is the lack of a division algorithm, obstructing the use of greatest common divisors. Fix a prime $p \in \mathbb{Z}$ and $f \in (\mathbb{Z}/p^n\mathbb{Z})[x]$ any nonzero polynomial of degree d whose coefficients are not all divisible by p. For the case $n = 2$, we prove a new efficient algorithm to count the roots of f in $\mathbb{Z}/p^2\mathbb{Z}$ within time $(d + \text{size}(f) + \log p)^{2+o(1)}$, based on a formula conjectured by Cheng, Gao, Rojas, and Wan.

1. Introduction

Since the days of Diophantus, mathematicians have been interested in finding rational or integer solutions to polynomial equations. In the 1940s, André Weil proved the Riemann hypothesis for zeta-functions of nonsingular curves over finite fields [8]. In 1949, Weil proposed enticing conjectures that connect finding solutions to polynomials over finite fields with studying the geometry of complex algebraic varieties [9]. Weil proved these conjectures in the case of curves, yielding a bound for counting the number of points on a curve over a finite field – the **Hasse − Weil bound**:

$$|N_q - (q+1)| \leq 2g\sqrt{q},$$

where q is a prime power and N_q is the number of points over $\mathbb{F}_q^2$ on a curve with genus g. Such bounds on point counts extend to higher dimensions, per work of Weil, Deligne, Dwork, and others.

We wish to count roots over the prime power ring $\mathbb{Z}/p^k\mathbb{Z}$. That said, the usual approaches do not work since the polynomial ring $(\mathbb{Z}/p^k\mathbb{Z})[x]$ does not have unique factorization when $k \geq 2$. Thus we must sleuth for alternate approaches to count roots of nonconstant univariate polynomials over $\mathbb{Z}/p^k\mathbb{Z}$, since traditional methods for factoring and root counting over finite fields are unavailable.

As a backdrop, suppose $p \in \mathbb{Z}$ is a prime, both $m, v \in \mathbb{Z}_+$, $f \in \mathbb{Z}[x_1, \ldots x_v]$ is a nonzero polynomial with at least one coefficient being a unit modulo p, and $N_m(f)$ denotes the number of solutions to $f \equiv 0 \mod p^m$ in $(\mathbb{Z}/p^m\mathbb{Z})^v$. Consider the **Igusa Poincaré Series** [6]:

$$Q(f;t) := \sum_{m>0} N_m(f) \cdot t^m \in \mathbb{Z}[[t]].$$

Igusa's proof that $Q(f;t)$ is rational [5], solving a conjecture of Borevich and Shafarevich, relied on Hironaka's resolution of singularities [4]. Zuniga-Galindo [10] later derived an algorithm to compute $Q(f;t)$, where the dependence on v in the complexity was of order 8. While one could in principle use standard generating function tricks to then extract $N_m(f)$ for any given m, Zuniga-Galindo's algorithm only works in the case where f splits completely into linear factors over $\mathbb{Q}$ – a severe restriction. Cheng, Gao, Rojas, and Wan, during a meeting at the American Institute for Mathematics (AIM) in May 2017, found an explicit formula for $N_2(f)$ when $v = 1$, but without

2010 *Mathematics Subject Classification:* Primary: 11Y05, 11Y16, 13F20. Secondary: 11M38, 11S05, 11T06.

Keywords: algebraic complexity theory, Hensel's lemma, prime power rings, univariate polynomial root counting.

a proof or complexity bound. We prove their formula is correct and that it has near–quadratic complexity.

Going forward, given a prime $p \in \mathbb{Z}_+$, and $k \in \mathbb{Z}_+$, we view the set $\mathbb{Z}/p^k\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{p^k - 1}\}$ as a ring, and let $\pi_{p^k} : \mathbb{Z}[x] \twoheadrightarrow (\mathbb{Z}/p^k\mathbb{Z})[x]$ denote the surjective ring homomorphism defined by

$$\pi_{p^k}\left(\sum_{i=0}^{e} c_i x^{e-i}\right) := \sum_{i=0}^{e} \overline{c_i} \cdot x^{e-i},$$

where $\overline{c} := \pi_{p^k}(c) \in \mathbb{Z}/p^k\mathbb{Z}$ when $c \in \mathbb{Z}$ [3, Ch. 9]. Given a polynomial $g \in (\mathbb{Z}/p^k\mathbb{Z})[x]$, we let $\widetilde{g} \in \mathbb{Z}[x]$ denote the lift of g – read, $\pi_{p^k}(\widetilde{g}) = g$ – whose coefficients all lie between 0 and $p^k - 1$. Also, for $g \in (\mathbb{Z}/p\mathbb{Z})[x]$, we say a root of multiplicity one is simple, and degenerate otherwise.

Throughout, let $f \in \mathbb{Z}[x] \setminus \{0\}$ be a nonconstant polynomial of degree $d = \deg(f)$. Fix any prime p not dividing every coefficient of f.

Definition 1.1. Given $k \in \mathbb{Z}_+$, let $V_{p^k}(f) := \{\zeta \in \mathbb{Z}/p^k\mathbb{Z} \colon [\pi_{p^k}(f)](\zeta) = 0 \in \mathbb{Z}/p^k\mathbb{Z}\}$. Also, we set $A_k(p) := \{0, 1, \ldots, p^k - 1\} \subseteq \mathbb{Z}$.

Definition 1.2. Write f as above as $f(x) = c_0 + c_1 x + \ldots + c_d x^d$. In terms of the natural logarithm, we define the **computational size** of f to be

$$\operatorname{size}(f) = \sum_{i=0}^{d} \log(2 + |c_i|).$$

Up to a constant factor, the computational size of f is the number of bits needed to record the above monomial term expansion of f.

We now state the main result of this note.

Main Theorem 1.3. *Given f and p as above, we define polynomials $f_1, \ldots, f_\ell, g, h_1, h_2, t$, all in $(\mathbb{Z}/p\mathbb{Z})[x]$, and polynomials $\mathcal{L}_1, \ldots, \mathcal{L}_\ell \in \mathbb{Z}[x]$ as follows.*

(1) *Factor $h_1 := \pi_p(f)$ as*

$$h_1 = \pi_p(f) = f_1 f_2^2 \cdots f_\ell^\ell g \in (\mathbb{Z}/p\mathbb{Z})[x], \tag{1.0.1}$$

where
  (a) *ℓ is the maximal multiplicity of a root $r \in \mathbb{Z}/p\mathbb{Z}$ of h_1–if h_1 has any;*
  (b) *the $f_i \in (\mathbb{Z}/p\mathbb{Z})[x]$ are monic, separable, and pairwise coprime; and*
  (c) *$g \in (\mathbb{Z}/p\mathbb{Z})[x]$ has no roots in $\mathbb{Z}/p\mathbb{Z}$.*
  So the degree of f_i is the number of roots of h_1 in $\mathbb{Z}/p\mathbb{Z}$ of multiplicity i.

(2) *Writing $f_i = \prod_{j=1}^{\deg(f_i)} L_{i,j}$ as a product (possibly empty) of distinct linear terms in $(\mathbb{Z}/p\mathbb{Z})[x]$, we define $\mathcal{L}_i \in \mathbb{Z}[x]$ to be $\mathcal{L}_i = \prod_{j=1}^{\deg(f_i)} \widetilde{L_{i,j}}$. Note that $\pi_p(\mathcal{L}_i) = f_i$.*

(3) *Define the polynomials $t, h_2 \in (\mathbb{Z}/p\mathbb{Z})[x]$ via*

$$t := \pi_p\Big[\frac{1}{p}\left(f - \widetilde{g} \cdot \prod_{i=1}^{\ell} \mathcal{L}_i^i\right)\Big], \quad h_2 := \gcd(f_2 \cdots f_\ell, t).$$

Following the notation above, we have:

(A) $\#V_{p^2}(f) = \#\left\{a \in A_2(p) \colon f(a) \equiv 0 \mod p^2\right\} = \deg(f_1) + p \cdot \deg(h_2).$

(B) *The polynomials t, f_1, and h_2 can be computed deterministically in time that is polynomial in $d+\operatorname{size}(f)+\log(p)$, where $d=\deg(f)$, counting the necessary arithmetic operations.*

While the first term in formula (A) counts the roots modulo p^2 that descend to simple roots modulo p, the second term counts the roots modulo p^2 that descend to degenerate roots modulo p.

2. Preliminaries for the Proof

Throughout, p is an arbitrary prime number. We state a proposition together with two versions of Hensel's Lemma, a crucial tool for proving Theorem 1.3(A).

Proposition 2.1 (Cf., [3, Sec. 13.5, Prop. 33])**.** If $g \in (\mathbb{Z}/p\mathbb{Z})[x]$ is nonconstant, and there is an $r \in \mathbb{Z}/p\mathbb{Z}$ such that $(x-r) \mid g$ but $(x-r)^2 \nmid g$, then $g'(r) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$.

In [7, Sec. 2.6, Thm. 2.23 + paragraph between Examples 11–12], a derivation of both versions of Hensel's Lemma below is given via Taylor expansion. We note that [7, Sec. 2.6] phrases both versions of Hensel's Lemma in terms of an arbitrary integer r rather than stipulating $0 \le r \le p-1$.

Lemma 2.2 (Hensel's Lemma Version I)**.** Let $f \in \mathbb{Z}[x]$ be nonconstant, and suppose there is an $r \in A_1(p)$ with $[\pi_p(f)](\overline{r}) = 0$. If $[\pi_p(f)]'(\overline{r}) \neq 0$, then there exists an $s \in A_2(p)$ such that $[\pi_{p^2}(f)](\overline{s}) = 0$ in $\mathbb{Z}/p^2\mathbb{Z}$ and $s \equiv r \mod p$, namely, $s = \widetilde{t}$ where $t := \overline{r} - \left(\overline{f'(r)}\right)^{-1} \cdot \overline{f(r)} \in \mathbb{Z}/p^2\mathbb{Z}$. Moreover, s is unique.

Lemma 2.3 (Hensel's Lemma Version II)**.** Let $f \in \mathbb{Z}[x]$ be nonconstant, and suppose there exists r in $A_1(p)$ such that $f(r) \equiv 0 \mod p^k$, where $k \in \mathbb{Z}_+$. If $f'(r) \equiv 0 \mod p$, then

$$s \equiv r \mod p^k \implies f(s) \equiv f(r) \mod p^{k+1}.$$

That is, $f(r+tp^k) \equiv f(r) \mod p^{k+1}$ for all $0 \le t \le p-1$, indeed for all $t \in \mathbb{Z}$.

Notably, we have p roots mod p^{k+1} when $f(r) \equiv 0 \mod p^{k+1}$. Thus Lemma 2.3 can lift roots modulo p^k to roots modulo p^{k+1}. Conversely, all the roots modulo p^{k+1} are obtained this way.

3. Proof of the Main Theorem

Proof of Theorem 1.3(A). Recall that we defined polynomials $\mathcal{L}_i \in \mathbb{Z}[x]$ such that $\pi_p(\mathcal{L}_i) = f_i$. Let $U := \{\widetilde{\zeta} \in A_2(p) \colon \zeta \in V_{p^2}(f)\}$, which is the disjoint union of the two sets

$$S := \{u \in U \colon \overline{u} \in V_p(\mathcal{L}_1)\}, \text{ and } T := U \setminus S.$$

Recall that we defined $h_2 = \gcd(f_2 \cdots f_\ell, t) \in (\mathbb{Z}/p\mathbb{Z})[x]$; this monic polynomial is a product (possibly empty) of distinct linear terms. Let $D(x) \in \mathbb{Z}[x]$ be the lift of h_2 constructed analogously to the $\mathcal{L}_i$, taking the corresponding product of the $\widetilde{\bullet}$ lifts of the linear factors. To get 1.3(A), it suffices to show that as maps of sets (a) $\pi_p|_S : S \to V_p(\mathcal{L}_1)$ is a bijection, and (b) $\pi_p|_T : T \to V_p(D)$ is a p-to-1 surjection. But first, we record a lemma.

Lemma 3.1. Let $\rho \colon A_2(p) \to A_1(p)$ be the map of sets sending an element $a \in A_2(p)$ to its remainder after long division by p. Fix $r \in A_2(p)$. If $f(r) \equiv 0 \mod p^2$, then $f(\rho(r)) \equiv 0 \mod p$. Equivalently, if $\overline{r} \in V_{p^2}(f)$, then $\overline{\rho(r)} \in V_p(f)$ in terms of the bar notation preceding Definition 1.1.

Indeed, if $f(a) = \sum_{i=0}^{d} c_{d-i} a^{d-i}$ for any $a \in \mathbb{Z}$, then $f(r) \equiv \sum_{i=0}^{d} c_{d-i} (\rho(r))^{d-i} = f(\rho(r)) \bmod p$.

(a) $\pi_p|_S$ **is a bijection:** This is vacuous if S is empty, so we may assume S is non-empty. First, given any element $r \in U$, Lemma 3.1 says $\pi_p(r) = \pi_p(\rho(r)) \in V_p(f)$, meeting the first hypothesis of Hensel's Lemma 2.2. Because of our stipulations in defining the polynomials f_i in (1.0.1), Proposition 2.1 applied to $h_1 = \pi_p(f)$ implies that $\pi_p(\rho(r))$ satisfies the second hypothesis under Hensel's Lemma 2.2 if and only if $\pi_p(\rho(r)) \in V_p(\mathcal{L}_1)$. Equivalently, $r \in S$ and it will be the *unique* lift to $A_2(p)$ of $\rho(r) \in A_1(p)$ as stipulated in Hensel's Lemma 2.2, since $r \equiv \rho(r) \mod p$. Thus we may conclude that $\pi_p|_S$ is both surjective and injective, hence bijective.

Before proceeding, we record another lemma.

Lemma 3.2. Given $r \in A_1(p)$ and $\overline{r} := \pi_p(r) \in \mathbb{Z}/p\mathbb{Z}$, the following assertions are equivalent to saying $(x - \overline{r})^2 \mid h_1$:

(1) $\overline{r}$ is a degenerate root of h_1, i.e., both $f(r) \equiv 0 \bmod p$ and $f'(r) \equiv 0 \bmod p$.
(2) $(x - \overline{r}) \mid f_i$ for some unique $i \geq 2$.
(3) $(x - \overline{r}) \mid f_2 \cdot \ldots \cdot f_\ell$.

Indeed, per the stipulations on the f_i in (1.0.1), all of these assertions mean $f_1(\overline{r}) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$.

(b) $\pi_p|_T$ **is a p–to–1 surjection:** This is vacuous if T is empty, so we may assume T is non-empty. We note that $\pi_p(T) \subseteq V_p(\mathcal{L}_2 \cdots \mathcal{L}_\ell)$: given $r \in T$, Lemmas 3.1 and 3.2 apply to $\rho(r)$. Let

$$E(x) := f(x) - \widetilde{g}(x) \cdot \prod_{i=1}^{\ell} \mathcal{L}_i^i(x) \in p\mathbb{Z}[x] = \ker \pi_p.$$

Then the integer polynomial $(1/p) \cdot E(x)$ is a lift of $t(x)$. Next, since h_2 divides h_1 in $(\mathbb{Z}/p\mathbb{Z})[x]$, we note that any $r \in A_1(p)$ for which $D(r) \equiv 0 \mod p$ also satisfies $\mathcal{L}_i(r) \equiv 0 \mod p$ for some $i \geq 2$ by Lemma 3.2. Thus $f(r) \equiv E(r) \mod p^2$. Additionally, $t(\overline{r}) = 0 \in \mathbb{Z}/p\mathbb{Z}$, so $(1/p)E(r) \equiv 0 \mod p$, hence $E(r) \equiv 0 \mod p^2$. Then $f(r) \equiv 0 \mod p^2$, so Hensel's Lemma 2.3 says that r can be lifted to p *distinct* roots $s_j = r + j \cdot p \in T$ of f modulo p^2 where $0 \leq j \leq p-1$. Thus $V_p(D) \subseteq \pi_p(T)$.

To conclude that $\pi_p|_T$ is a p–to–1 surjection onto $V_p(D)$, it remains to show that conversely, given $u \in T$, $\overline{u} := \pi_p(u) \in V_p(D)$. Since $\pi_p(T) \subseteq V_p(\mathcal{L}_2 \cdots \mathcal{L}_\ell)$, we have $(f_2 \cdots f_\ell)(\overline{u}) = 0 \in \mathbb{Z}/p\mathbb{Z}$ and $(\mathcal{L}_i(u))^i \equiv 0 \mod p^2$ for some $i \geq 2$. Thus $f(u) \equiv E(u) \equiv 0 \mod p^2$: indeed, since $u \in T$, $f(u) \equiv 0 \mod p^2$. It follows that $(1/p)E(u) \equiv 0 \mod p$. Equivalently, $t(\overline{u}) = 0 \in \mathbb{Z}/p\mathbb{Z}$. We may conclude that $(x - \overline{u}) | (f_2 \cdots f_\ell)$ and $(x - \overline{u}) | t$ in $(\mathbb{Z}/p\mathbb{Z})[x]$, so by the definition of greatest common divisor $(x - \overline{u}) | h_2$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Thus $\overline{u} \in V_p(D)$. This completes the proof of claim (b), so we are done. $\square$

Corollary 3.3. *With notation as in Definition 1.1 and Theorem 1.3, exactly*

$$\#\{a \in A_1(p) \colon \overline{a} \in V_p(\mathcal{L}_2 \cdots \mathcal{L}_\ell),\ f(a) \not\equiv 0 \mod p^2\} = \deg(f_2 \cdots f_\ell) - \deg(h_2) \tag{3.0.1}$$

degenerate roots of f modulo p fail to lift to roots of f modulo p^2.

Proof. To start, continuing from the proof of Theorem 1.3(A), the right-hand side is equal to $\#V_p(\mathcal{L}_2 \cdots \mathcal{L}_\ell) - \#V_p(D)$, since $f_2 \cdots f_\ell$ and h_2 are separable. Our argument for claim (b) in the proof of Theorem 1.3(A) suffices to show that $\pi_p(T) = V_p(D) = V_p(\mathcal{L}_2 \cdots \mathcal{L}_\ell) \cap V_p[(1/p)E]$, and that the set stated in the corollary coincides with $\{a \in A_1(p) \colon \overline{a} \in V_p(\mathcal{L}_2 \cdots \mathcal{L}_\ell) - V_p[(1/p)E]\}$. $\square$

Proof of Theorem 1.3(B). First note that the decomposition (1.0.1) stated in the main theorem can be found via any classical factoring algorithm (see, e.g., [1, 2]). The gcd of polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$ of degree $\leq d$ can be computed in near linear time $O(d^{1+o(1)}(\log p)^{1+o(1)})$, per an algorithm of Knuth and Schönhage [2, Ch. 3]. Also, division with remainder for polynomials of degree $\leq d$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ takes time $O(d^{1+o(1)}\log p)$, and reduction mod p of a polynomial $f\in\mathbb{Z}[x]$ can be done in time linear in $\mathrm{size}(f)+\log p$ (see, e.g., [2, Ch. 3] and [1, Ch. 7]). Finally, note that the gcd of h_1 and x^p-x can be computed in time $O(d^{1+o(1)}(\log p)^{1+o(1)})$ by applying the binary method to the computation of $x^p \mod h_1$ (see, e.g., [1, pp. 102–104, 121–122, & 170–171]).

Going forward, we may assume that the maximal multiplicity $\ell\geq 1$. Now observe that $s_1:=\gcd(h_1,x^p-x)\in(\mathbb{Z}/p\mathbb{Z})[x]$ has the property that $V_p(h_1)=V_p(s_1)$ and s_1 has exactly $\deg(s_1)$ distinct linear factors. In particular, s_1 factors as $f_1f_2\cdots f_\ell$. Next, note that $s_2:=h_1/s_1$ factors as $g\cdot\prod_{i=1}^{\ell}f_i^{i-1}$. So then, $s_3:=\gcd(s_1,s_2)=\prod_{i=2}^{\ell}f_i$. So we can then compute f_1 as s_1/s_3 and h_2 as $\gcd(s_3,t)$ within $(\mathbb{Z}/p\mathbb{Z})[x]$. This amounts to 3 gcds and 2 divisions in $(\mathbb{Z}/p\mathbb{Z})[x]$, which is clearly within the stated complexity bound — provided we can compute t efficiently. That t can be computed efficiently is immediate since it only involves a distinct degree factorization in $(\mathbb{Z}/p\mathbb{Z})[x]$, a subtraction in $\mathbb{Z}[x]$, and a single polynomial division (by p) in $\mathbb{Z}[x]$. $\square$

To conclude, now that the main arguments have been recorded, we certainly invite readers to either: (a) generate many simple examples to better appreciate the root counting formula under Theorem 1.3(A); or (b) try implementing the algorithm in a computer algebra system they find palatable. We close the paper by providing the following example.

Example 3.4. Fix the prime $p=5$, and consider the polynomial $f\in\mathbb{Z}[x]$ defined by

$$\begin{aligned}f(x)&=x(x+2)^2(x+4)^5(x+3)^{14}(x^3+2x+1)+5(x+2)(x+4)\\&=x^{25}+66x^{24}+2073x^{23}+41225x^{22}+582597x^{21}+6225421x^{20}+52256469x^{19}\\&+353428921x^{18}+1960388179x^{17}+9032286149x^{16}+34894415443x^{15}\\&+113842103703x^{14}+315375403239x^{13}+745101000855x^{12}+1506289490631x^{11}\\&+2610867590739x^{10}+3879338706288x^{9}+4921047219861x^{8}+5275209809592x^{7}\\&+4688604525204x^{6}+3350344836816x^{5}+1835957176704x^{4}\\&+716433486336x^{3}+174686782469x^{2}+19591041054x+40.\end{aligned}$$

In particular, invoking language in the proof of Theorem 1.3(A), we have

$$h_1(x)=x(x-3)^2(x-1)^5(x-2)^{14}(x^3+2x+1)\in(\mathbb{Z}/p\mathbb{Z})[x]$$

$$f_1=x,\quad f_2=x-3,\quad f_5=x-1,\quad f_{14}=x-2,\quad g=x^3+2x+1,$$

$$t(x)=(x-3)(x-1),\quad h_2=\gcd(f_2f_5f_{14},t)=(x-3)(x-1)\in(\mathbb{Z}/5\mathbb{Z})[x].$$

Thus Theorem 1.3(A) says that

$$\#\{a\in A_2(5)\colon f(a)\equiv 0 \mod 25\}=\deg(f_1)+5\cdot\deg(h_2)=1+5(2)=11.$$

Now, $f(x)\equiv 0 \mod 5$ when $x=0,1,2,3\in A_1(5)$. The simple root $x=0$ mod 5 lifts uniquely to the root $x=15$ mod 25 per Hensel's Lemma 2.2. Among the three degenerate roots mod 5, only $x=1$ and $x=3$ satisfy $f(x)\equiv 0 \mod 25$, and Hensel's Lemma 2.3 lifts them 5–to–1. The values $x\in A_2(5)$ for which $f(x)\equiv 0 \mod 25$ are 1, 3, 6, 8, 11, 13, 15, 16, 18, 21, and 23. We note that $1\equiv 6\equiv 11\equiv 16\equiv 21 \mod 5$, while $3\equiv 8\equiv 13\equiv 18\equiv 23 \mod 5$, as indicated under our discussion of Hensel's Lemma 2.3. In line with formula 3.0.1 under Corollary 3.3, we note in passing that only $x=2$ fails to lift to a root modulo 25.

4. Acknowledgements

This research was conducted during the MSRI Undergraduate Program in Summer 2017 with Dr. Federico Ardila serving as the on-site program director; we thank the Mathematical Sciences Research Institute and Dr. Ardila for the opportunity. The first three authors would like to thank their research advisor, Dr. J. Maurice Rojas, for exceptional guidance throughout the REU program. We thank three anonymous referees for feedback that improved the quality of exposition. Indeed, we thank one referee for asking whether we could deduce Corollary 3.3 above. We thank the Alfred P. Sloan Foundation and the National Science Foundation (Grant No. DMS-1659138) for providing financial support to run MSRI-UP. We also acknowledge the partial REU support of MSRI's NSF grant (DMS-1440140), NSF grant CCF-1409020, and NSF DMS-1460766. Robert Walker was supported by a NSF GRF under Grant Number PGF-031543, NSF RTG grant 0943832, and a 2017-18 Ford Foundation Dissertation Fellowship.

References

[1] E. Bach and J. Shallit. *Algorithmic Number Theory, Vol. I: Efficient Algorithms*. MIT Press, Cambridge, MA, 1996.

[2] P. Burgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic complexity theory, with the collaboration of Thomas Lickteig, Grundlehren der Mathematischen Wissenschaften, 315*. Springer-Verlag, Berlin, Cambridge, MA, 1997.

[3] D.S. Dummit and R.M. Foote. *Abstract Algebra, 3rd Edition*. Wiley Publishing, Hoboken, NJ, 2004.

[4] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: I. *Annals of Mathematics*, 79(1):109–203, 1964.

[5] J.-I. Igusa. *Forms of higher degree, Tata Institute of Fundamental Research, Bombay*. Narosa Publishing House, New Delhi, 1978.

[6] J.-I. Igusa. *An Introduction to the Theory of Local Zeta Functions, AMS/IP Studies in Advanced Mathematics*. AMS, Providence, RI, 2000.

[7] H. Montgomery, I. Niven, and H. Zuckerman. *An Introduction to the Theory of Numbers, 5th Edition*. John Wiley and Sons, Inc. New York, 1991.

[8] A. Weil. *Sur les courbes algébriques et les variétés qui s' en déduisent*. Number 1041. Hermann, 1948.

[9] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55, 1949. pp. 497–508.

[10] W.A. Zuniga-Galindo. Computing Igusa's local zeta functions of univariate polynomials, and linear feedback shift registers. *Journal of Integer Sequences*, 6(2):3, 2003.

Department of Mathematics, Carnegie Mellon University, Pittsburgh, PA, 15289

E-mail address: thammond@andrew.cmu.edu

Department of Mathematics, Humboldt State University, Arcata, CA, 95521

E-mail address: jsj132@humboldt.edu

Department of Mathematics, University of Pennsylvania, Philadelphia, PA, 19104

E-mail address: apatini@sas.upenn.edu

Department of Mathematics, University of Michigan, Ann Arbor, MI, 48109

E-mail address: robmarsw@umich.edu