Root Sets of Polynomials Modulo Prime Powers

Davesh Maulik

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138  
E-mail: maulik@fas.harvard.edu  
Communicated by László Babai

Received February 9, 1999

A subset $R$ of the integers modulo $n$ is defined to be a root set if it is the set of roots of some polynomial. Using the Chinese Remainder Theorem, the question of finding and counting root sets modulo $n$ is reduced to finding root sets modulo a prime power. In this paper, we provide a recursive construction for root sets modulo a prime power. We use this recursion to show that the number of root sets modulo $p^k$ for fixed $k$ is a polynomial in $p$, raised to the $p^k$th power. Moreover, we show that the leading term of this polynomial is $c_k p^{k^2/4}$, where $c_k = (\frac{k}{2})^{-1}$ if $k$ is even and $c_k = (\frac{k}{2})^{-1} + (\frac{k+1}{2})^{-1}$ if $k$ is odd, thus giving an asymptotic estimate on the number of root sets for fixed $k$. Finally, we generalize these results to arbitrary Dedekind domains.

1. INTRODUCTION

A subset $R$ of $\mathbb{Z}/n\mathbb{Z}$ is a root set modulo $n$ if there is a polynomial over $\mathbb{Z}$ whose roots modulo $n$ are exactly the elements of $R$. It appears that very few existing papers discuss the nature of root sets modulo $n$. Sierpinski [3] seems to have been the first to observe that, when $n$ is a composite number other than 4, not all subsets of $\mathbb{Z}/n\mathbb{Z}$ are root sets. Chojnacka-Pniewska [4] expanded on Sierpinski’s work and introduced the notion of a root set modulo $n$. Note that $\emptyset$ and $\mathbb{Z}/n\mathbb{Z}$ are always root sets; for a prime $p$, every subset of $\mathbb{Z}/p\mathbb{Z}$ is a root set. Moreover, by the Chinese Remainder Theorem, if $a$ and $b$ are relatively prime, then $R \subseteq \mathbb{Z}/ab\mathbb{Z}$ is a root set if and only if its reductions mod $a$ and mod $b$ are also root sets. This reduces the question of finding and counting root sets to the case of prime powers.

1 Current address: 39 Hummingbird Drive, Roslyn, NY 11576.
Dearden and Metzger [2] simplified the question of finding all root sets modulo \( p^k \) with the following two results.

**Theorem 1 [2].** Let \( R \) be a root set modulo \( p^k \). For each \( j = 0, 1, 2, ..., p-1 \), there is a polynomial \( f_j \), the root set modulo \( p^k \) of which is exactly \( R_j = \{ r \in R | r \equiv j \pmod{p} \} \).

**Theorem 2 [2].** Let \( R_0, R_1, ..., R_{p-1} \) be a collection of root sets modulo \( p^k \) such that for \( 0 \leq j \leq p-1 \), the elements of \( R_j \) are all congruent to \( j \) modulo \( p \). Then \( R_0 \cup R_1 \cup R_2 \cdots \cup R_{p-1} \) is a root set modulo \( p^k \).

Using these two results, it suffices to find root sets all of whose elements are divisible by \( p \). In this paper, we shall call these \( p \)-root sets.

If \( N_{p^k} \) is the number of \( p \)-root sets modulo \( p^k \) (including the empty set), then the total number of root sets is \( T_{p^k} = (N_{p^k})^p \). Direct enumeration of cases provides formulas for \( N_{p^k} \) for small values of \( k \) (see [2]). In particular, we have that \( N_{p^1} = 2, N_{p^2} = p + 2, N_{p^3} = \frac{1}{2}(3p^2 + p + 4) \) for \( p > 2 \), and \( N_{p^4} = \frac{1}{2}(3p^4 + 4p^3 + 6p^2 + 5p + 12) \) for \( p > 3 \).

In this paper, we first recursively determine upper and lower recursive bounds on \( N_{p^k} \) which allow us to calculate the following asymptotic estimate for \( N_{p^k} \) as a function of \( p \) for fixed \( k \):

**Theorem 3.** For fixed \( k \), \( N_{p^k} \approx c_k p^{\frac{k^2}{4}+k} \) where

\[
c_k = \begin{cases} (\frac{k}{2})^{-1} & \text{if } k \text{ is even} \\ (k-1)\frac{1}{2} + (k+1)\frac{1}{2} & \text{if } k \text{ is odd}. \end{cases}
\]

Also, for \( k \geq 4 \), is \( T_{p^k} \approx c_k p^{\frac{k^2}{4}+k} \), where

\[
d_k = \begin{cases} (\frac{k-2}{2})^{-1} + (k+2)\frac{1}{2} - 2(\frac{k-4}{2})^{-1} & \text{if } k \text{ is even} \\ \frac{1}{2}(k-3)\frac{1}{2} + (k-5)\frac{1}{2} & \text{if } k \text{ is odd}. \end{cases}
\]

We then prove a precise, although somewhat unwieldy, recursive formula for \( N_{p^k} \) for \( p > k \) which allows us to prove the following theorem:

**Theorem 4.** For fixed \( k \), \( N_{p^k} \) is a polynomial function of \( p \) for \( p > k \) of degree \( \lfloor k^2/4 \rfloor \) and leading coefficient \( c_k \).
2. PRELIMINARY DEFINITIONS AND RESULTS

In order to attack the above questions, we shall apply the extremely useful notion of \textit{p-ordering}, introduced by Bhargava [1]. We begin by recalling the necessary terminology and stating some useful lemmas.

For an element \(a \in \mathbb{Z}\), let \(w_p(a)\) denote the highest power of \(p\) dividing \(a\) and \(v_p(a)\) the exponent of this highest power. Given \(S \subset \mathbb{Z}\), we obtain a \(p\)-ordering of \(S\) as follows. Choose \(a_0\) to be any element of \(S\), and for \(j = 1, 2, \ldots\) recursively define \(a_j\) to be an element of \(S\) which minimizes the highest power of \(p\) dividing \((a_j - a_0)(a_j - a_1) \cdots (a_j - a_{j-1})\). Write \(j!_S\) for \(w_p((a_j - a_0)(a_j - a_1) \cdots (a_j - a_{j-1}))\), and define \(0!_S = 1\).

\textbf{Definition 1.} Given \(S \subset \mathbb{Z}\), the sequence \([a_0, a_1, \ldots]\) defined above is a \(p\)-ordering of \(S\). The sequence \(j!_S\) is called the \textit{associated p-sequence} of our \(p\)-ordering. Given \(S \subset \mathbb{Z}_{p^k}\), we define a \(p\)-ordering of \(S\) to be a \(p\)-ordering of its preimage in \(\mathbb{Z}\). Note that under this definition, the elements of a \(p\)-ordering of \(S\) lie in the integers.

Bhargava [1] shows that the sequence \(j!_S\) is independent of our choice of \(p\)-ordering. For further properties of these "generalized factorials" \(j!_S\), see [1].

We shall also need the following definition:

\textbf{Definition 2.} The smallest \(j\) such that \(p^k | (j!)_S\) is denoted by \(\mu(S, k)\). For reasons of degeneracy, define \(\mu(\emptyset, k) = 0\).

We now establish how \(\mu(S, k)\) behaves under the partition of sets into congruence classes modulo \(p\) as in Theorem 1.

\textbf{Lemma 1.} Let \(S\) be a subset of the integers and define \(S_j = \{s \in S | s \equiv j \pmod{p}\}\) for \(j = 0, 1, \ldots, p - 1\). Then we have

\[\mu(S, k) = \sum_{j=0}^{p-1} \mu(S_j, k).\]

This also holds if \(S\) is a subset of \(\mathbb{Z}_{p^k}\).

\textbf{Proof.} It suffices to prove the first statement, since the second statement then follows from our definitions. Let \(X = [a_0, a_1, \ldots]\) be a \(p\)-ordering of \(S\). Fix \(j = 0, \ldots, p - 1\) and let \(X_j = [a_j, a_{j}, \ldots]\) be the subsequence of \(X\) whose elements are in \(S_j\). It is easy to see that \(X_j\) is a \(p\)-ordering of \(S_j\). Moreover, we have that \(\Pi_S = \Pi_{S_j}^{j!_S}\).

Let \(n = \mu(S, k)\) and \(r = \mu(S_j, k)\). We then have that \(i_r \geq n\). Since \(n!_S \geq p^k\) \(> (r - 1)!_S = i_{r-1}!_S\) and the \(j!_S\) are nondecreasing, we also know that \(i_{r-1} < n\).
Therefore exactly \( \mu(S, k) \) elements of \( S_j \) are contained in \( \{a_0, \ldots, a_{n-1}\} \). Summing over all \( j \) gives the desired result.

Bhargava [1] proves the following proposition.

**Proposition 1 [1]**. Let \( S \) be a subset of \( \mathbb{Z}/p^k\mathbb{Z} \) with \( p \)-ordering \( \{a_0, a_1, \ldots\} \) and let \( f \) be a polynomial function. Then \( f \) can be represented by a polynomial

\[ g(x) = \sum_{j=0}^{d} c_j (x - a_0) \cdots (x - a_{j-1}) \]

with \( c_j \in \mathbb{Z} \) and \( d \leq \mu(S, k) \).

In particular, using the above proposition, we obtain a bound of \( \mu(S, k) \) on the degree of the polynomial of minimal degree which generates a given root set \( S \).

3. **RECURSIVE CONSTRUCTION OF LOWER AND UPPER BOUNDS**

For the sake of the following discussion, we extend our definition of root sets slightly as follows. Given \( S \subseteq \mathbb{Z} \), we say that \( S \) is a root set modulo \( p^k \) if it is the preimage in \( \mathbb{Z} \) of some root set of \( \mathbb{Z}/p^k\mathbb{Z} \) in our original sense of the term. We extend the definition of \( p \)-root sets in an analogous manner. Note that these definitions are equivalent to saying that \( S \) is the set of zeros of some polynomial function from \( \mathbb{Z} \) to \( \mathbb{Z}/p^k\mathbb{Z} \).

In counting \( p \)-root sets modulo \( p^k \) recursively, our general approach will be as follows. Rather than count \( p \)-root sets directly, we will instead bound \( F(k, r) \), the number of \( p \)-root sets \( T \) modulo \( p^k \) such that \( \mu(T, k) = r \). Given a \( p \)-root set, we want to divide through by \( p \) and obtain a root set for some smaller modulus, which can then be broken down into \( p \)-root sets for this smaller modulus using Theorem 1. To be specific, given a \( p \)-root set in \( \mathbb{Z} / T = \{a_0, a_1, a_2, \ldots\} \), we want to show that the set \( S = \{a_0, a_1, \ldots\} \) is the preimage of a root set modulo some smaller modulus. Using the results of the previous section, rather than count the total number of \( p \)-root sets mod \( p^k \), we will instead count the total number of \( p \)-root sets with a specified value of \( \mu(S, k) \). The following pair of propositions helps construct this recursion.

**Proposition 2**. Let \( T = \{s_0, s_1, s_2, \ldots\} \subseteq \mathbb{Z} \) be a \( p \)-root set modulo \( p^k \). Then the set \( S = \{s_0, s_1, \ldots\} \) is a root set modulo \( p^{k-\mu(T, k)} \).
Proof. Note that, since \( T \) is a \( p \)-root set, we know that \((i+1)!_T \geq p \cdot i!_p\), so \( \mu(T, k) \leq k \) and it makes sense to work modulo \( p^{k-\mu(T,k)} \).

We can assume \( \{s_0, p, s_1, p, \ldots\} \) is a \( p \)-ordering of \( T \). Applying Proposition 1, we know that \( T \) is the root set of a polynomial of the form \( f(x) = \sum_{i=0}^{s} c_i (x-s_0) \cdots (x-s_{i-1}p) \), where \( p^k \mid c_i \cdot i!_T \). From the definition of \( \mu(T, k) \), we know that \((\mu(T, k) - 1)!_T \leq p^{k-1} \). Since the associated \( p \)-sequence for \( T \) always increases, we have that \( i!_T \mid p^{k-\mu(T,k) - i} \) and thus that \( p^{\mu(T,k)-i} \mid c_i \) for \( i \leq \mu(T, k) \).

Consider the polynomial \( \tilde{f}(x) = \sum_{i=0}^{s} c_i \cdot p^{i-\mu(T,k)}(x-s_0) \cdots (x-s_{i-1}) \), whose coefficients are integers by our above reasoning. Then it is clear that, for \( a \in \mathbb{Z} \), \( \tilde{f}(a) \equiv 0 \pmod{p^{k-\mu(T,k)}} \) if and only if \( f(ap) \equiv 0 \pmod{p^k} \), so that \( \mathcal{S} \) is the root set of \( \tilde{f} \) modulo \( p^{k-\mu(T,k)} \).

We can also lift root sets in the other direction.

Proposition 3. Let \( \mathcal{S} = \{a_0, a_1, \ldots\} \subset \mathbb{Z} \) be a root set modulo \( p^k \). Then the set \( T = \{a_0^0, a_1^0, \ldots\} \) is a \( p \)-root set modulo \( p^{k+\mu(S,k)} \).

Proof. Let \( \{s_0, s_1, \ldots \} \) be a \( p \)-ordering of \( \mathcal{S} \). Once again, using Proposition 1, we can assume that \( \mathcal{S} \) is generated by a polynomial of the form 
\[
\tilde{f}(x) = \sum_{i=0}^{s} c_i (x-s_0) \cdots (x-s_{i-1}).
\]
Consider the polynomial \( f(x) = \sum_{i=0}^{\mu(S,k)} c_i \cdot p^{i-\mu(S,k)}(x-s_0) \cdots (x-s_{i-1})p \). By Theorem 1, in order to show that \( T \) is a root set modulo \( p^{k+\mu(S,k)} \), it suffices to show that \( T \) is exactly the set of roots of \( f \) which are multiples of \( p \). Clearly every element of \( T \) is a root of \( f \). Given an integer \( rp \) which is a root of \( f \), we have that
\[
f(rp) = \sum_{i=0}^{\mu(S,k)} c_i \cdot p^{i-\mu(S,k)}(r-s_0) \cdots (r-s_{i-1}) \equiv 0 \pmod{p^{k+\mu(S,k)}}
\]
or, equivalently, that \( f(r) \equiv 0 \pmod{p^k} \) and \( r \in \mathcal{S} \).

It turns out that, in lifting from \( \mathcal{S} \) to \( T \) in Proposition 3, the \( \mu \)-value for these two sets and their respective moduli is preserved. Indeed, it is easy to verify that \( \mu(T) = \mu(T, k + \mu(S, k)) = \mu(S, k) \). Unfortunately, the \( \mu \)-value is not preserved in the other direction. That is, in our operation from \( T \) to \( \mathcal{S} \) of Proposition 2, it is not necessarily the case that \( \mu(T, k) = \mu(S, k - \mu(T, k)) \). For instance, in the case where \( \mu(T, k) = p^{k-1} \), we would have that \( \mu(S, k - \mu(T, k)) = p^{k-\mu(T,k)} \) so that \( \mu(S, k - \mu(T, k)) = \mu(T, k) - 1 \).

Since \( \mu(T, k) \mid p^k \), we do know that \( \mu(S, k - \mu(T, k)) \leq \mu(T, k) \). If it were true that \( \mu \)-value was preserved in both directions, then Propositions 2 and 3 would have given a one-to-one correspondence between \( p \)-root sets \( T \mod p^k \) with \( \mu(T, k) = r \) and root sets \( S \mod p^{k-\mu(T,k)} \) with \( \mu(S, k-r) = r \) which, in turn, would have allowed us to calculate a precise recursion for
Proposition 4. Assume $p > k$. Consider the function $f(k, r)$, where $f(k, k) = 1$, $f(k, 0) = 1$, $f(k, r) = 0$ for $r > k$, and otherwise

$$f(k, r) = \sum_{r_0 + \cdots + r_{p-1} = r} \left( \prod_{i=0}^{p-1} f(k-r, r_i) \right).$$

Then $f(k, r) \leq F(k, r)$ for all $k$ and $r$.

Proof. In the cases when $r > k$ or $r = 0$, the statement is clear. For example, if $r = 0$, then $F(k, r) = 1$ since only the empty set has $\mu(S, k - r) = 0$. Also, if we consider the set $X$ of multiples of $p$, we can see that $X$ is the root set of the polynomial $p^{k-r}X$ and satisfies $\mu(X, k) = k$, since $p > k$. We thus have that $F(k, k) \geq 1 = f(k, k)$.

We now proceed by induction on $k$. For all cases, we know from our previous discussion that each root set $S$ modulo $p^{k-r}$ with $\mu(S, k - r) = r$ lifts to a unique $p$-root set $T$ modulo $p^k$ such that $\mu(T, k) = r$. Therefore, $F(k, r)$ is at least the number of root sets $S$ modulo $p^{k-r}$ such that $\mu(S, k - r) = r$.

Now, since we can assume $k > r$, we know from Lemma 1 that each $S$, when decomposed according to congruence classes mod $p$, gives root sets $S_0, S_1, \ldots, S_{p-1}$ modulo $p^{k-r}$ such that $\sum_{i=0}^{p-1} \mu(S_i, k - r) = r$. If we add $-i$ to each element of $S_i$, we get $p$-root sets $T_0, \ldots, T_{p-1}$ mod $p^{k-r}$ which also satisfy $\sum_{i=0}^{p-1} \mu(T_i, k - r) = r$. Conversely, given $p$-root sets $T_0, \ldots, T_{p-1}$ mod $p^{k-r}$ such that $\sum_{i=0}^{p-1} \mu(T_i, k - r) = r$, we can add $i$ to each $T_i$ to get a root set $S_i$ mod $p^{k-r}$. Then the set $S = \bigcup_{i=0}^{p-1} S_i$, which is a root set by Theorem 2, satisfies $\mu(S, k - r) = r$. Thus, we have a bijection between root sets $S$ modulo $p^{k-r}$ with $\mu(S, k - r) = r$ and $p$-tuples of $p$-root sets $(T_0, \ldots, T_{p-1})$ mod $p^{k-r}$ whose $\mu$ values add up to $r$. In order to count these $p$-tuples of $p$-root sets, we simply look at all partitions of $r$ into $p$ ordered parts $r_0, \ldots, r_{p-1}$ and count $p$-tuples $\{ T_i \}$ of $p$-root sets mod $p^{k-r}$ such that $\mu(T_i, k - r) = r_i$. This is just $\prod_{i=0}^{p-1} F(k-r, r_i)$. Thus, if $G(k, r)$ is the number of these root sets $S$ modulo $p^k$ such that $\mu(S, k) = r$, then we have that

$$F(k, r) \geq G(k-r, r) = \sum_{r_0 + \cdots + r_{p-1} = r} \left( \prod_{i=0}^{p-1} F(k-r, r_i) \right) \geq \sum_{r_0 + \cdots + r_{p-1} = r} \left( \prod_{i=0}^{p-1} f(k-r, r_i) \right) = f(k, r).$$
In the case that \( p \leq k \), we can still achieve a recursive lower bound using the above approach. However, since complications arise in setting the initial conditions and only the \( p > k \) result is relevant to our future discussion, we have omitted the result.

The reason we are only able to get a lower bound in the above proof is that, in our recursion, we overlook \( p \)-root sets \( T \mod p^k \) for which the corresponding root set \( S \mod p^{k-r} \) of Proposition 2 does not satisfy \( \mu(S, k - \mu(T, k)) = \mu(T, k) \). Fortunately, the following lemma gives us a way of bounding the number of these exceptions.

**Lemma 2.** Given \( S \) and \( T \) as in Proposition 2 such that \( s = \mu(S, k - \mu(T, k)) < \mu(T, k) = r \), then \( T \) is also a \( p \)-root set modulo \( p^{k-r+s} \) and \( \mu(T, k - r + s) = \mu(S, k - r) \). Moreover, the number of such \( p \)-root sets \( T \) is at most \( \sum_{s=0}^{r-1} F(k-r+s,s) \).

**Proof.** This is a direct application of Proposition 3, since the elements of \( T \) are just the elements of \( S \) multiplied by \( p \). The second statement follows from summing over all possible values of \( \mu(S, k - r) \).

If we insert this upper bound on our exceptions into our recursion from Proposition 3, we obtain the following upper bound on \( F(k, r) \).

**Proposition 5.** Consider the function \( g(k, r) \) where \( g(k, k) = 1 \), \( g(k, 0) = 1 \), \( g(k, r) = 0 \) for \( r > k \), and otherwise

\[
g(k, r) = \sum_{s=0}^{r-1} g(k-r+s,s) + \sum_{r_0 + \cdots + r_{r-1} = r} \left( \prod_{i=0}^{p-1} g(k-r_i, r_i) \right).
\]

Then \( g(k, r) \geq F(k, r) \) for all \( k \) and \( r \).

**Proof.** As before, the base cases are easily verified for \( r = 0 \) and \( r > k \). As for \( r = k \), it suffices to show that there is at most one \( p \)-root set \( T \mod p^k \) such that \( \mu(T, k) = k \). Indeed, if \( S \) is the set obtained by dividing each element of \( T \) by \( p \), then we know from Proposition 2 that \( S \) must be a root set mod \( p^{k-r} = 1 \) and therefore that \( S = \mathbb{Z} \) and \( T = p\mathbb{Z} \).

We now proceed by induction. Given \( k \) and \( r \), the number of \( p \)-root sets \( T \mod p^r \) for which \( \mu(T, k) = r \) and \( \mu(S, k - r) < r \) is bounded by Lemma 2 and the number of \( p \)-root sets \( T \) for which \( \mu(S, k - r) = r \) is exactly \( \sum_{r_0 + \cdots + r_{r-1} = r} (\prod_{i=0}^{r-1} F(k-r_i)) \), as shown in the proof of Proposition 4. We thus have that
\[ F(k, r) \leq \sum_{s=0}^{r-1} F(k-r+s, s) + \sum_{r_0 + \cdots + r_{p-1} = r} \left( \prod_{i=0}^{p-1} F(k-r_i) \right) \]
\[ \leq \sum_{s=0}^{r-1} g(k-r+s, s) + \sum_{r_0 + \cdots + r_{p-1} = r} \left( \prod_{i=0}^{p-1} g(k-r_i) \right) \]
\[ = g(k, r). \]

For primes \( p > k \geq r \), our recursions for \( f(k, r) \) and \( g(k, r) \), which sum over partitions of \( r \) into at most \( p \) parts, will include all possible partitions of \( r \) into nonzero parts. That is, given an ordered partition \( r = r_1 + \cdots + r_a \) into nonzero parts, there will be \( \binom{r}{a} \) partitions of \( r \) into \( p \) ordered parts with the same sequence of nonzero terms. As a result, instead of summing over partitions of \( r \) into \( p \) parts, we can instead sum over all partitions of \( r \) and insert the appropriate binomial coefficient factor. This fact leads to the following proposition.

**Proposition 6.** For fixed \( k \) and \( r \), \( f(k, r) \) and \( g(k, r) \) are polynomials in \( p \) for \( p > k \). The leading term of both these polynomials, for \( r < k \), is \( \frac{r!}{r^r} \). If \( k - r > 1 \) then for both polynomials, the term of second highest degree is \( -\frac{1}{(k-r)^2} \).

**Proof.** We prove both statements by induction on \( k \). For the first statement, the base cases are clear for \( r = 0 \) or \( r > k \). If \( r = k \), then, since \( p > k \), we know that \( f(k, k) = 1 \) and thus, is a polynomial function of \( p \).

Since we are assuming \( p > k \), we can rewrite our recursion for \( f(k, r) \) in terms of all partitions of \( r \) as

\[ f(k, r) = \sum_{r_0 + \cdots + r_a = r} \binom{a}{p} \prod_{i=0}^{a} f(k-r_i). \] (1)

Since the summation itself is independent of \( p \) and \( \binom{a}{p} \) is a polynomial in \( p \), we are done by induction. A similar proof works for \( g(k, r) \).

For the second statement, we once again consider \( f(k, r) \) first. Since \( f(1, 1) = 1 \) and \( f(k, 1) = pf(k-1, 1) \), we know that \( f(k, 1) = p^{k-1} \) for \( k \geq 1 \).

If we look at the term in Eq. (1) corresponding to the partition \( r = 1 + \cdots + 1 \), we see that this contributes a term of \( \binom{r}{a} p^{r(r-1)/2} \) to the sum. This has leading term \( \frac{1}{2} p^{r(r-1)/2} \). For any other partition \( r = r_1 + \cdots + r_a \) into nonzero parts, we know that \( a < r \). Applying our inductive hypothesis, the degree of each factor in the product in (1) is \( r_j(k-r_j) \), while \( \binom{a}{p} \) has degree \( a \). The degree of the term corresponding to this partition is then

\[ a + \sum_{i=0}^{a} r_i(k-r_i) < rk - r^2 - \sum_{i=0}^{a} (r_i^2 - r_i) < r(k-r) \] (2)
since \( r_1^2 - r_1 > 0 \) unless \( r_1 = 0 \) or 1. Thus, every term in the recursion other than that corresponding to \( r = 1 + \cdots + 1 \) contributes a term of degree less than \( r(k-r)-1 \), since both inequalities are strict. A similar proof works for \( g(k,r) \). Since \( g(k,1) = p^{k-1} + \cdots + 1 \), only the partition \( r = 1 + \cdots + 1 \) contributes a term of degree \( r(k-r) \). Also, the sum \( \sum_{r=0}^{r-1} g(k-r+s,s) \) contributes terms of degree at most \( (k-r)s < (k-r)r \), which gives the desired result.

Finally, for the last statement, we know that the term of \( \binom{r}{s} p^{(k-r-1)s} \) corresponding to the partition \( r = 1 + \cdots + 1 \) contributes a term of \(-\frac{1}{s r \cdots r} p^{(k-r)-1} \). Moreover, since both inequalities in (2) are strict, every other partition contributes a term of degree less than \( r(k-r)-1 \), which gives us the result for \( f \). For \( g \), we must also consider the terms arising from \( g(k-r+s,s) \); however, by the second statement, we know that the largest degree from such a term is \((k-r)s \leq (k-r)(r-1) < (k-r)r - 1 \) since \( k-r > 1 \). This concludes the proof.

**Corollary 1.** For fixed \( k \) and for \( p \geq k \), \( \sum_{r=0}^{k} f(k, r) \) and \( \sum_{r=0}^{k} g(k, r) \) are polynomial functions of \( p \) whose leading term is \( c_k p^{(k^2/4)-1} \) where \( c_k \) is defined as in Theorem 3. If \( k > 4 \) then the coefficient of \( p^{(k^2/4)-1} \) is \( d_k \), where \( d_k \) is defined as in Theorem 3.

**Proof.** This follows immediately from Proposition 6 since \( r(k-r) \) achieves maximum value \( \lfloor k^2/4 \rfloor \) when \( r = k/2 \) if \( k \) is even and when \( r = (k - 1)/2 \) or \((k+1)/2 \) if \( k \) is odd.

As for the second statement, we first consider \( \sum_{r=0}^{k} f(k, r) \). If \( k \) is even, there are three values of \( r \) which contribute a nonzero coefficient to \( p^{(k^2/4)-1} \). First, there is the second term of \( f(k, k/2) \); there is also the leading term of \( f(k, k/2-1) \) and \( f(k, k/2+1) \). If \( k \) is odd, only the second terms of \( f(k, (k-1)/2) \) and \( f(k, (k+1)/2) \) contribute nonzero coefficients, since for all other \( r \), the degree of \( f(k, r) \) is at most \( \lfloor k^2/4 \rfloor - 2 \).

We may now proceed to our proof of Theorem 3.

**Proof.** The first statement of Theorem 3, an asymptotic for \( N_{\alpha} \), is an immediate consequence of the above corollary, since we have that \( \sum_{r=0}^{k} f(k, r) \) and \( \sum_{r=0}^{k} g(k, r) \) are, respectively, lower and upper bounds for \( N_{\alpha} = \sum_{r=0}^{k} F(k, r) \).

Using the fact from elementary calculus that \( \lim_{x \to \infty} (1 + b_1/x + \cdots + b_n/x^n) = e^{b_1} \), we know that both \( (\sum_{r=0}^{k} f(k, r))^p \) and \( (\sum_{r=0}^{k} g(k, r))^p \) are asymptotic to \( e^{p^{k^2/4}} \cdot (cp^{k^2/4})^p \), where \( c \) is a constant. We apply Corollary 1 to calculate the second coefficients for both polynomials. Since \( (\sum_{r=0}^{k} f(k, r))^p \) and \( (\sum_{r=0}^{k} g(k, r))^p \) are, respectively, lower and upper bounds for on the total number of root sets mod \( p^k \), we are done.
4. A PRECISE RECURSION

Throughout this section, we assume that $p > k$.

In order to calculate $N_{p^s}$ exactly, we complicate our recursion to avoid the shortcomings of our previous approach. We first begin with some additional definitions.

**Definition 3.** Let $T \subset \mathbb{Z}$ be a non-empty $p$-root set mod $p^k$ for $k > 0$ with $r = \mu(T, k)$. Then we define the set $A(T) = \{i \mid i | T = p^{k-r} + i\}$. We also define the functions $\sigma(T) = \text{the smallest element of } A(T)$ and $\tau(T) = \text{the size of } A(T)$. In the case when $A(T) = \emptyset$, that is, when $\tau(T) = 0$, we define $\sigma(T) = r$. In the degenerate case when $T = \emptyset$, we define $\sigma(T) = \tau(T) = 0$ for convenience.

The motivation for all this additional terminology is that, when we divide $T$ through by $p$ as in Proposition 2 to get a root set $S$ mod $p^{k-r}$, the elements of $A(T)$ are precisely those $i$ for which $l!_S = p^{k-r}$. In particular, we have that $\sigma(T) = \mu(S, k-r)$. This property will be extremely useful in our recursion. Finally, let $H(k, r, s, t)$ be the number of $p$-root sets $T$ mod $p^k$ such that $\mu(T, k) = r$, $\sigma(T) = s$, and $\tau(T) = t$. We now proceed to calculate a precise recursion for $H(k, r, s, t)$.

We begin by establishing some basic facts about our newly defined terms.

**Lemma 3.** Let $T$ be a $p$-root set mod $p^k$ such that $\mu(T, k) = r$, $\sigma(T) = s$, and $\tau(T) = t$. If $r \notin A(T)$ then $l \notin A(T)$ for $l \geq r$. Also, if $r-1 \notin A(T)$ then $l \notin A(T)$ for $l < r-1$. Last, if $t \neq 0$, then $A(T) = \{s, \ldots, s + t - 1\}$.

**Proof.** First, as we have noted before, since $T$ is a $p$-root set, its associated $p$-sequence is strictly increasing, that is $v_p(i + 1)!_T \geq 1 + v_p(i)!_T$ for all $i$. If $r \notin A(T)$ then, since $v_p(r!_T) \geq k$, we must have $v_p(r!_T) > k$ and, using the above reasoning, that $v_p(l!_T) > k + l - r$ for all $l \geq r$. Similarly, if $r-1 \notin A(T)$ then, since $v_p((r-1)!_T) \leq k - 1$, we must have $v_p((r-1)!_T) < k - 1$ and therefore that $v_p(l!_T) < k + l - r$ for all $l < r-1$.

As for the last statement, we first show that if $a, h \in A(T)$, then $\{a, a + 1, \ldots, b\} \subset A(T)$. Since $a, b \in A(T)$, we know that $a!_T = p^{k-a} + \cdots$ and $b!_T = p^{k-b}$. For every $i \geq a$, we have that $v_p(i!_T) \geq (k + a - r) + (t-a)$; similarly, for every $i < b$, we have that $v_p(i!_T) \leq (k + b - r) - (b-i)$. Therefore, for all $a \leq i \leq b$, we conclude that $i \in A(T)$. Since $A(T)$ contains $t$ elements and $s$ is its smallest element, we must have that $s + t - 1$ is its largest element and that $\{s, \ldots, s + t - 1\} = A(T)$.
As a direct consequence of the above lemma, we know that if either \( s > r \) or \( s + t < r \), then \( H(k, r, s, t) = 0 \). We will also need the following general lemma.

**Lemma 4.** Let \( T \in \mathbb{Z} \) be a \( p \)-root set mod \( p^k \) with \( p \)-ordering \( \{a_0, p, a_1, p, \ldots\} \) and suppose that \( c'_T = p^m \) and \( (c+d)!_T = p^{m+d} \) for some integers \( c, d \) and \( m \). Then the \( d+1 \) integers \( a_i, \ldots, a_{i+d} \) are in distinct congruence classes mod \( p \).

**Proof.** As in the proof of Lemma 3, we use the fact that the associated \( p \)-sequence of \( T \) is strictly increasing. As before, since \( c'_T = p^m \) and \( (c+d)!_T = p^{m+d} \), we know that \( (c+i)!_T = p^{m+i} \) for all \( 0 \leq i \leq d \). Moreover, for any such \( i \), we have that

\[
m + i = v_p \left( (a_{i+1} + p - a_{i+1-1}p) \cdots (a_{i+1} + p - a_{i}p) \prod_{j=0}^{i-1} (a_{i+1} + p - a_{j}p) \right)
\]

\[
= v_p \left( p^i (a_{i+1} + p - a_{i+1-1}p) \cdots (a_{i+1} + p - a_{i}p) \prod_{j=0}^{i-1} (a_{i+1} + p - a_{j}p) \right)
\]

\[
= i + v_p((a_{i+1} + p - a_{i+1-1}p) \cdots (a_{i+1} + p - a_{i}p)) + v_p \left( \prod_{j=0}^{i-1} (a_{i+1} + p - a_{j}p) \right)
\]

\[
\geq i + v_p((a_{i+1} + p - a_{i+1-1}p) \cdots (a_{i+1} + p - a_{i}p)) + m.
\]

Therefore, we must have that \( a_{i+1} \not\equiv a_{i+j} \) (mod \( p \)) for \( j < i \), which gives us the desired result.

In calculating our recursion for \( H(k, r, s, t) \), there are a few exceptional \( p \)-root sets which we need to dispense with first. The first, and most significant, of these cases is the set of all multiples of \( p \), for which \( r = k \), \( s = 0 \), and \( t = p > r \). We now show that this is the only \( p \)-root set which satisfies any of these three properties.

**Lemma 5.** Let \( T \) be a nonempty \( p \)-root set mod \( p^k \) such that \( \mu(T, k) = r \), \( \sigma(T) = s \), and \( \tau(T) = t \). Suppose that either \( k = r \), \( s = 0 \), or \( t > r \). Then \( T = p \mathbb{Z} \).

**Proof.** Suppose that \( k = r \). If \( S \) is the set obtained by dividing each element of \( T \) by \( p \), then we know from Proposition 2 that \( S \) must be a root set mod \( p^{k-1} \) and therefore that \( S = \mathbb{Z} \), which gives the desired result. In the case where \( s = 0 \), we know that \( 0 \in A(T) \) so that \( 1 = 0!_T = p^{k-r+0} \) and hence \( k = r \). We are reduced to the previous case.

Finally, suppose that \( t > r \). Let \( \{a_0, p, \ldots\} \) be a \( p \)-ordering of \( T \). We know from Lemma 3 that \( s'_T = p^{k-r+i} \) and \( (s+i)!_T = p^{k-r+i+p+i-1} \) and, using Lemma 4, we have that \( \{a_i, \ldots, a_{i+t-1}\} \) are all distinct mod \( p \). Since
$t > r$, we must have that $\{a_0, \ldots, a_r\}$ are also all distinct mod $p$ or else any sequence of elements from $T$ beginning $\{a, p, \ldots, a_{s+1} \}$ would have a smaller associated $p$-sequence, contradicting our choice of $p$-ordering. Therefore, we have that $r!^p = p^r$ and therefore that $r = k$, once again reducing us to the first case.

We have so far established that $H(k, 0, 0, 0) = 0$, $H(k, k, 0, p) = 1$, and $H(k, r, s, t) = 0$ when $r > k$, $s > r$ or $s + t < r$. We now handle the remaining cases recursively.

Let $T$ be a $p$-root set mod $p^k$ such that $\mu(T, k) = r$, $\sigma(T) = s$, and $\tau(T) = t$, where we assume that $r < k$ and $t \leq r$. We construct a bijection between $p$-root sets mod $p^k$ with these properties and $p$-tuples of $p$-root sets mod $p^{k-r}$, $(T_0, \ldots, T_{p-r-1})$ for which $\sum_{j=0}^{p-r-1} \mu(T_j, k-r) = s$ and exactly $t$ of the $T_j$ contain a $p^{k-r}$ in their associated $p$-sequence.

We assume first that $t > 0$. Following the same procedure of the previous section, we use Proposition 2 to divide $T$ through by $p$ and obtain a root set $S$ mod $p^{k-r}$. If we write the associated $p$-sequence for $S$, we know that $s_1S = (s+1)!, s_2 = \ldots = (s+t-1)!$, $S = p^{k-r}$, $v_p(s-1)!S < k-r$, and $v_p(s+t)!S > k-r$. We then decompose $S$ based on congruence classes mod $p$ into subsets $S_0, \ldots, S_{p-r-1}$. As before, if we add $-j$ to every element in $S_j$, we get a $p$-root set $T_j$ with the same associated $p$-sequence as $S_j$. We know from Lemma 1 that the associated $p$-sequence for $S$ is the union of the associated $p$-sequences of the subsets $T_j$. Since the $p$-sequence for a $p$-root set is strictly increasing, the sequence for a given $T_j$ contains at most one $p^{k-r}$. Therefore, exactly $t$ of the $T_j$ contain a $p^{k-r}$ in their associated $p$-sequence. Also, if $\mu(T_j, k-r) = r_j$ then we know that $\sum_{j=0}^{p-r-1} r_j = s$. If $t = 0$, then this is still true, since $s = r$ by definition and the $p$-sequence for $S$ does not contain a $p^{k-r}$ term.

Conversely, suppose we have a $p$-tuple of $p$-root sets mod $p^{k-r}$, $(T_0, \ldots, T_{p-r-1})$ for which exactly $t$ of the $T_j$ contain a $p^{k-r}$ and $\sum_{j=0}^{p-r-1} r_j = s$, where $r_j = \mu(T_j, k-r)$. As in the previous section, we add $j$ to each element of $T_j$ to get a root set $S_j$ for which every element is congruent to $j$ mod $p$. If we let $S = \bigcup_{j=0}^{p-r-1} S_j$, then, once again by Lemma 1, the $p$-sequence of $S$ is the union of the $p$-sequences of $T_j$ and $\mu(S, k-r) = \sum_{j=0}^{p-r-1} r_j = s$. In particular, the $p$-sequence for $S$ contains exactly $t$ terms of $p^{k-r}$. If $t > 0$, then, since $\mu(S, k-r) = s$ and the $p$-sequence for $S$ is nondecreasing, we must have that $s_1S = (s+1)!S = \ldots = (s+t-1)!S = p^{k-r}$, $v_p(s-1)!S < k-r$, and $v_p(s+t)!S > k-r$. If $t = 0$, then we have that $v_p(s-1)!S < k-r$ and $v_p(s+t)!S > k-r$. In either case, we lift $S$ to a $p$-root set $T$ mod $p^{k-r}$ using Proposition 3. Since $s \leq r$, $T$ is also a $p$-root set mod $p^k$. Since $\mu(T) = p^{k-r}$, we have that $A(T) = \{s, \ldots, s+t-1\}$ if $t > 0$ and $A(T) = \emptyset$ if $t = 0$. We thus have a bijection between $p$-root sets $T$ mod $p^k$ such that $\mu(T, k) = r$, $\sigma(T) = s$, and $\tau(T) = t$, and $p$-tuples of $p$-root sets mod $p^{k-r}$, $(T_0, \ldots, T_{p-r-1})$. 


for which exactly \( t \) of the \( T_j \) contain a \( p^{k-r} \) and \( \sum_{j=0}^{p-1} r_j=s \), where 
\[ \mu(T_j, k-r) = r_j. \]

We count these \( p \)-tuples as follows. Fix a partition \( s = \sum_{j=0}^{p-1} r_j \) and a subset \( X \) of \( \{0, ..., p-1\} \) of size \( t \). For \( j \in X \), we wish to count the number of \( p \)-root sets \( T_j \mod p^{k-r} \) such that \( \mu(T_j, k-r) = r_j \) and whose \( p \)-sequence contains \( p^{k-r} \), i.e. such that \( r_j! \mod p^{k-r} \). In this case, then, we have that \( r_j \in A(T_j) \) and, therefore, that \( \sigma(T_j) \leq r_j < \sigma(T_j) + \tau(T_j) \) or, equivalently, that \( r_j - \tau(T_j) < \sigma(T_j) \leq r_j \). Conversely, any \( T_j \) which satisfies this inequality will have a \( p^{k-r} \) in its \( p \)-sequence. The total number of such \( T_j \) is then

\[
\sum_{0 \leq d < p \atop r_j-d < c < r_j} H(k-r, r_j, c, d) \cdot \text{for } j \notin X.
\]

For \( j \notin X \), we wish to count the number of \( p \)-root sets \( T_j \) such that \( \mu(T_j, k-r) = r_j \) and whose \( p \)-sequence does not contain \( p^{k-r} \), i.e. such that \( e_j(r_j, x) > k-r \). Applying Lemma 3 in this case, we have that either \( \tau(T_j) = 0 \) or that \( \sigma(T_j) + \tau(T_j) = r_j \), since the largest element of \( A(T_j) \) must be \( r_j - 1 \). Similarly, any \( T_j \) which satisfies this last equality will not have \( p^{k-r} \) in its \( p \)-sequence. The total number of such \( T_j \) is then

\[
\sum_{c+d=r_j} H(k-r, r_j, c, d).
\]

For a given partition of \( s \) and subset \( X \), we then multiply these terms over \( j = 0, ..., p-1 \). Finally, we add over all partitions and subsets. Distinct partitions give rise to distinct \( p \)-tuples, since the corresponding sets \( T_j \) will have different \( \mu \)-values for some \( j \). Similarly, distinct subsets \( X \) and \( Y \) of \( \{0, ..., p-1\} \) must give rise to distinct \( p \)-tuples. Take \( j \notin X \); then \( T_j \) in a \( p \)-tuple from the subset \( X \) has a \( p^{k-r} \) in its \( p \)-sequence while the \( T_j \) in a \( p \)-tuple from the subset \( Y \) does not. Therefore, there is no over-counting in this last step. This gives us the following recursion for \( H(k, r, s, t) \):

\[ \text{Proposition 7. For } r < k, \text{ we have that} \]

\[
H(k, r, s, t) = \sum_{r_0 + \cdots + r_{p-1} = s \atop |X| = t} \left( \prod_{j \in X} \left( \sum_{0 \leq d < p \atop r_j-d < c < r_j} H(k-r, r_j, c, d) \right) \right) \times \left( \prod_{j \notin X} \left( \sum_{c+d=r_j} H(k-r, r_j, c, d) \right) \right).
\]

(3)

Together with our previously listed exceptional cases, this gives us a full characterization of \( H(k, r, s, t) \). It would nice if we could then show that \( H(k, r, s, t) \) is a polynomial function of \( p \) for fixed \( k, r, s \), and \( t \) and \( p > k \).
This is not true, however, since $H(k, k, 0, p) = 1$ for a fixed prime $p$, but $H(k, k, 0, p) = 0$ for all other primes $q > k$. Since all other nonzero values of $H$ have $t \leq r$, this is essentially the only counterexample.

**Corollary 2.** Fix $k, r, s, t$ such that $t \leq r$. Then $H(k, r, s, t)$ is a polynomial function of $p$ for $p > k$.

**Proof.** As in the previous section, we proceed by induction on $k$. The base cases for $k = 1$ are $H(1, 0, 0, 0) = 1$ and $H(1, r, s, t) = 0$ otherwise (for $t \leq r$). The exceptional cases listed above are also easy to check. We are left with $r < k$; as in the proof of Proposition 6, we rewrite our recursion in terms independent of $p$. In particular, note that in our recursion (3), the values $c = 0$, $d = p$ are always permissible in the summation for $j \in X$ and never permissible in the summation for $j \notin X$. Proceeding as before, we can express our recursion as

$$
H(k, r, s, t) = \sum_{r_1 + \ldots + r_a = a} \binom{p}{a} 
\times \sum_{X \subseteq \{1, \ldots, a\} \text{ s.t. } |X| = r} \left( \prod_{j \in X} \left( 1 + \sum_{0 \leq d < c \leq r_j} H(k - r, r_j, c, d) \right) \right)
\times \left( \prod_{j \notin X} \left( \sum_{c + d = r_j} H(k - r, r_j, c, d) \right) \right).
$$

Since no term aside from $H(k - r, r_j, c, d)$, where $c \leq r_j$, and $(\xi)$ depends on $p$, and both of these are polynomial functions of $p$, we are done by induction. 

We know, using Lemma 5, that

$$
N_{p^k} = \sum_{k, r, s, t} H(k, r, s, t) = H(k, k, 0, p) + \sum_{k, r, s, t} H(k, r, s, t)
= 1 + \sum_{k, r, s, t} H(k, r, s, t).
$$

In particular, Theorem 4 follows.

Let $q_k(x)$ be the polynomial function of Theorem 4. From Theorem 3 in the previous section, we know that the leading term of $q_k$ is $c_k p^{k^2/4}$. We also calculate the constant term of $q_k$ in the following proposition.
Proposition 8. For all positive integers \( k \) and primes \( p \), we have that \( N_{p^k} \equiv 2 \pmod{p} \). Also, the constant term of \( q_k(x) \) is 2.

Proof. Let \( g \) be the map on \( \mathbb{Z} \) defined by translation by \( p \), that is \( g(x) = x + p \). Then if \( T \) is a \( p \)-root set mod \( p^k \) generated by the polynomial \( f(x) \), then \( g(T) \) is also a \( p \)-root set mod \( p^k \), generated by \( f(x - p) \). Therefore, we have that \( g \) permutes the elements of \( U \), the set of all \( p \)-root sets mod \( p^k \). If we now view \( g \) as a permutation of \( U \) and consider the cyclic subgroup \( G \) generated by \( g \), we see that \( g^{p^{k-1}} = \text{id} \). We now decompose \( U \) into disjoint orbits under the action of \( G \); the size of each orbit is \( p^j \) for some \( j \geq 0 \). It suffices to show that there are exactly 2 fixed points of \( G \) in \( U \). Clearly the empty set and the set of all multiples of \( p \) are fixed points. Let \( T \) be a nonempty fixed point of \( G \). If \( ap \not\equiv T \pmod{p} \) for some \( j \geq 0 \), then \( kp \not\equiv g^{k-1}T = T \pmod{p} \) for any \( k \). Thus, these are the only two fixed points and \( N_{p^k} \equiv 2 \pmod{p} \). For the second statement, write \( q_k(x) = (x r(x) + c_0)/n \), where \( r(x) \) has integer coefficients and \( n \) and \( c_0 \) are integral constants. For all primes \( p \), this gives that \( c_0 \equiv pr(p) + c_0 \equiv nN_{p^k} \equiv 2n \pmod{p} \). Therefore, we have that \( c_0 = 2n \) so \( q_k(x) \) has constant term 2.

5. Conclusion

Since we only use the condition that \( p > k \) in the previous section to classify the exceptional sets of Lemma 5 and to express \( H(k, r, s, t) \) as a polynomial function, we can generalize some of our results from the previous section to the case when \( p \leq k \). In particular, the proof of Proposition 7 goes through as written, with the added assumption that \( s > 0 \). It now remains to classify the cases when \( k = r \) or \( s = 0 \). Once again, most of the proof of Lemma 5 generalizes. That is, given a \( p \)-root set \( T \pmod{p^k} \) such that either \( \mu(T, k) = k \) or \( \sigma(T) = 0 \), then we must have that \( T = p\mathbb{Z} \). However, if \( p < k \), the set \( T = p\mathbb{Z} \) does not satisfy either of these conditions, so there are no exceptional sets. If \( p = k \), then \( T = p\mathbb{Z} \) satisfies both of these conditions and must thus be considered separately. We thus have a recursive classification of the number of root sets mod \( p^k \). Moreover, note that in proving a recursion for the number of \( p \)-root sets, we in fact provide a method of constructing all \( p \)-root sets mod \( p^k \), given the root sets for all smaller moduli, by applying the recursion for \( H(k, r, s, t) \).

Also, in the proofs of this paper as well as those of [1, 2], the only significant property of the integers is that \( \mathbb{Z} \) is a principal ideal domain such that every residue ring is finite. Therefore, our main results easily generalize to these rings. Moreover, given a Dedekind domain \( R \) and a prime ideal \( P \), if \( S \) is the localization of \( R \) at \( P \) and \( (p) \) is its unique
maximal ideal, then \( S \) is a principal ideal domain and \( R/P^k \cong S/p^k \). Consequently, we can generalize to Dedekind domains as well. That is, given a Dedekind domain \( R \) and prime ideal \( P \), let \( N(P) \) denote the size of \( R/P \), we then have the following theorem:

**Theorem 5.** Given a Dedekind domain \( R \), then for all prime ideals \( P \) such that \( N(P) \) is finite and \( N(P) > k \), the total number of root sets mod \( P^k \) is \( (q_k(N(P)))^{N(P)} \), where \( q_k \) is a polynomial function of \( N(P) \). Moreover, this polynomial \( q_k \) is the same polynomial function described in Theorem 4 for \( \mathbb{Z} \).

The last statement follows from the fact that our recursion and base cases are independent of our choice of ring.

Finally, we discuss open questions left to consider. First of all, since we have only fully addressed the case where \( p > k \), we can ask the same questions when \( p \leq k \); in particular, using the recursion for \( p \leq k \), it should be possible to obtain bounds on the size of \( N_{p,k} \) for all \( p \) and \( k \). Also, it might be interesting to consider the growth of \( N_{p,k} \) for fixed \( p \) as \( k \) increases.

**ACKNOWLEDGMENTS**

This work was done under the supervision of Joseph Gallian at the University of Minnesota, Duluth, with financial support from the National Science Foundation (Grant DMS-9531373-001) and the National Security Agency (Grant MDA-904-98-1-0523). The author wishes to thank Manjul Bhargava, Samit Dasgupta, and Joseph Gallian for their suggestions and encouragement.

**REFERENCES**