On Least Common Multiples of Polynomials in $\mathbb{Z}/n\mathbb{Z}[x]$
Nicholas J. Werner
werner@math.osu.edu
Department of Mathematics, The Ohio State University,
231 West 18th Avenue, Columbus, OH 43210

Abstract
Let $\mathcal{P}(n, D)$ be the set of all monic polynomials in $\mathbb{Z}/n\mathbb{Z}[x]$ of degree $D$. A least common multiple for $\mathcal{P}(n, D)$ is a monic polynomial $L \in \mathbb{Z}/n\mathbb{Z}[x]$ of minimal degree such that $f$ divides $L$ for all $f \in \mathcal{P}(n, D)$. A least common multiple for $\mathcal{P}(n, D)$ always exists, but need not be unique; however, its degree is always unique. In this paper, we establish some bounds for the degree of a least common multiple for $\mathcal{P}(n, D)$, present constructions for common multiples in $\mathbb{Z}/n\mathbb{Z}[x]$, and describe a connection to rings of integer-valued polynomials over matrix rings.

Keywords: polynomial, least common multiple, finite ring, matrix

MSC Primary 13M10; Secondary 11C99

Notation
All rings under consideration contain unity and, with the exception of matrix rings, are commutative. Throughout this paper, we use the following notations:

- For any integer $n > 1$, $\mathbb{Z}_n$ represents the quotient ring $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$.
- For any integer $D > 0$ and any ring $R$, $M_D(R)$ denotes the ring of $D \times D$ matrices over $R$.
- $p$ is always a prime, and $k$ is an integer greater than 0, so that $p^k$ is a power of a prime.
- For any $n, D \in \mathbb{Z}$ with $n > 1$ and $D > 0$, we let $\mathcal{P}(n, D)$ be the set of all monic polynomials in $\mathbb{Z}_n[x]$ of degree $D$.
- For any real number $x$, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to $x$.

(to appear in Comm. Algebra)
• If $R$ is a local ring with maximal ideal $\mathfrak{m}$, then we use a bar to denote passage to the quotient ring $R/\mathfrak{m}$. That is, if $\alpha \in R$, then $\bar{\alpha}$ represents the residue class of $\alpha$ in $R/\mathfrak{m}$. We adopt the same convention with polynomials and matrices: if $f \in R[x]$, then $\overline{f}$ represents the residue class of $f$ in $(R/\mathfrak{m})[x]$; and if $A \in M_D(R)$, then $\overline{A}$ is the residue of $A$ in $M_D(R/\mathfrak{m})$.

• lcm stands for “least common multiple.”

1 Linear Polynomials in $\mathbb{Z}_{p^k}[x]$

Consider the following situation. Let $n, D \in \mathbb{Z}$ with $n > 1$ and $D > 0$. Let $\mathcal{P}(n, D)$ denote the set of all monic polynomials in $\mathbb{Z}_n[x]$ of degree $D$. Since $\mathcal{P}(n, D)$ is finite, $g := \prod_{f \in \mathcal{P}(n, D)} f$ is a monic polynomial in $\mathbb{Z}_n[x]$ that is a common multiple of all the polynomials in $\mathcal{P}(n, D)$; that is, $f | g$ for all $f \in \mathcal{P}(n, D)$. Among all such common multiples, there must be one of least degree.

**Definition 1.1.** Let $R$ be a ring and $X$ a subset of $R[x]$. A least common multiple for $X$ is a monic polynomial $L \in R[x]$ of least degree such that $f | L$ for all $f \in X$. We say that $L$ is an lcm for $X$.

Note that we require an lcm to be monic. An lcm for $\mathcal{P}(n, D)$ always exists, but if $n$ is not a prime, then an lcm for $\mathcal{P}(n, D)$ need not be unique. Indeed, by Proposition 1.5 below, any monic polynomial in $\mathbb{Z}_{p^2}[x]$ of degree $2p$ that kills everything in $\mathbb{Z}_{p^2}$ is an lcm for $\mathcal{P}(p^2, 1)$. So, $L(x) = (x^p - x)^2$ is such an lcm; but so is $L(x) + p(x^p - x)$.

An lcm for $\mathcal{P}(n, D)$ need not be unique, but the degree of an lcm for $\mathcal{P}(n, D)$ is always unique.

**Definition 1.2.** Let $R$ be a ring and $X$ a subset of $R[x]$. We define $\delta(X)$ to be the degree of an lcm for $X$, if one exists.

The goal of this paper is to establish bounds for $\delta(\mathcal{P}(n, D))$. The first observation we make is that it suffices to consider the case where $n$ is a power of a prime.

**Proposition 1.3.** Let $n, D \in \mathbb{Z}$ with $n > 1$ and $D > 0$. Assume that $n$ factors as $n = ml$, where $m > 1$ and $\ell > 1$ are relatively prime integers.
Then, \( \delta(\mathcal{P}(n, D)) = \max\{\delta(\mathcal{P}(m, D)), \delta(\mathcal{P}(\ell, D))\} \). Furthermore, if \( n \) has prime factorization \( n = p_1^{e_1}p_2^{e_2} \cdots p_t^{e_t} \), then \( \delta(\mathcal{P}(n, D)) = \max_{1 \leq j \leq t}\{\delta(\mathcal{P}(p_j^{e_j}, D))\} \).

**Proof.** The first assertion follows from the Chinese Remainder Theorem, and the second follows from induction on \( t \). \( \square \)

Not surprisingly, if \( n = p^k \) then the easiest situation to handle occurs when \( D = 1 \), where we can determine \( \delta(\mathcal{P}(p^k, 1)) \) exactly. In this case, \( \mathcal{P}(p^k, 1) = \{x - a \mid a \in \mathbb{Z}_{p^k}\} \), and if \( f \in \mathbb{Z}_{p^k}[x] \), then \( x - a \mid f \) if and only if \( f(a) = 0 \). Thus, we seek a monic polynomial \( L \in \mathbb{Z}_{p^k}[x] \) of minimal degree such that \( L(a) = 0 \) for all \( a \in \mathbb{Z}_{p^k} \).

For a prime \( p \) and a positive integer \( N \), let

\[
\text{w}_p(N) = \sum_{j \geq 1} \left\lfloor \frac{N}{p^j} \right\rfloor. \tag{1.4}
\]

This formula is sometimes known as Legendre’s formula (Cahen and Chabert, 2006, Sec. 1.2) and it is well-known that \( \text{w}_p(N) \) equals the number of powers of \( p \) in \( N! \).

**Proposition 1.5.** Let \( N = \min_{m \in \mathbb{N}}\{\text{w}_p(m) \geq k\} \). Then, \( \delta(\mathcal{P}(p^k, 1)) = N \).

**Proof.** Let \( g(x) = x(x - 1) \cdots (x - (N - 1)) \). Then, \( g(\mathbb{Z}) \subseteq p^k\mathbb{Z} \), so \( g \) is a monic common multiple for \( \mathcal{P}(p^k, 1) \). Thus, \( \delta(\mathcal{P}(p^k, 1)) \leq N \).

Let \( L \) be an lcm for \( \mathcal{P}(p^k, 1) \). It follows from a theorem due to Pólya (Bhargava, 1998, Thm. 1) that whenever \( f \in \mathbb{Z}[x] \) is monic and \( \deg(f) = m \), then the gcd of values of \( f \) on \( \mathbb{Z} \) divides \( m! \). Since \( L(\mathbb{Z}) \subseteq p^k\mathbb{Z} \), Pólya’s result implies that \( p^k \mid (\deg(L))! \), i.e. \( \text{w}_p(\deg(L)) \geq k \). By the minimality of \( N \), \( \deg(L) \geq N \). Hence, \( \delta(\mathcal{P}(p^k, 1)) = N \). \( \square \)

The majority of the rest of this paper is dedicated to the more difficult task of finding bounds for \( \delta(\mathcal{P}(p^k, D)) \) when \( D > 1 \). In some circumstances we will be able to give exact values for \( \delta(\mathcal{P}(p^k, D)) \); at other times, we will only be able to calculate upper bounds.

About notation: we will derive several bounds for the values of \( \delta(\mathcal{P}(n, D)) \) and \( \delta(\mathcal{P}(p^k, D)) \). To concisely distinguish these bounds, we will refer to each one by the number of the result where it was established. Thus, the bound for \( \delta(\mathcal{P}(p^k, 1)) \) found in Proposition 1.5 is Bound (1.5).
2 A Connection to Matrix Rings

In finding Bound (1.5), it was useful to establish a connection between an lcm for $P(p^k, 1)$ and polynomials that kill everything in $\mathbb{Z}_{p^k}$. We can realize an analogous connection for $P(n, D)$ by using the matrix ring $M_D(\mathbb{Z}_n)$. Except for terminology and notational differences, the results of this section are generally the same as in (Frisch, 2005, Sec. 3).

**Definition 2.1.** For a ring $R$ and $D > 0$, we define

$$P(R, D) = \{ \text{monic polynomials in } R[x] \text{ of degree } D \}, \quad \text{and}$$

$$\mathcal{K}(M_D(R)) = \{ f \in R[x] \mid f(A) = 0 \text{ for all } A \in M_D(R) \}.$$

Thus, $\mathcal{K}(M_D(R))$ consists of all the polynomials in $R[x]$ that kill everything in $M_D(R)$.

Generally, the ring $R$ in the above definition will be either $\mathbb{Z}_n$ or a ring extension of $\mathbb{Z}_{p^k}$, but there is no harm in stating the above definitions and the following theorems for an arbitrary ring.

As shown by (Frisch, 2005, Lem. 3.4), $\mathcal{K}(M_D(R))$ equals the set of common multiples for $P(R, D)$. So, to test whether a polynomial $L$ is a common multiple for $P(n, D)$, it is enough to check that $L$ kills every matrix in $M_D(\mathbb{Z}_n)$. Furthermore, it gives us another characterization of an lcm for $P(n, D)$.

**Proposition 2.2.** A polynomial $L$ is an lcm for $P(n, D)$ if and only if $L$ is of minimal degree among all the monic polynomials in $\mathcal{K}(M_D(\mathbb{Z}_n))$.

Next, we mention a useful lemma regarding companion matrices. For any ring $R$ and any monic polynomial $f(x) = \sum_{j=0}^{D} a_j x^j \in R[x]$, the companion matrix of $f(x)$ is the $D \times D$ matrix in $M_D(\mathbb{R})$ with 1’s down the first sub-diagonal, $-a_0, -a_1, \ldots, -a_{D-1}$ down the last column, and zeros elsewhere. If $A$ is the companion matrix for $f$, it is well-known that $f(A) = 0$. The following lemma—which is equivalent to (Frisch, 2005, Lem. 3.3)—slightly generalizes this result. The proof is a straightforward calculation involving companion matrices.

**Lemma 2.3.** Let $R$ be a ring, let $f \in R[x]$ be monic of degree $D$, and let $A \in M_D(R)$ be the companion matrix for $f$. Let $g \in R[x]$. Then, $f \mid g$ if and only if $g(A) = 0$. 

It is important that we use the companion matrix for $f$ in the above lemma. For example, if $R = \mathbb{Z}_4$ and $f(x) = x^2 \in R[x]$, then $f$ is a monic polynomial of minimal degree that kills $A = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \in M_2(R)$. However, $g(x) = 2x$ also kills $A$, but $f \nmid g$.

One application of the work in this paper involves integer-valued polynomials over matrix rings. For any $D > 0$, let

$$\text{Int}(M_D(\mathbb{Z})) = \{ f \in M_D(\mathbb{Q})[x] \mid f(M_D(\mathbb{Z})) \subseteq M_D(\mathbb{Z}) \},$$

called the set of integer-valued polynomials over $M_D(\mathbb{Z})$. In (Werner, 2010, Sec. 2), the author outlined a proof that $\text{Int}(M_D(\mathbb{Z}))$ has a (non-commutative) ring structure. By identifying $\mathbb{Q}$ with the scalar matrices in $M_D(\mathbb{Q})$, one may also study the commutative ring

$$\text{Int}(M_D(\mathbb{Z})) \cap \mathbb{Q}[x] = \{ f \in \mathbb{Q}[x] \mid f(M_D(\mathbb{Z})) \subseteq M_D(\mathbb{Z}) \},$$

as S. Frisch did in an earlier paper (Frisch, 2005) where the ring was called $\text{Mint}_D(\mathbb{Z})$.

It is not hard to see that the polynomial $\frac{2}{n} \in \mathbb{Q}[x]$ (where $g \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}, n > 0$) is in $\text{Int}(M_D(\mathbb{Z})) \cap \mathbb{Q}[x]$ if and only if the residue of $g$ mod $n$ lies in $\mathcal{K}(M_D(\mathbb{Z}_n))$, which is to say that $g$ is a common multiple for $\mathcal{P}(n, D)$. Thus, producing elements of $\text{Int}(M_D(\mathbb{Z})) \cap \mathbb{Q}[x]$ amounts to constructing common multiples in $\mathbb{Z}_n[x]$, and it is the study of these polynomials that inspired the current paper. Furthermore, the bounds established herein for $\delta(\mathcal{P}(n, D))$ also bound the minimal degree of a monic $g \in \mathbb{Z}[x]$ such that $\frac{2}{n} \in \text{Int}(M_D(\mathbb{Z})) \cap \mathbb{Q}[x]$. Such polynomials $\frac{2}{n}$ are of interest because they can be used to generate the ring $\text{Int}(M_D(\mathbb{Z})) \cap \mathbb{Q}[x]$.

3 What Happens in $\mathbb{Z}_p[x]$ and a First Bound

Having reduced the problem of finding an lcm for $\mathcal{P}(n, D)$ to finding an lcm for $\mathcal{P}(p^k, D)$, we consider the case where $k = 1$. Since $\mathbb{Z}_p$ is a field, we can get a unique lcm for $\mathcal{P}(p, D)$.

**Theorem 3.1.** Let $D > 0$. Then, $L(x) = (x^{pD} - x)(x^{pD-1} - x) \cdots (x^p - x)$ is the unique lcm for $\mathcal{P}(p, D)$.

**Proof.** Let $\mathcal{I}$ be the set of all the irreducible polynomials in $\mathbb{Z}_p[x]$ of degree less than or equal to $D$. It is a standard theorem in abstract algebra that
$x^{p^n} - x$ is the product of all the irreducible polynomials in $\mathbb{Z}_p[x]$ of degree dividing $n$. For each $\iota \in \mathcal{I}$, let $e(\iota) = \lfloor \frac{D}{\deg(\iota)} \rfloor$. Then, the factorization of $L$ into irreducibles is $L = \prod_{\iota \in \mathcal{I}} \iota^{e(\iota)}$.

Let $L'$ be any common multiple for $\mathcal{P}(p, D)$. Then, for each $\iota \in \mathcal{I}$, $\iota^{e(\iota)}$ divides $L'$, so $L | L'$. Thus, $L$ is an lcm for $\mathcal{P}(p, D)$. If $\ell$ is any other lcm for $\mathcal{P}(p, D)$, then $\ell$ is monic, $\deg(\ell) = \deg(L)$, and $L | \ell$; thus, we must have $\ell = L$.

Theorem 3.1 allows us to construct a bound for $\delta(\mathcal{P}(p^k, D))$.

**Proposition 3.2.** Let $D > 0$. Then, $\delta(\mathcal{P}(p^k, D)) \leq k(p^D + p^{D-1} + \cdots + p)$.

**Proof.** Let $L(x) = (x^{p^D} - x)(x^{p^{D-1}} - x) \cdots (x^p - x) \in \mathbb{Z}_p[x]$, and let $f \in \mathbb{Z}_{p^k}[x]$ be a monic polynomial such that $\overline{f} = L$. Now, $L \in K(M_D(\mathbb{Z}_p))$, so $f^k \in K(M_D(\mathbb{Z}_{p^k}))$, and thus $\delta(\mathcal{P}(p^k, D)) \leq \deg(f^k)$.

As the value of $k$ increases, we can find bounds for $\delta(\mathcal{P}(p^k, D))$ that are more accurate than Bound (3.2). For example, Bound (3.2) for $\delta(\mathcal{P}(p^k, 1))$ is $kp$, but $w_p(p^n) = p^{n-1} + \cdots + p + 1$, so when $k = p^{n-1} + \cdots + p + 1$, Bound (1.5) is $p^n < kp$, and the difference between the two bounds grows larger as $k$ increases. The rest of this paper will examine ways to beat Bound (3.2) when $D > 1$.

## 4 Primary Factorization of Polynomials

The lcm of a set of positive integers can be found by first taking the prime factorization of each integer, and then taking the product over all primes $p$ of the highest power of $p$ that occurs among the factorizations. Since polynomials in $\mathbb{Z}_{p^k}[x]$ do not factor uniquely into prime elements, the same procedure cannot be mimicked exactly in our situation. However, we can formulate a similar strategy by using primary polynomials (defined below) in place of prime numbers.

In the forthcoming sections, we will begin to work with rings of the form $\mathbb{Z}_{p^k}[\alpha]$, where $\alpha$ is a root of a monic irreducible polynomial in $\mathbb{Z}_{p^k}[x]$. As shown by (Ganske and McDonald, 1973, Cor. 3.8), $\mathbb{Z}_{p^k}[\alpha]$ is—like $\mathbb{Z}_{p^k}$—a finite local ring. So, where possible, our theorems will be phrased in terms of local rings.
Definition 4.1. Let $R$ be a local ring with maximal ideal $\mathfrak{M}$. A monic polynomial $f \in R[x]$ is called primary if $\overline{f}$ is a positive power of an irreducible polynomial in $(R/\mathfrak{M})[x]$. If $\overline{f}$ is a positive power of the irreducible polynomial $\iota$, then we say that $f$ is $\iota$-primary.

This definition is similar to the definition of a primary polynomial in $\mathbb{Z}_p^k[x]$ given in (Frei and Frisch, Def. 3.6), where $f \in \mathbb{Z}_p^k[x]$ is defined to be primary if $f$ is not a zero divisor and $\overline{f}$ is a power of an irreducible polynomial in $\mathbb{Z}_p[x]$. Note, however, that we require a primary polynomial to be monic. One may show (Wan, 2003, Lem. 13.4) that for a monic polynomial $f \in \mathbb{Z}_p^k[x]$, $f$ is primary (under Definition 4.1) if and only if $(f)$ is a primary ideal of $\mathbb{Z}_p^k[x]$.

A local ring $R$ is called Henselian if Hensel’s Lemma holds for $R$; in particular, a finite local ring is Henselian. It is a consequence of Hensel’s Lemma that a monic polynomial over a Henselian ring has a factorization into primary polynomials.

Lemma 4.2. Let $R$ be a Henselian ring with maximal ideal $\mathfrak{M}$. Let $f \in R[x]$ be monic. Then, there exist distinct irreducible polynomials $\iota_1, \iota_2, \ldots, \iota_n \in (R/\mathfrak{M})[x]$ and primary polynomials $f_1, f_2, \ldots, f_n \in R[x]$ such that $f_j$ is $\iota_j$-primary for each $1 \leq j \leq n$, and $f = f_1f_2 \cdots f_n$.

Definition 4.3. Let $R$ be a Henselian ring and let $f \in R[x]$ be monic. When $f = f_1f_2 \cdots f_n$ as in the above lemma, we call this a primary factorization of $f$.

It turns out that primary factorizations of $f$ are unique up to permutation of the primary factors. We shall prove this below in Theorem 4.6. A proof for the case $R = \mathbb{Z}_p^k$ is given in (Wan, 2003, Thm. 13.8).

The following result is an elementary lemma regarding matrices. A proof was not readily available in the literature, so one is provided.

Lemma 4.4.

(i) Let $F$ be a field and let $f$ and $g$ be coprime polynomials in $F[x]$. Let $A \in M_D(F)$ be such that $f(A) = 0$. Then, $g(A)$ is a unit in $M_D(F)$.

(ii) Let $R$ be a local ring with maximal ideal $\mathfrak{M}$. Let $f, g \in R[x]$ be such that $\overline{f}$ and $\overline{g}$ are coprime in $(R/\mathfrak{M})[x]$. Let $A \in M_D(R)$ be such that $f(A) = 0$. Then, $g(A)$ is a unit in $M_D(R)$. 

7
Proof. (i) Since \( f \) and \( g \) are coprime, there exist \( a, b \in F[x] \) such that \( af + bg = 1 \). Then, letting \( I \) be the identity matrix in \( M_D(F) \), we have \( I = a(A)f(A) + b(A)g(A) = b(A)g(A) \), so \( g(A) \) is a unit.

(ii) By part (i), \( g(\mathcal{A}) \) is a unit in \( R/\mathfrak{M} \). So, \( \det(g(\mathcal{A})) \neq 0 \) in \( R/\mathfrak{M} \), i.e. \( \det(g(A)) \notin \mathfrak{M} \) in \( R \). But then, \( \det(g(A)) \) is a unit in \( R \), so \( g(A) \) is a unit in \( M_D(R) \).

Lemma 4.5. Let \( R \) be a Henselian ring with maximal ideal \( \mathfrak{M} \), let \( \iota \in (R/\mathfrak{M})[x] \) be an irreducible polynomial, let \( f \in R[x] \) by \( \iota \)-primary, and let \( g \in R[x] \) be a monic polynomial such that \( f \mid g \). Let \( g = g_1 g_2 \cdots g_n \) be a primary factorization of \( g \). Then, some \( g_j \) is \( \iota \)-primary, and \( f \mid g_j \).

Proof. Assume that \( \overline{f} = \iota^e \) and that for each \( 1 \leq j \leq n \), \( g_j = \iota_j^{e_j} \), where \( \iota_j \) is an irreducible polynomial in \( (R/\mathfrak{M})[x] \).

Working in \( (R/\mathfrak{M})[x] \), we have \( \iota^e \mid \iota_1^{e_1} \cdots \iota_n^{e_n} \), so \( \iota^e \) divides some \( \iota_j^{e_j} \). WLOG, assume that \( j = 1 \), so \( \iota_1 = \iota \) and \( e_1 \geq e \). Then, \( \overline{g} = \overline{g_1} \overline{h} \), where \( h = g_2 \cdots g_n \).

Now, \( \overline{g_1} = \iota^{e_1} \) and \( \overline{h} \) are coprime in \( (R/\mathfrak{M})[x] \). Let \( A \) be the companion matrix for \( f \) in \( M_D(R) \), where \( D = \deg(f) \). By Lemma 4.4 part (ii), \( h(A) \) is a unit in \( M_D(R) \). Since \( f \mid g \), we have \( 0 = g(A) = g_1(A) h(A) \), so \( g_1(A) = 0 \). By Lemma 2.3, we have \( f \mid g_1 \).

Theorem 4.6. Let \( R \) be a Henselian ring with maximal ideal \( \mathfrak{M} \) and let \( f \in R[x] \) be monic. Let \( f = f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m \) be two primary factorizations of \( f \). Then, \( n = m \) and, after reindexing, \( f_j = g_j \) for each \( 1 \leq j \leq n \). Thus, the primary factorization of \( f \) is unique up to the permutation of the factors.

Proof. Let \( t \) be the number of irreducible polynomials in \( (R/\mathfrak{M})[x] \) that divide \( \overline{f} \). Then, \( n = t = m \).

Next, fix \( r \in \{1, 2, \ldots, n\} \) and assume that \( f_r \) is \( \iota \)-primary. Since \( f_r \mid g_1 \cdots g_n \), one of the \( g_j \) is \( \iota \)-primary and divisible by \( f_r \). After reindexing, we may assume that \( f_r \mid g_j \). Since \( r \) was arbitrary, we have \( f_j \mid g_j \) for each \( 1 \leq j \leq n \). We can repeat the argument of this paragraph with the roles of \( f_j \) and \( g_j \) reversed, so we conclude that for each \( j \), \( f_j \mid g_j \) and \( g_j \mid f_j \). Since all of the \( f_j \) and \( g_j \) are monic, we must have \( f_j = g_j \) for each \( j \), which proves the result.

Because of Theorem 4.6, we may speak of the primary factorization of a monic polynomial with coefficients in a Henselian ring.
5 Reduction to Primary Polynomials

The next theorem shows that, in determining an lcm for $P(p^k, D)$, it suffices to work with primary polynomials.

**Theorem 5.1.** Let $R$ be a finite local ring with maximal ideal $\mathfrak{m}$. Let $D > 0$ and let $\mathcal{P} = \mathcal{P}(R, D)$. Let $\iota_1, \iota_2, \ldots, \iota_t$ be all the irreducible polynomials in $(R/\mathfrak{m})[x]$ of degree less than or equal to $D$. For each $1 \leq j \leq t$, let

$$\mathcal{P}_j = \{\iota_j\text{-primary polynomials in } R[x] \text{ of degree } \deg(\iota_j)\lfloor \frac{D}{\deg(\iota_j)} \rfloor\}.$$

Then,

(i) For each $1 \leq j \leq t$, let $L_j$ be an lcm for $\mathcal{P}_j$. Then, $L_j$ is $\iota_j$-primary.

(ii) Let $\mathcal{P}' = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \ldots \cup \mathcal{P}_t$ and let $L'$ be an lcm for $\mathcal{P}'$. Then, $L'$ is an lcm for $\mathcal{P}$.

(iii) For each $1 \leq j \leq t$, let $L_j$ be as in (i), and let $L = L_1L_2\cdots L_t$. Then, $L$ is an lcm for $\mathcal{P}$.

**Proof.** (i) Fix $j$ between 1 and $t$. For any $f_j \in \mathcal{P}_j$, we have $f_j | L_j$. By Lemma 4.5, the primary factorization of $L_j$ has an $\iota_j$-primary factor $F$, and $f_j | F$. So, $F$ is a monic common multiple for $\mathcal{P}_j$. Since $F | L_j$, we must have $\deg(L_j) = \deg(F)$; and since both $L_j$ and $F$ are monic, we must have $L_j = F$.

(ii) Let $f \in \mathcal{P}$ with primary factorization $f = f_1f_2\cdots f_n$. For each $1 \leq r \leq n$, $f_r$ divides some polynomial in $\mathcal{P}'$, so $f_r | L'$. It follows that $f | L'$ and hence $L'$ is a common multiple for $\mathcal{P}$. Let $L$ be an lcm for $\mathcal{P}$; then, $\deg(L) \leq \deg(L')$. But, $L$ is also a common multiple for $\mathcal{P}'$, so $\deg(L') \leq \deg(L)$ and hence $\deg(L') = \deg(L)$.

(iii) Let $\mathcal{P}'$ be as in part (ii). Then, $L$ is a common multiple for $\mathcal{P}'$. Let $g$ be any monic common multiple for $\mathcal{P}'$. Then, $g$ has primary factorization $g = g_1g_2\cdots g_t$, where each $g_j$ is $\iota_j$-primary. Now, each $g_j$ is a common multiple for $\mathcal{P}_j$, so $\deg(L_j) \leq \deg(g_j)$. Thus, $\deg(L) \leq \deg(g)$, $L$ is an lcm for $\mathcal{P}'$, and therefore $L$ is an lcm for $\mathcal{P}$. \qed

Theorem 5.1 reduces the problem of finding $\delta(P(p^k, D))$ to finding $\delta(P_i)$, where $P_i$ is the set of all the $\iota$-primary polynomials in $\mathbb{Z}_{p^k}[x]$ of degree $\deg(\iota)\lfloor \frac{D}{\deg(\iota)} \rfloor$. We can get an upper bound for $\delta(P_i)$ by the same technique used in Proposition 3.2.
Proposition 5.2. Let $D > 0$ and let $\iota \in \mathbb{Z}_p[x]$ be irreducible of degree $d$. Let $\mathcal{P}_\iota = \{\iota$-primary polynomials in $\mathbb{Z}_{p^k}[x]$ of degree $d\lfloor \frac{D}{d} \rfloor \}$. Then, $\delta(\mathcal{P}_\iota) \leq kd\lfloor \frac{D}{d} \rfloor$.

Proof. Let $m = \lfloor \frac{D}{d} \rfloor$. Fix $g \in \mathcal{P}_\iota$, let $f \in \mathcal{P}_\iota$ and let $A$ be the companion matrix for $f$ in $M_{dm}(\mathbb{Z}_{p^k})$. Then, $g = \iota^m = \overline{f}$, so $g(A) = 0$ in $M_{dm}(\mathbb{Z}_p)$. Thus, $g(A)^k = 0$ in $M_{dm}(\mathbb{Z}_{p^k})$. By Lemma 2.3, we have $f \mid g^k$, and thus $g^k$ is a monic common multiple for $\mathcal{P}_\iota$. Hence, $\delta(\mathcal{P}_\iota) \leq \deg(g^k) = kdm$. \hfill $\square$

As with Bound (3.2), subsequent results in this paper will lead to bounds for $\delta(\mathcal{P}_\iota)$ that are better than Bound (5.2).

6 Reduction to Powers of Linear Polynomials

We can further reduce our problem by working in ring extensions of $\mathbb{Z}_{p^k}$. If $\iota$ is an irreducible polynomial in $\mathbb{Z}_p[x]$, then $\iota$ factors completely over the extension field $\mathbb{Z}_p(\alpha)$ of $\mathbb{Z}_p$, where $\alpha$ is a root of $\iota$. Thus, if we can work in an extension ring $S$ of $\mathbb{Z}_{p^k}$ with $\mathbb{Z}_p(\alpha)$ as a residue field, then instead of considering $\iota$-primary polynomials in $\mathbb{Z}_{p^k}[x]$, we may consider $(x-\alpha)$-primary polynomials in $\mathbb{Z}[x]$. The rest of this section makes this idea more precise.

Let $R = \mathbb{Z}_{p^k}$ and let $\iota \in \mathbb{Z}_p[x]$ be a monic irreducible polynomial of degree $d$. Let $f \in R[x]$ be monic and such that $f = \iota$. Then, $f$ is irreducible in $R[x]$ and $\deg(f) = d$. Let $S = R[x]/(f)$.

We know that $R$ is a finite local ring. In (Ganske and McDonald, 1973), Ganske and McDonald studied ring extensions of finite local rings. The following properties of $R$ and $S$ are consequences of their results:

- $S$ is a finite local ring (Ganske and McDonald, 1973, Cor. 3.8), with maximal ideal $pS$. Also, note that $S/pS \cong \mathbb{Z}_p[x]/(\iota) \cong \mathbb{F}_{p^d}$, the field with $p^d$ elements.
- $f$ has exactly $d$ distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ in $S$, and for each $1 \leq j \leq d$, $\alpha_j$ is a root of $\iota$ in $\mathbb{F}_{p^d}$ (Ganske and McDonald, 1973, Thms. 3.16, 3.18).
- $S$ is a Galois extension of $R$ in the following sense. Let $G = \text{Gal}(S/R)$ be the group of $S$-automorphisms that fix $R$. Then, $G$ is cyclic of order $d$, the elements of $G$ transitively permute the roots of $f$, and the subring of $S$ fixed by all the elements of $G$ is $R$ (Ganske and McDonald, 1973, Thms. 5.6, 5.11).
In light of these properties, we can simplify our notation a bit and let $S = \mathbb{Z}_{p^k}[\alpha]$, where $\alpha$ is a root of $f$. Then, $S/pS \cong \mathbb{Z}_p(\bar{\alpha}) \cong \mathbb{F}_{p^d}$. We can also prove the promised theorem that reduces our problem to the consideration of $(x - \bar{\alpha})$-primary polynomials.

**Theorem 6.1.** Let $D > 0$, let $\iota$ be an irreducible polynomial in $\mathbb{Z}_p[x]$ of degree $d$ and let

$$
\mathcal{P}_\iota = \{\iota\text{-primary polynomials in } \mathbb{Z}_p^k[x] \text{ of degree } \lfloor \frac{D}{d} \rfloor \}.
$$

Let $f \in \mathbb{Z}_p^k[x]$ be monic and such that $f = \iota$, and let $S = \mathbb{Z}_p^k[\alpha]$, where $\alpha$ is a root of $f$. Let

$$
\mathcal{P}_\alpha = \{(x - \bar{\alpha})\text{-primary polynomials in } S[x] \text{ of degree } \lfloor \frac{D}{d} \rfloor \}
$$

Then, $\delta(\mathcal{P}_\iota) = d\delta(\mathcal{P}_\alpha)$.

**Proof.** Let $L_\iota$ be an lcm for $\mathcal{P}_\iota$ and let $L_\alpha$ be an lcm for $\mathcal{P}_\alpha$. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the roots of $f$ in $S$. The polynomial $L_\alpha$ is $(x - \bar{\alpha})$-primary, so $L_\alpha = (x - \bar{\alpha})^e$ for some $e$, and $\deg(L_\alpha) = e$. For each $1 \leq j \leq d$, let $L_{\alpha_j}$ be the image of $L_\alpha$ under the automorphism in $\text{Gal}(S/\mathbb{Z}_p^k)$ sending $\alpha$ to $\alpha_j$. Then, $L_{\alpha_j}$ is an lcm for the set

$$
\mathcal{P}_{\alpha_j} = \{(x - \bar{\alpha}_j)\text{-primary polynomials in } S[x] \text{ of degree } \lfloor \frac{D}{d} \rfloor \}.
$$

Let $L' = L_{\alpha_1}L_{\alpha_2}\cdots L_{\alpha_d}$. Then, $L'$ is fixed by all the automorphisms of $S$ in $\text{Gal}(S/\mathbb{Z}_p^k)$, so $L' \in \mathbb{Z}_p^k[x]$.

Furthermore, by considering primary factorizations, we see that if $g \in \mathcal{P}_\iota$, then $g \mid L'$. So, $L'$ is a monic common multiple for $\mathcal{P}_\iota$; hence, $\delta(\mathcal{P}_\iota) \leq \deg(L') = d\delta(\mathcal{P}_\alpha)$.

Next, let $L_\iota = \ell_1\ell_2\cdots\ell_d$ be the primary factorization of $L_\iota$ in $S[x]$, where each $\ell_j$ is $(x - \bar{\alpha}_j)$-primary. If $g_j \in \mathcal{P}_{\alpha_j}$, then the product of the Galois conjugates of $g_j$ divides $L_\iota$, so $g_j \mid L_\iota$ and $g_j \mid \ell_j$ by Lemma 4.5. So, $\ell_j$ is a common multiple for $\mathcal{P}_{\alpha_j}$. Thus, $\deg(\ell_j) \geq \deg(L_{\alpha_j})$ and therefore $\delta(\mathcal{P}_\iota) \geq d\delta(\mathcal{P}_\alpha)$. \qed

### 7 The Case $\lfloor \frac{D}{\deg(\iota)} \rfloor = 1$

After Theorem 5.1, it was mentioned that to determine $\delta(\mathcal{P}(p^k, D))$, it suffices to find lcm’s for the $\iota$-primary polynomials in $\mathbb{Z}_{p^k}[x]$ of degree $\deg(\iota)\lfloor \frac{D}{\deg(\iota)} \rfloor$. 
where \( \iota \) runs along all the irreducible polynomials in \( \mathbb{Z}_p[x] \). In these circumstances, we achieve the best results when \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor = 1 \). To see why, assume that \( f \in \mathbb{Z}_{p^k}[x] \) is monic and \( \overline{f} = \iota \). Let \( \alpha \) be a root of \( f \), let \( S = \mathbb{Z}_{p^k}[\alpha] \), let

\[
\mathcal{P}_\alpha = \{(x - \overline{\alpha})\text{-primary polynomials in } S[x] \text{ of degree } \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor \},
\]

and let \( T = \{ \gamma \in S \mid \overline{\gamma} = \overline{\alpha} \} \). If \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor = 1 \), then \( \mathcal{P}_\alpha = \{x - \gamma \mid \gamma \in T\} \). In this case, a polynomial \( L \) is a common multiple for \( \mathcal{P}_\alpha \) if and only if \( L(\gamma) = 0 \) for all \( \gamma \in T \). Thus, when \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor = 1 \), common multiples for \( \mathcal{P}_\alpha \) may be characterized as those polynomials that kill everything in \( T \). This need not be the case if \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor > 1 \). For example, if \( k = D = 2 \), \( \iota = x \), and \( f = x \), then \( x^2 \) kills everything in \( T = p\mathbb{Z}_p^2 \), but \( x^2 \) is not a common multiple for \( \mathcal{P}_\alpha \) (in particular, \( x^2 \nmid x^2 + p \)). In Section 8 we will approach the case \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor > 1 \) by describing polynomials in \( \mathcal{P}_\alpha \) as those that kill certain matrices.

In Section 1, factorials were useful in finding \( \delta(\mathcal{P}^k(p^k,1)) \). In (Gunji and McQuillan, 1970), Gunji and McQuillan studied a generalization of the factorial to rings of algebraic integers. One of the tools they used was a variation on Legendre’s formula (1.4). We state this formula as presented in (Cahen and Chabert, 2006, Sec. 1.2). Let \( q \) be a power of a prime, and for a positive integer \( N \), define

\[
w_q(N) = \sum_{j \geq 1} \left\lceil \frac{N}{q^j} \right\rceil
\]

(7.1)

In (Bhargava, 1998), Bhargava further extended the notion of factorial to Dedekind domains. We can use \( w_q(N) \) and Bhargava’s results to get an exact value for \( \delta(\mathcal{P}_\iota) \) when \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor = 1 \).

**Theorem 7.2.** Let \( D > 0 \). Let \( d \) be such that \( \left\lfloor \frac{D}{d} \right\rfloor = 1 \), and let \( \iota \in \mathbb{Z}_p[x] \) be irreducible of degree \( d \). Let \( q = p^d \), and let \( N = \min_{m \in \mathbb{N}} \{ w_q(m) \geq k \} \). Let

\[
\mathcal{P}_\iota = \{ \iota\text{-primary polynomials in } \mathbb{Z}_{p^k}[x] \text{ of degree } d \}.
\]

Then, \( \delta(\mathcal{P}_\iota) = d(N q) \).

**Proof.** Let \( f \in \mathbb{Z}_{p^k}[x] \) be monic and such that \( \overline{f} = \iota \). Let \( \alpha \) be a root of \( f \), and let \( S = \mathbb{Z}_{p^k}[\alpha] \). Let

\[
\mathcal{P}_\alpha = \{(x - \overline{\alpha})\text{-primary polynomials in } S[x] \text{ of degree 1} \}.
\]
By Theorem 6.1, it suffices to show that $\delta(\mathcal{P}_a) = \frac{N}{q}$.

We first claim that $S$ is a quotient ring of a valuation domain. Indeed, if $F \in \mathbb{Z}(\omega)[x]$ is such that $\overline{F} = \omega$, then $B = \mathbb{Z}(\omega)[x]/(F)$ is a discrete valuation domain with maximal ideal $p = pB$ (Serre, 2000, Chap. 1, §6, Prop. 15), and $S \cong B/p^k$.

Use a tilde to denote passage from $B$ to $S$. Let $L \in B[x]$ be monic and such that $\overline{L}$ is an lcm for $\mathcal{P}_a$. Let $\ell = \deg(L)$, and let $e = \ell + w_q(\ell) = w_q(q\ell)$. Fix $a \in B$ such that $\overline{a} = \alpha$, and let $X = a + p = \{b \in B \mid b = \overline{b}\}$. By (Bhargava, 1998, Thm. 2), the ideal of $B$ generated by the values of $L$ on $X$ divides $p^e$. But $L(X) \subseteq p^k$, so $p^k \supseteq p^e$. Hence, $k \leq e = w_q(q\ell)$. By the minimality of $N$, we have $\frac{N}{q} \leq \ell = \delta(\mathcal{P}_a)$.

Now, by (Bhargava, 1998, Thm. 4), there exists a monic $H \in B[x]$ of degree $\frac{N}{q}$ such that $H(X) \subseteq p^k$. Since $\left\lfloor \frac{D}{q} \right\rfloor = 1$, this means that $\overline{H}$ is an lcm for $\mathcal{P}_a$. Hence, $\delta(\mathcal{P}_a) \leq \frac{N}{q}$. More directly, we can produce an lcm as follows.

Let $\mathfrak{M} = pS$ be the maximal ideal of $S$. Let $N$ have $q$-adic expansion $N = N_1q + N_2q^2 + \cdots + N_tq^t$. Let $T = \{\gamma \in S \mid \overline{\gamma} = \overline{\alpha}\}$, for each $1 \leq j \leq t$ let $\Gamma_j$ be a set of representatives for $S/\mathfrak{M}^j$, and let $T_j = \{\gamma \in \Gamma_j \mid \overline{\gamma} = \overline{\alpha}\}$. Define

$$g(x) = \prod_{1 \leq j \leq t} \left( \prod_{\gamma \in T_j} (x - \gamma) \right)^{N_j}.$$ 

Then, $\deg(g) = \frac{N}{q}$, and one may show that $g$ kills everything in $T$. Since $\left\lfloor \frac{D}{q} \right\rfloor = 1$, $g$ is a common multiple for $\mathcal{P}_a$. \hfill \Box

When $D$ and $d$ are such that $\left\lfloor \frac{D}{q} \right\rfloor = 1$, Bound (5.2) for $\mathcal{P}_r$ is $kd$. Bound (7.2) is usually better than this. For example, since $w_q(q^t) = q^{t-1} + \cdots + q + 1$, Bound (7.2) for $k = q^{t-1} + \cdots + q + 1$ is $dq^{t-1}$, whereas Bound (5.2) is $d(q^{t-1} + \cdots + q + 1)$.

8 The Case $\left\lfloor \frac{D}{\deg(I)} \right\rfloor > 1$

About notation: in this section, we will be dealing with expressions of the form $f(A)$, where $f$ is a polynomial and $A$ is a matrix. An equation such as $f(A) = A + 3$ should, technically, be written as $f(A) = A + 3I$, where $I$ is the identity matrix of proper dimension. However, to simplify notation, we suppress the $I$ and write only $f(A) = A + 3$. Similarly, if $A^m = pB$ for some matrix $B$, then we will say that $p$ (rather than $pI$) divides $A^m$. 

13
We begin by defining something akin to a valuation.

**Definition 8.1.** As in previous sections, let $S = \mathbb{Z}_p[\alpha]$ with maximal ideal $\mathfrak{m} = pS$. Let $m > 0$ and let $A \in M_m(S)$ be such that $\overline{A^m} = 0$ in $M_m(S/\mathfrak{m})$, but $\overline{A^{m-1}} \neq 0$. Let $f \in S[x]$.

If $f(A) \neq 0$, then factor $f(A) = p^{e_1}g(A)$, where $g \in S[x]$ and $g(A) \neq 0$. Then, there exists $e_2 \in \{0, 1, \ldots, m - 1\}$ that is maximal with respect to having $\overline{A^{m-e_2}g(A)} = 0$. We define $v_A(f) = me_1 + e_2$.

The idea behind this definition is that we wish to treat $A$ like an $m$th root of $p$ and use $v_A(f)$ to count the number of powers of $A$ in $f(A)$. For example, assume $A$ is such that $A^3 = 0$. Then $v_A(x^3) \geq 3$, since we could have $A^3 = p$, or $A^3 = pA$, or $A^3 = 0$, etc. Similarly, $v_A(x + p) \geq 1$, since $A^2(A + p)$ is known to be divisible by $p$, and thus we may think of $A + p$ as bearing one power of $A$.

It is straightforward to check that for $f, g \in S[x]$, we have $v_A(fg) \geq v_A(f) + v_A(g)$ and $v_A(f + g) \geq \min\{v_A(f), v_A(g)\}$; notice that these properties are reminiscent of the axioms for a valuation. Additionally—and most importantly for our purposes—we have the following.

**Lemma 8.2.** With $S$ as in Definition 8.1, let $\beta \in S$ and let $g \in S[x]$ be $(x - \beta)$-primary of degree $m$. Let $A$ be the companion matrix for $g$. Let $h \in S[x]$. Then, $g(x) | h(x - \beta)$ if and only if $v_{A-\beta}(h) \geq mk$.

**Proof.** Note that $(A - \beta)^m = 0$. We know that $g(x) | h(x - \beta)$ if and only if $h(A - \beta) = 0$, and this holds if and only if $v_{A-\beta}(h) \geq mk$. □

The use of Definition 8.1 and the constructions presented in this section are best introduced with an example.

**Example 8.3.** Let $P_x$ be the set of all the $x$-primary polynomials in $\mathbb{Z}_{3^k}[x]$ of degree 2. Bound (5.2) for $P_x$ is $2k$.

Let $f \in P_x$ and let $A$ be the companion matrix for $f$ in $M_2(\mathbb{Z}_{3^k})$; then, $A^2 = 0$ in $M_2(\mathbb{Z}_3)$. If $\ell$ is a potential lcm for $P_x$, to check that $f | \ell$, it suffices to show that $v_A(\ell) \geq 2k$.

Consider the polynomial

$$\ell_1(x) = x^2(x^2 + 3)(x^2 + 6).$$
Since \( A^2 \) is divisible by 3, we have \( v_A(\ell_1) \geq 6 \). However, since \( \overline{f} = x^2 \), we may write \( f(x) = x^2 + 3bx + 3c \) for some \( b, c \in \mathbb{Z}_{3^k}. \) Then, one of \( A^2, A^2 + 3, \) or \( A^2 + 6 \) is congruent mod 9 to \( f(A) - 3bA = -3bA \). This means that one of \( v_A(x^2), v_A(x^2 + 3), \) or \( v_A(x^2 + 6) \) is greater than or equal to 3. Hence, \( \ell_1(x) \) is a polynomial of degree 6 such that \( v_A(\ell_1) \geq 7 \).

Write \( 2k = k_0 + k_1(7) \), where \( 0 \leq k_0 < 7 \) and \( 0 \leq k_1, \) and take \( \ell(x) = x^{k_0}\ell_1(x)^{k_1}. \) Then, \( v_A(\ell) \geq 2k \), so \( \delta(P_x) \leq \deg(\ell) = k_0 + k_1(6). \)

In fact, for larger values of \( k \), we can do a bit better by using the polynomial

\[
\ell_2(x) = x^2(x^2 + 3)(x^2 + 6) \\
\times (x^2 + 3x)(x^2 + 3x + 3)(x^2 + 3x + 6) \\
\times (x^2 + 6x)(x^2 + 6x + 3)(x^2 + 6x + 6).
\]

Arguing as above, we have \( v_A(\ell_2) \geq 7 + 7 + 8 = 22 \). We get a better bound for the degree of an lcm for \( P_x \) by writing \( 2k = k_0 + k_1(7) + k_2(22) \), where we now have \( 0 \leq k_0 < 7, 0 \leq k_1 \leq 3, \) and \( 0 \leq k_2, \) and taking \( \ell(x) = x^{k_0}\ell_1(x)^{k_1}\ell_2(x)^{k_2}. \) Then, \( \delta(P_x) \leq \deg(\ell) = k_0 + k_1(6) + k_2(18). \)

In Example 8.3, we had \( \lfloor \frac{D}{d} \rfloor = 2. \) The construction above can be adapted to deal with the general case of \( P(p^k, D) \) and \( m = \lfloor \frac{D}{d} \rfloor \) once several changes are made.

As in previous sections, let \( D > 0 \) and let \( \iota \in \mathbb{Z}_{p^k}[x] \) be irreducible of degree \( d. \) Let \( m = \lfloor \frac{D}{d} \rfloor, \) and let

\[
P_\iota = \{ \iota \text{-primary polynomials in } \mathbb{Z}_{p^k}[x] \text{ of degree } dm \}.
\]

Let \( f \in \mathbb{Z}_{p^k}[x] \) be such that \( \overline{f} = \iota. \) Let \( \alpha \) be a root of \( f, \) let \( S = \mathbb{Z}_{p^k}[\alpha], \) and let \( \mathfrak{M} = pS \) be the maximal ideal of \( S. \) Let \( q = p^d, \) so that \( |S/\mathfrak{M}| = q. \)

Let \( \Gamma \subseteq S \) be a set of representatives for the residues in \( S/\mathfrak{M}^2, \) and let \( T = \{ \gamma \in \Gamma \mid \overline{\gamma} = 0 \}; \) then, \(|T| = q. \) For each \( 1 \leq j \leq m, \) let

\[
\psi_j(x) = \prod_{\gamma_0, \gamma_1, \ldots, \gamma_{j-1} \in T} (x^m + \gamma_{j-1}x^{j-1} + \cdots + \gamma_1x + \gamma_0).
\]

Then, \( \psi_1(x) = \prod_{\gamma_0 \in T}(x^m + \gamma_0) \) is analogous to \( \ell_1(x) \) in Example 8.3, and \( \psi_2(x) \) is analogous to \( \ell_2(x). \) Notice that \( \deg(\psi_j) = mq^j. \) Finally, let

\[
P_\alpha = \{ (x - \overline{\alpha}) \text{-primary polynomials in } S[x] \text{ of degree } m \}.
\]

We first prove a lemma regarding the \( \psi_j \) polynomials and elements of \( P_\alpha. \)
Lemma 8.4. With notation as above, let \( g \in \mathcal{P}_\alpha \) and let \( A \) be the companion matrix for \( g \) in \( M_m(S) \). Then, for each \( 1 \leq j \leq m \), \( v_{\alpha - \alpha}(\psi_j) \geq mq^j + q^{j-1} + \cdots + q + 1 \).

Proof. Since \( g \) is \((x - \alpha)\)-primary of degree \( m \), we may write
\[
g(x) = (x - \alpha)^m + p\beta_{m-1}(x - \alpha)^{m-1} + \cdots + p\beta_1(x - \alpha) + p\beta_0,
\]
where \( \beta_r \in S \) for each \( 0 \leq r \leq m - 1 \). Note that \((A - \alpha)^m = g(A)\) is 0 in \( M_m(S/\mathfrak{m}) \). Thus, \( p \) divides \((A - \alpha)^m\).

Let
\[
h(x) = g(x + \alpha) = x^m + p\beta_{m-1}x^{m-1} + \cdots + p\beta_1x + p\beta_0,
\]
and let \( B \) be the companion matrix for \( h \); then, \( p \) divides \( B^m \). Note that \( v_{\alpha - \alpha}(\psi_j) = v_B(\psi_j) \). So, WLOG, we may assume that
\[
g(x) = x^m + p\beta_{m-1}x^{m-1} + \cdots + p\beta_1x + p\beta_0
\]
and that \( p \) divides \( A^m \).

We proceed by induction on \( j \). The base case is \( j = 1 \), for which we have \( \psi_1(x) = \prod_{\gamma_0 \in T} (x^m + \gamma_0) \). Since each of the factors for \( \psi_1 \) is equivalent to \( g \) modulo \( \mathfrak{m} \), \( v_A(\psi_1) \geq mq \). However, there is exactly one \( \gamma'_0 \in T \) such that \( \gamma'_0 \) is equivalent to \( p\beta_0 \) modulo \( \mathfrak{m}^2 \). So, \( \gamma'_0 = p\beta_0 + p^2\beta'_0 \) for some \( \beta'_0 \in S \). Then, since \( g(A) = 0 \), we have
\[
A^m + \gamma'_0 = -(p\beta_{m-1}A^{m-1} + \cdots + p\beta_1A) + p^2\beta'_0
\]
Now, \( v_A(p^2\beta'_0) \geq 2m \) and for each \( 1 \leq r \leq m - 1 \), \( v_A(p\beta_rx^r) \geq m + r \). Thus, \( v_A(x^m + \gamma'_0) \geq m + 1 \). It follows that \( v_A(\psi_1) \geq mq + 1 \). This completes the base case of the induction.

Next, assume that the result holds for \( j \); we will show it also holds for \( j + 1 \). First, we will write \( \psi_{j+1} \) in a different way. By definition,
\[
\psi_j(x) = \prod_{\gamma_0, \gamma_1, \ldots, \gamma_{j-1} \in T} (x^m + \gamma_{j-1}x^{j-1} + \cdots + \gamma_1x + \gamma_0).
\]
Let \( \mathfrak{T} = \{ \gamma_{j-1}x^{j-1} + \cdots + \gamma_1x + \gamma_0 \mid \gamma_0, \gamma_1, \ldots, \gamma_{j-1} \in T \} \). Then,
\[
\psi_j(x) = \prod_{\tau \in \mathfrak{T}} (x^m + \tau)
\]
and 
\[ \psi_{j+1}(x) = \prod_{\gamma_j \in T} \left( \prod_{\tau \in \Sigma} (x^m + \gamma_j x^j + \tau) \right). \]

Let \( N = mq^j + q^{j-1} + \cdots + q + 1 \). By induction, \( v_A(\prod_{\tau \in \Sigma}(x^m + \tau)) \geq N \). Furthermore, for each \( \tau \in \Sigma \), we have \( v_A(x^m + \tau) \geq m + e_\tau \) for some \( 0 \leq e_\tau \leq j - 1 \), and the \( e_\tau \) are such that \( \sum_{\tau \in \Sigma}(m + e_\tau) \geq N \).

Since \( v_A(\gamma_j x^j) \geq m + j \), for each \( \tau \) we have \( v_A(x^m + \gamma_j x^j + \tau) \geq m + e_\tau \).

So, for each \( \gamma_j \in T \), \( v_A(\prod_{\tau \in \Sigma}(x^m + \gamma_j x^j + \tau)) \geq N \). Thus, \( v_A(\psi_{j+1}) \geq qN \).

Now, there is exactly one \( \gamma'_j \in T \) and one \( \tau' \in \Sigma \) such that \( \gamma'_j x^j + \tau' \) is equivalent to \( p\beta_j x^j + \cdots + p\beta_1 x + p\beta_0 \) modulo \( \mathfrak{M}^2 \). By following the same steps as in the base case, we can show that \( v_A(x^m + \gamma'_j x^j + \tau') \geq m + j \).

Hence, we effectively gain one extra power of \( A \) in \( \psi_{j+1}(A) \), and so
\[ v_A(\psi_{j+1}) \geq qN + 1 = mq^j + q^{j-1} + \cdots + q + 1, \]

as required. Thus, the lemma holds. \( \square \)

With Lemma 8.4 in hand, we can prove the following theorem, which generalizes the bounds found in Example 8.3

**Theorem 8.5.** Continue to use the notation given prior to Lemma 8.4. For each \( 1 \leq j \leq m \), let \( a_j = mq^j + q^{j-1} + \cdots + q + 1 \). Write \( mk \) in the form
\[ mk = k_0 + k_1 a_1 + \cdots + k_{m-1} a_{m-1} + k_m a_m, \]
where \( 0 \leq k_0 < a_1, 0 \leq k_j \leq q \) for \( 1 \leq j \leq m - 1 \), and \( 0 \leq k_m \). Then, \( \delta(\mathcal{P}_i) \leq d(k_0 + k_1 (mq) + k_2 (mq^2) + \cdots + k_m (mq^m)) \).

**Proof.** First, note that \( a_{j+1} = qa_j + 1 \) for each \( 1 \leq j \leq m - 1 \), so any value of \( mk \) will have a unique expansion of the type in the statement of the theorem. Second, because of Theorem 6.1, it suffices to show that \( \delta(\mathcal{P}_\alpha) \leq k_0 + k_1 (mq) + k_2 (mq^2) + \cdots + k_m (mq^m) \).

For each \( 1 \leq j \leq m \), let \( \psi_j \) be as defined prior to Lemma 8.4, and let
\[ \psi(x) = x^{k_0} \psi_1(x)^{k_1} \psi_2(x)^{k_2} \cdots \psi_m(x)^{k_m}. \]

Let \( g \in \mathcal{P}_\alpha \) and let \( A \) be the companion matrix for \( g \) in \( M_m(S) \). By Lemma 8.4, \( v_{A-\alpha}(\psi_j) \geq a_j \) for each \( j \). So, \( v_{A-\alpha}(\psi) \geq mk \). By Lemma 8.2, \( g(x) \) divides \( \psi(x - \alpha) \). Thus, \( \psi(x - \alpha) \) is a monic common multiple for \( \mathcal{P}_\alpha \); and
\[ \delta(\mathcal{P}_\alpha) \leq \deg(\psi(x - \alpha)) = k_0 + k_1 (mq) + k_2 (mq^2) + \cdots + k_m (mq^m). \] \( \square \)
With notation as in Theorem 8.5, notice that each \( mq^j < a_j \), so we have \( \deg(\psi) \leq mk \). Bound (5.2) for \( \delta(\mathcal{P}_i) \) is \( dmk \) and Bound (8.5) for \( \delta(\mathcal{P}_i) \) is \( d \deg(\psi) \), so Bound (8.5) will, in general, be better than Bound (5.2).

The construction used in Lemma 8.4 and Theorem 8.5 can be modified to potentially get better bounds. In defining our notation prior to Lemma 8.4, we let the set \( \Gamma \) consist of residue representatives for \( S/\mathfrak{M}^2 \). We could use residue representatives for \( S/\mathfrak{M}^3, S/\mathfrak{M}^4 \), or in general \( S/\mathfrak{M}^e \) for any \( e > 0 \). However, with the \( \psi_j \) polynomials defined in terms of residues for \( S/\mathfrak{M}^e \), computing lower bounds for \( v_A(\psi_j) \) becomes increasingly more complicated.

**Summary**

The end result of this paper is less a formula for \( \delta(\mathcal{P}(n, D)) \) than a procedure to find an upper bound. Proposition 1.3 and Theorem 5.1 reduce the problem to working with \( \mathcal{P}_i \), and Theorems 7.2 and 8.5 can be used to compute bounds for \( \delta(\mathcal{P}_i) \). Notice that Theorems 7.2 and 8.5 depend only upon the degree of an irreducible polynomial \( \iota \in \mathbb{Z}_p[x] \), and not on \( \iota \) itself. Thus, in practice, one could compute a bound for each degree \( d \) between 1 and \( D \), and then multiply this bound by the number of irreducible polynomials in \( \mathbb{Z}_p[x] \) of degree \( d \). A formula for this number is well-known; see, for instance, (Dummit and Foote, 2004, Sec. 13.4).

Two questions regarding this topic are worth mentioning:

- The theorems in (Bhargava, 1998) allowed us to get an exact value for \( \delta(\mathcal{P}_i) \) when \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor = 1 \). How can we get an exact value for \( \delta(\mathcal{P}_i) \) when \( \left\lfloor \frac{D}{\deg(\iota)} \right\rfloor > 1 \)?

- This paper specifically studied lcms for the sets \( \mathcal{P}(n, D) \) in \( \mathbb{Z}_n[x] \). To what extent do the results and techniques in this paper carry over to lcms for arbitrary finite subsets of \( \mathbb{Z}_n[x] \)?

**Acknowledgment**

The author would like to thank the referee for the many helpful suggestions made during the review process.
References


