2010

DIAGONAL FORMS AND THE RATIONALITY OF THE POINCARÉ SERIES

Dibyajyoti Deb
University of Kentucky, iamddeb@gmail.com

ABSTRACT OF DISSERTATION

Dibyajyoti Deb

The Graduate School
University of Kentucky
2010

DIAGONAL FORMS AND THE RATIONALITY OF THE POINCARÉ SERIES.

ABSTRACT OF DISSERTATION

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the College of Arts and Sciences at the University of Kentucky

By
Dibyajyoti Deb
Lexington, Kentucky

Director: Dr. David Leep, Professor of Mathematics
Lexington, Kentucky 2010

ABSTRACT OF DISSERTATION

DIAGONAL FORMS AND THE RATIONALITY OF THE POINCARÉ SERIES.

The Poincaré series, $P_y(f)$ of a polynomial f was first introduced by Borevich and Shafarevich in [BS66], where they conjectured, that the series is always rational. Denef and Igusa independently proved this conjecture. However it is still of interest to explicitly compute the Poincaré series in special cases. In this direction several people looked at diagonal polynomials with restrictions on the coefficients or the exponents and computed its Poincaré series. However in this dissertation we consider a general diagonal polynomial without any restrictions and explicitly compute its Poincaré series, thus extending results of Goldman, Wang and Han. In a separate chapter some new results are also presented that give a criterion for an element to be an m^{th} power in a complete discrete valuation ring.

KEYWORDS: number theory, Poincaré series, diagonal forms, p-adic numbers.

Author's signature: Dibyajyoti Deb

Date: August 5, 2010

DIAGONAL FORMS AND THE RATIONALITY OF THE POINCARÉ SERIES.

By
Dibyajyoti Deb

Director of Dissertation: David Leep

Director of Graduate Studies: Qiang Ye

Date: August 5, 2010

RULES FOR THE USE OF DISSERTATIONS

Name	Date

DISSERTATION

Dibyajyoti Deb

The Graduate School
University of Kentucky
2010

DIAGONAL FORMS AND THE RATIONALITY OF THE POINCARÉ SERIES.

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Dibyajyoti Deb
Lexington, Kentucky

Director: Dr. David Leep, Professor of Mathematics
Lexington, Kentucky 2010

Dedicated to my family, especially my parents and grandparents.

ACKNOWLEDGMENTS

The writing of this dissertation would not have been possible without the help and support of several people. First and foremost, I would like to thank my adviser, Prof. David Leep, for all of the advice, support, and encouragement that he provided throughout this process. I am thankful for the many hours he sacrificed and for his continual interest in helping me to learn and become a better mathematician. I would also like to thank Prof. Uwe Nagel, Prof. Edgar Enochs, Prof. Cidambi Srinivasan, and Prof. Margaret Schroeder for serving on my advisory committee, reading this dissertation, and providing helpful comments.

Last but not least I would like to thank my parents for their moral support and the mathematics department at the University of Kentucky for their financial support, without which this wouldn't have been possible.

Our greatest glory is not in never falling, but in rising every time we fall.

- Confucius (551 BC -479 BC)

TABLE OF CONTENTS

Chapter 1 Introduction

The Poincaré Series, $P_f(y)$ of a polynomial f is defined to be the formal power series given by

$$P_f(y) = \sum_{i=0}^{\infty} c_i y^i.$$

Here c_m denotes the number of solutions of the equation $f = 0$ in $\mathbb{Z}/p^m\mathbb{Z}$ with $c_0 = 1$. Z.I. Borevich and I.R. Shafarevich in [BS66] conjectured that $P_f(y)$ is always a rational function. The conjecture was proved by Igusa in [Igu79] and a second somewhat simpler proof was given in the appendix of [Igu77]. These proofs are nonconstructive and depend on Hironaka's theorem on resolution of singularities. D. Meuser in [Meu81] generalized Igusa's theorem to a system of polynomials. Jan Denef gave an additional proof in [Den84] that avoided Hironaka's theorem, but still used sophisticated methods.

It is still of interest to explicitly compute the Poincaré Series, at least in special cases. This was investigated by J.R. Goldman in [Gol83] and [Gol86] for strongly nondegenerate forms and algebraic curves all of whose singularities are "locally" of the form $\alpha x^a = \beta y^b$. The papers of Wang, [Wan92] and [Wan93] and Han in [Han99] considered the Poincaré series of diagonal polynomials. Let R denote a discrete valuation ring with maximal ideal generated by the prime element π and let R_π denote the completion of R with respect to the π-adic topology on R with a finite residue field. Let

$$f(x_1, \ldots, x_n) = \epsilon_1 x_1^{t_1} + \cdots + \epsilon_n x_n^{t_n} + b$$

where $\epsilon_1, \ldots, \epsilon_n \in R_\pi$, $t_1, \ldots, t_n$ are positive integers, and $b \in R_\pi$. Wang computed $P_f(y)$ in [Wan92] when $b = 0, R_\pi = \mathbb{Z}_p$, the ring of p-adic integers, and $\epsilon_1, \ldots, \epsilon_n$ are units in R_π. Wang generalized this computation in [Wan93] to the case when $b = 0, R_\pi$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, the field of p-adic integers, and $\epsilon_1, \ldots, \epsilon_n$ are units in R_π. Han considered the case when R is a discrete valuation ring with a finite residue field, $\epsilon_1, \ldots, \epsilon_n$ and the positive integers $t_1, \ldots, t_n$ are units in R_π (the case of so-called strongly nondegenerate diagonal polynomials), and $b \in R_\pi$ is arbitrary.

In this dissertation, $P_f(y)$ is computed for an arbitrary diagonal polynomial when R is a discrete valuation ring with char $R = 0$ and having a finite residue field and with no restrictions on $\epsilon_1, \ldots, \epsilon_n, t_1, \ldots, t_n$ or b.

In Chapter 2, a brief history of earlier work of Goldman, Wang and Han on this topic is outlined including their main results. In Chapter 3, some basics of local field theory are covered. These include sections on discrete valuations, completions and Hensel's lemma. In Chapter 4, we look at powers of elements in a complete discrete valuation ring. The result in this chapter is presented in Theorem 4.3.5, where it is shown that if $i > \frac{e}{p-1} + \gamma e$ and $x^m \equiv b \bmod \pi^i$ has a solution in R, then the equation $x^m = b$ has a solution in R_π, where R is a discrete valuation ring. In Chapter 5, the main results of this dissertation are outlined in Theorems 5.5.1 and 5.5.2, where the Poincaré series is computed for a general diagonal polynomial without any restrictions. In the next chapter a different formulation of c_m, the number of solutions of the diagonal polynomial is given. Finally in Chapter 7, a simple example is used to illustrate the results from the previous chapters.

Chapter 2 Brief History

Significant work have been done by Goldman, Wang and Qing in [Gol83], [Wan92], [Wan93] and [Han99] involving the Poincaré Series of certain polynomials with restrictions on the coefficients and exponents. Their results are discussed in the next few sections.

2.1 Work of J.R. Goldman

Definition 2.1.1. *Let R be a Unique Factorization Domain(UFD), π a prime element in R and let $A \in R^{(n)}$ be a solution of $f(x_1, \ldots, x_n) \equiv 0 \bmod \pi$. If $\frac{\partial f(A)}{\partial x_i} \equiv 0 \bmod \pi$ for all $1 \le i \le n$, then A is a singular solution of f otherwise A is nonsingular.*

Definition 2.1.2. *Let $F(x_1, \ldots, x_n)$ be a homogeneous polynomial such that the only singular solution of $F \equiv 0 \bmod \pi$ is $(0, 0, \ldots, 0)$. Then $F(x_1, \ldots, x_n)$ is called a strongly nondegenerate form.*

Examples of such forms include $\sum_{i=1}^{k} e_i x_i^d$, where $p \nmid d$ and the e_i are p-adic units, and $x^2 + y^2 + xy$ where $p \neq 2, 3$.

Here is a theorem due to Goldman where he computes an expression for the number of solutions of strongly nondegenerate forms of a certain degree and also computes the resulting Poincaré Series upto a polynomial.

Theorem 2.1.3 ([Gol83], p.588)**.** *Let $F(x_1, \ldots, x_n)$ be a strongly nondegenerate form of degree d with coefficients in $\mathbb{Z}_p$. Let c_m denote the number of solutions of $F = 0$ in $(\mathbb{Z}/p^m\mathbb{Z})^n$, with $c_0 = 1$. Then*

$$c_m = \begin{cases} (c_1 - 1)p^{(m-1)(n-1)} + p^{n(m-1)}, & 1 \le m \le d; \\ (c_1 - 1)p^{(m-1)(n-1)} + p^{n(d-1)}c_{m-d}, & m > d. \end{cases}$$

The Poincaré Series is given by

$$P_f(y) = \frac{R(y)}{(1-p^{n-1}y)(1-p^{n(d-1)}y^d)}$$

where $R(y)$ is a polynomial of degree d, which is effectively and easily computable.

Definition 2.1.4. *Let R be a UFD, π a prime element in R and let $F(x_1,\ldots,x_n) = a_1x_1^{l_1}+\ldots+a_nx_n^{l_n}+b$, with $\gcd(l_ia_i,\pi)=1$. Then F is called a* strongly nondegenerate *diagonal polynomial.*

In Goldman's theorem if we restrict F to the strongly nondegenerate diagonal polynomial $F(x_1,\ldots,x_n) = \varepsilon_1x_1^d+\cdots+\varepsilon_nx_n^d$, where $p\nmid d$, then we can explicitly compute the polynomial $R(y)$. It turns out to be

$$R(y) = 1-p^{n-1}y+(c_1-1)y+\sum_{i=0}^{d-2}(p^ny)^i(y-p^{n-1}y^2)$$

2.2 Work of J. Wang

Wang in [Wan92] considers a diagonal form

$$f(x) = a_1x_1^{d_1}+\cdots+a_nx_n^{d_n},$$

where $n,d_1,\ldots,d_n$ are positive integers and $a_1,\ldots,a_n$ are units in $\mathbb{Z}_p$. Let $d=\operatorname{lcm}\{d_1,\ldots,d_n\}$, $f_i = d/d_i$, $r=f_1+\cdots+f_n$ and $\bar{c}_m = p^{-m(n-1)}c_m$, where c_m is the number of solutions of the congruence $f(x)\equiv 0 \bmod p^m$. Here is the theorem due to Wang.

Theorem 2.2.1 ([Wan92])**.** *For any prime p and $f(x)$ as above, we have*

1. *For $m\ge 2$, $\bar{c}_{m+d} = c+p^{d-r}\bar{c}_m$;*

2. *the Poincaré Series is given by*

$$P_f(y) = \frac{(1-p^{n-1}y)(\sum_{i=0}^{d+1}c_iy^i)+cp^{(d+2)(n-1)}y^{d+2}-p^{dn-r}y^d(1-p^{n-1}y)(1+c_1y)}{(1-p^{n-1}y)(1-p^{dn-r}y^d)}$$

where $c=\bar{c}_{d+1}-p^{d-r}\bar{c}_1$ is a constant depending upon the polynomial $f(x)$.

Wang's proof of the above theorem uses properties of exponential sums. He simplifies the expression of the Poincaré series. This simplification is presented next.

Theorem 2.2.2 ([Wan92])**.** *Suppose that p is an odd prime or $p = 2$, $d_i \neq 2, 4$ for each i, $1 \leq i \leq s$. Then we have*

1. *For $m \geq 0$, $\bar{c}_{m+d} = c' + p^{d-r}\bar{c}_m$;*

2. *the Poincaré series is given by*

$$P_f(y) = \frac{(1 - p^{n-1}y)(\sum_{i=0}^{d-1} c_i y^i) + c' p^{d(n-1)} y^d}{(1 - p^{n-1}y)(1 - p^{dn-r}y^d)}$$

   where $c' = \bar{c}_{d-1} - p^{d-r-1}$ is a constant depending upon the polynomial $f(x)$.

2.3 Work of Q. Han

Han, on the other hand, considers a strongly nondegenerate polynomial with a constant involved and having different exponents. He also computes the Poincaré Series associated to it. Here is Han's result.

Theorem 2.3.1 ([Han99], p.271)**.** *Suppose that R is a UFD, π a prime element in R and $\mid R/(\pi) \mid \;= P$. Let $f(x_1, \ldots, x_n) = a_1 x_1^{l_1} + \ldots + a_n x_n^{l_n} - b$ be a strongly nondegenerate diagonal polynomial. If $b \neq 0$, let $b = \bar{b}\pi^l, \gcd(\bar{b}, \pi) = 1$; if $b = 0$, let $l = m$. Then the number of solutions c_m of*

$$a_1 x_1^{l_1} + \ldots + a_n x_n^{l_n} \equiv b \bmod \pi^m$$

is equal to

$$\begin{aligned} & (1 - \theta(l,m))P^{n(m-1)-[(m-1)/l_1]-\ldots-[(m-1)/l_n]} + P^{(n-1)(m-1)} \\ \times \Bigg(& \sum_{t=2}^{n} \sum_{1 \leq i_1 < \ldots < i_t \leq n} e(i_1, \ldots, i_n) \sum_{k=0}^{[(\min(m,l)-1)/[l_{i_1}, \ldots, l_{i_t}]]} P^{[l_{i_1}, \ldots, l_{i_t}]k - \sum_{j=1}^{n}[[l_{i_1}, \ldots, l_{i_t}]k/l_j]} \\ & + \theta(l,m) P^{l - \sum_{j=1}^{n}[l/l_j]} \sum_{t=1}^{n} \sum_{1 \leq i_1 < \ldots < i_t \leq n,\ [l_{i_1}, \ldots, l_{i_t}] \mid l} \bar{e}(i_1, \ldots, i_t) \Bigg), \end{aligned}$$

where $e(i_1, \dots, i_t)$ *and* $\bar{e}(i_1, \dots, i_t)$ *are the number of primitive solutions of*

$$a_{i_1} x_1^{l_{i_1}} + \ldots + a_{i_t} x_t^{l_{i_t}} \equiv 0 \bmod \pi$$

and

$$a_{i_1} x_1^{l_{i_1}} + \ldots + a_{i_t} x_t^{l_{i_t}} \equiv \bar{b} \bmod \pi$$

respectively, and

$$\theta(l, m) = \begin{cases} 0, & l \geq m; \\ 1, & l < m. \end{cases}$$

Han also precisely computes the Poincaré Series for the strongly nondegenerate polynomial $f(x_1, \dots, x_n)$ when $b = 0$. According to him if $d = \mathrm{lcm}(l_1, \dots, l_n)$, then the Poincaré Series is given by

$$P_f(y) = \frac{(c_d - P^{d(n-1/l_1-\ldots-1/l_n)}) y^d + (1 - P^{n-1} y) \sum_{i=0}^{d-1} c_i y^i}{(1 - P^{n-1} y)(1 - P^{d(n-1/l_1-\cdots-1/l_n)} y^d)}$$

The motivation for the work in this thesis arises out of the fact that the work of Wang, Goldman and Han does not give a complete picture of the Poincaré series of an arbitrary diagonal polynomial. There are some restrictions attached to all the theorems that we mentioned above.

In this thesis, an arbitrary diagonal polynomial given by

$$f(x_1, \dots, x_n) = \epsilon_1 x_1^{t_1} + \cdots + \epsilon_n x_n^{t_n} + b$$

over a discrete valuation ring R with a finite residue field is considered. There are no restrictions on $\epsilon_1, \dots, \epsilon_n, t_1, \dots, t_n$ or b. An expression is constructed for c_m, the number of solutions of the congruence

$$f(x_1, \dots, x_n) \equiv 0 \bmod \pi^m,$$

where π is a prime element in R that generates the maximal ideal. Finally the Poincaré Series of this diagonal polynomial is computed. A review of discrete valuation rings is presented in the next chapter.

Chapter 3 Discrete Valuation Ring

3.1 Discrete Valuations

Let K be any field. A discrete(non-Archimedean) valuation on K is a mapping $v : K\backslash\{0\} \to \mathbb{Z}$ with the additional value $v(0) = +\infty$, such that for any $x, y \in K$,

$$v(xy) = v(x) + v(y)$$

and

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

Given the field K with a valuation v, the set $R_v = \{x \in K : v(x) \geq 0\}$ is a ring with the unique maximal ideal $M_v = \{x \in K : v(x) > 0\}$. The set R_v is called the discrete valuation ring of v. The subgroup $U_v = U = \{x \in K^\times : v(x) = 0\}$ is the group of units of R_v. The quotient R_v/M_v is a field, and is called the residue field of the discrete valuation ring R_v. If we fix any $\rho \in (0, 1) \subset \mathbb{R}$, then the valuation v induces a norm on K, defined as $\mid x \mid_v = \rho^{v(x)}$, for any $x \in K\backslash\{0\}$ (with $\mid 0 \mid_v$ set to be 0). The metric induced by such a norm makes K an ultrametric space and its topology is independent of the choice of ρ. We will refer to this topology directly in terms of v in later sections.

Choose an element $\pi \in K$ such that $v(\pi) = 1$. Then every $a \in K^\times$ has a unique representation

$$a = \pi^n u, n \in \mathbb{Z}, u \in U$$

It is also seen that $M_v = (\pi)$, and every non-zero ideal of the ring R_v is the set $M_v^n = \{x \in R_v : v(x) \geq n\}$ for positive values of n. Therefore $M_v^n = (\pi^n)$. Such an element π is called the *uniformizing element* of R_v (or *uniformizer*; Weil [Wei74] calls it a "prime element").

3.2 Completion

Let R be a discrete valuation ring, with uniformizer π and valuation v. Let K denote the field of fractions of R, $K^\times$ the multiplicative group of non-zero elements of K. If $x \in K^\times$, one can again write x in the form

$$x = \pi^n u, n \in \mathbb{Z}$$

and set $v(x) = n$. The properties from the previous section are easily verified making v into a discrete valuation which we denote from now on by v_π. The norm $\mid \quad \mid_v$ induced by the valuation v on the field K induces a topology in which the basis for the neighbourhoods of α are the "open spheres"

$$S_\delta(\alpha) = \{x \in K : \mid x - \alpha \mid_v < \delta\}$$

for $\delta > 0$ and $\alpha \in K$.

So one can introduce the notion of a *fundamental sequence* in order to define completion.

Definition 3.2.1. *A sequence $(\alpha_n)_{n\geq 0}$ of elements of K is called a fundamental sequence if for every real number c, there is a $M \geq 0$ such that $v(\alpha_n - \alpha_m) \geq c$ for $m, n \geq M$.*

If (α_n) is a fundamental sequence then for every integer r there is a n_r, such that for all $n, m \geq n_r$ we have $v(\alpha_n - \alpha_m) \geq r$. We can assume that $n_1 \leq n_2 \leq \ldots$. If for every r, there is a $n'_r \geq n_r$, such that $v(\alpha_{n'_r}) \neq v(\alpha_{n'_r+1})$, then $v(\alpha_{n'_r}) \geq r$ and $v(\alpha_n) \geq r$ for $n \geq n'_r$, and hence $\lim v(\alpha_n) = +\infty$. Otherwise $\lim v(\alpha_n)$ is finite.

Lemma 3.2.2. *The set A of all fundamental sequences form a ring with respect to component wise addition and multiplication. The set of all fundamental sequences $(\alpha_n)_{n\geq 0}$ with $\alpha_n \to 0$ as $n \to +\infty$ forms a maximal ideal M of A. The field A/M is a discrete valuation field with its discrete valuation $\hat{v}$ defined by $\hat{v}((\alpha_n)) = \lim v(\alpha_n)$ for a fundamental sequence $(\alpha_n)_{n\geq 0}$.*

Proof. A sketch of the proof is as follows. It suffices to show that M is a maximal ideal of A. Let $(\alpha_n)_{n\geq 0}$ be a fundamental sequence with $\alpha_n \not\to 0$ as $n \to +\infty$. Hence, there is an $n_0 \geq 0$ such that $\alpha_n \neq 0$ for $n \geq n_0$. Put $\beta_n = 0$ for $n < n_0$ and $\beta_n = \alpha_n^{-1}$ for $n \geq n_0$. Then $(\beta_n)_{n\geq 0}$ is a fundamental sequence and $(\alpha_n)(\beta_n) \in (1) + M$. Therefore M is maximal. □

Definition 3.2.3. *The quotient field A/M is called the completion of R with respect to the valuation v, and is denoted by $\widehat{R_v}$ with valuation $\hat{v}$ derived from above. $\{a_n\}$ is written as the coset of the fundamental sequence (a_n).*

Theorem 3.2.4. *$\widehat{R_v}$ is complete with respect to the valuation $\hat{v}$. Moreover, R can be identified with a dense subring of $\widehat{R_v}$.*

Proof. First observe that for $a \in R$, the constant sequence $(a_n) = (a)$ is fundamental and so we obtain the element $\{a\}$ in $\widehat{R_v}$; this allows us to embed R as a subring of $\widehat{R_v}$. We will identify R with its image without further comment; thus we will often use $a \in R$ to denote the element $\{a\} \in \widehat{R_v}$. It is easy to verify that if (a_n) is a fundamental sequence in R with respect to v, then (a_n) is also a fundamental sequence in $\widehat{R_v}$ with respect to $\hat{v}$. Of course it may not have a limit in R, but it always has a limit in $\widehat{R_v}$, namely the element $\{a_n\}$ by definition on $\widehat{R_v}$.

Now suppose that (a_n) is a fundamental sequence in $\widehat{R_v}$ with respect to the norm $\hat{v}$. Then we must show that there is an element $\alpha \in \widehat{R_v}$ for which

$$\lim_{n\to\infty} |\alpha_n|_{\hat{v}} = \alpha.$$

Notice that each α_m is in fact equivalence class of a fundamental sequence (a_{mn}) in R with respect to the valuation v, hence if we consider each a_{mn} as an element of $\widehat{R_v}$ as above, we can write

$$\alpha_m = \lim_{n\to\infty} |a_{mn}|_{\hat{v}}. \tag{3.1}$$

We need to construct a fundamental sequence (c_n) in R with respect to v such that

$$\{c_n\} = \lim_{m\to\infty} |\alpha_m|_{\hat{v}}.$$

Then $\alpha = \{c_n\}$ is the required limit of (a_n).

Now for each m, by Equation (3.1) there is an M_m such that whenever $n > M_m$,

$$|\alpha_m - a_{mn}|_{\hat{v}} < \frac{1}{m}.$$

For each m we now choose an integer $k(m) > M_m$. We can assume that these integers are strictly increasing, hence

$$k(1) < k(2) < \cdots < k(m) < \cdots .$$

We define our sequence (c_n) by setting $c_n = a_{n\,k(n)}$. We must show it has the required properties.

Lemma 3.2.5. *(c_n) is fundamental with respect to v and hence $\hat{v}$.*

Proof. Let $\epsilon > 0$. As (α_n) is fundamental there is an M' such that if $n_1, n_2 > M'$ then

$$|\alpha_{n_1} - \alpha_{n_2}|_{\hat{v}} < \frac{\epsilon}{3}.$$

Thus

$$\begin{aligned} |c_{n_1} - c_{n_2}|_{\hat{v}} &= |(a_{n_1\,k(n_1)} - \alpha_{n_1}) + (\alpha_{n_1} - \alpha_{n_2}) + (\alpha_{n_2} - a_{n_2\,k(n_2)})|_{\hat{v}} \\ &\leq |(a_{n_1\,k(n_1)} - \alpha_{n_1})|_{\hat{v}} + |(\alpha_{n_1} - \alpha_{n_2})|_{\hat{v}} + |(\alpha_{n_2} - a_{n_2\,k(n_2)})|_{\hat{v}} \end{aligned}$$

If we now choose $M = \max\{M', 3/\epsilon\}$, then for $n_1, n_2 > M$, we have

$$|c_{n_1} - c_{n_2}|_{\hat{v}} < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon,$$

and so the sequence (c_n) is indeed fundamental. □

Lemma 3.2.6. $\lim_{m\to\infty} |\alpha_m|_{\hat{v}} = \{c_n\}.$

Proof. Let $\epsilon > 0$. Then denoting $\{c_n\}$ by γ we have

$$\begin{aligned} |\gamma - \alpha_m|_{\hat{v}} &= |(\gamma - a_{m\,k(m)}) + (a_{m\,k(m)} - \alpha_m)|_{\hat{v}} \\ &\leq |(\gamma - a_{m\,k(m)})|_{\hat{v}} + |(a_{m\,k(m)} - \alpha_m)|_{\hat{v}} \\ &= \lim_{n\to\infty} |(a_{n\,k(n)} - a_{m\,k(m)})|_v + |(a_{m\,k(m)} - \alpha_m)|_{\hat{v}} \end{aligned}$$

Next choose M'' so that $M'' \geq 2/\epsilon$ and whenever $n_1, n_2 > M''$ then

$$|a_{n_1\,k(n_1)} - a_{n_2\,k(n_2)}|_v < \frac{\epsilon}{2}.$$

So for $m, n > M''$ we have

$$|(a_{m\,k(m)} - a_{n\,k(n)})|_v + |(a_{m\,k(m)} - \alpha_m)|_{\hat{v}} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Hence we see that

$$|(\gamma - \alpha_m)|_{\hat{v}} < \epsilon, \;\; \forall m > M''.$$

Lemmas 3.2.5 and 3.2.6 complete the proof of Theorem 3.2.4. □ □

3.3 Hensel's Lemma

Even though Hensel's Lemma is used in this thesis to *lift* solutions, it nevertheless can be stated in it's original form.

Theorem 3.3.1. *(Hensel's Lemma). Let R be a complete discrete valuation ring with uniformizer π, $(v(\pi) = 1)$. Let $\overline{p(x)}$ denote the coefficients of the polynomial $p(x)$ reduced $\bmod \pi$. Let $f(x) \in R[x]$ be monic. If $f(x) \equiv g_0(x)h_0(x) \bmod \pi$ for some monic $g_0(x), h_0(x) \in R[x]$, such that $\gcd(\overline{g_0(x)}, \overline{h_0(x)}) = 1$, then $f(x) = g(x)h(x)$ for some monic polynomials $g(x), h(x) \in R[x]$, where $g(x) \equiv g_0(x) \bmod \pi, h(x) \equiv h_0(x) \bmod \pi$.*

We will define a sequence of g_i's and h_i's that converge to the desired g and h. We will use the fact that if $f \equiv gh \bmod \pi^n$, $\forall\, n$ then $f = gh$.

Proof. By induction assume that there are $g_0(x), \ldots, g_{n-1}(x), h_0(x), \ldots, h_{n-1}(x) \in R[x]$ monic, such that $f(x) \equiv g_i(x)h_i(x) \bmod \pi^{i+1}$ and $g_i(x) \equiv g_{i-1}(x) \bmod \pi^i$, $h_i(x) \equiv h_{i-1}(x) \bmod \pi^i$ for $i = 1, \ldots, n$.

We want to find $g_n(x), h_n(x)$ such that $f(x) \equiv g_n(x)h_n(x) \bmod \pi^{n+1}$ and $g_n(x) \equiv g_{n-1}(x) \bmod \pi^n$, $h_n(x) \equiv h_{i-n}(x) \bmod \pi^n$.

To satisfy the above conditions we need $g_n(x) = g_{n-1}(x) + \pi^n u_n(x)$ and $h_n(x) = h_{n-1}(x) + \pi^n v_n(x)$ for some polynomials $u_n(x), v_n(x)$. So $g_n h_n \equiv g_{n-1}h_{n-1} + \pi^n(u_n h_{n-1} + v_n g_{n-1}) \bmod \pi^{n+1}$. The congruences $\bmod \pi^n$ are clear. We must show there exists u_n and v_n that satisfy the congruence to $f(x) \bmod \pi^{n+1}$.

We want $\frac{f(x)-g_{n-1}(x)h_{n-1}(x)}{\pi^n} \equiv u_n h_{n-1} + v_n g_{n-1} \bmod \pi$. Observe that $u_n h_{n-1} + v_n g_{n-1} \equiv u_n \overline{h_0} + v_n \overline{g_0} \bmod \pi$. Since $\gcd(\overline{g_0(x)}, \overline{h_0(x)}) = 1$ therefore there exists solutions for u_n and v_n. Consider the sequences $\{g_i\}_{i \in \mathbb{N}}$ and $\{h_i\}_{i \in \mathbb{N}}$. These are fundamental sequences. Since R is complete therefore these sequences converge in R. If g and h are their respective limits then $f = gh$ as desired. $\square$

The following corollary, rather than the theorem just proved is sometimes referred to as Hensel's Lemma.

Corollary 3.3.2. *Let $f(x) \in R[x]$, f monic, and $f(a) \equiv 0 \bmod \pi$ for some $a \in R$. Suppose that $f'(a) \not\equiv 0 \bmod \pi$, then there exists $b \in R$ such that $f(b) = 0$.*

Proof. Observe that $f'(a) \not\equiv 0 \bmod \pi$ means that a is a single root so the relatively prime condition is met and proof is done by setting $g_0(x) = x - a$. $\square$

The above corollary can be generalized to a polynomial of n variables. This is stated as a theorem next.

Theorem 3.3.3. *Let $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$. Let $\gamma_1, \ldots, \gamma_n \in R$ and $\delta \in \mathbb{Z}_{\geq 0}$, such that for some i, $f(\gamma_1, \ldots, \gamma_n) \equiv 0 \bmod \pi^{2\delta+1}$ and $\dfrac{\partial f}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \bmod \pi^{\delta+1}$. Then there exists $\theta_1, \ldots, \theta_n \in R$, such that $f(\theta_1, \ldots, \theta_n) = 0$ and $\theta_i \equiv \gamma_i \bmod \pi^{\delta+1}$ $(1 \leq i \leq n)$.*

Proof. See [BS66], p.42. □

Note that Corollary 3.3.2 is special case of the above theorem when $\delta = 0$.

Chapter 4 Powers of elements in Complete Discrete Valuation Rings

4.1 Introduction

Let R denote a discrete valuation ring with uniformizer π, and let R_π denote the completion of R with the π-adic topology on R. In this chapter we consider the interesting problem of determining the least value of i, if one exists, such that if $\alpha \in R_\pi$ is an m^{th} power modulo π^i, then α is an m^{th} power in R_π. This result is needed in the next chapter where we introduce our main problem. Our main result in this section is stated in Theorem 4.3.5.

Let U denote the group of units of R_π.

Proposition 4.1.1. $R/\pi^i R \cong R_\pi/\pi^i R_\pi$

Proof. Consider the map $\phi : R_\pi \to R/\pi^i R$, given by

$$a_0 + a_1\pi + a_2\pi^2 + \cdots \longmapsto a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1} \bmod \pi^i$$

It is easy to check that ϕ is a well defined homomorphism. Moreover Ker $\phi = \{a_0 + a_1\pi + \cdots \in R_\pi | a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1} \in \pi^i R\}$. Therefore it is clear that Ker $\phi \subseteq \pi^i R_\pi$. On the other hand if $a \in \pi^i R_\pi$, then $\phi(a) = 0$, in $R/\pi^i R$, therefore $a \in$ Ker ϕ. Therefore the proposition is proved by the isomorphism theorem. $\square$

For each integer $i \geq 1$, the set $U_i = 1 + \pi^i R_\pi$ is an open multiplicative subgroup of U (For example, $(1 - a\pi^i)^{-1} = 1 + \sum_{j=1}^{\infty} a^j \pi^{ij} \in U_i$), and $\bigcap_i U_i = 1$.

We assume that char $R = 0$ and that the residue field has char $R/(\pi) = p$. Then $p \in (\pi)$, and we let $p = \pi^e s$ where $e \in \mathbb{Z}_{>0}$ and $\pi \nmid s$.

Many aspects of this problem has been dealt with in [Art67](p.209-211), [FV02](p.14-16), [Has80](p.219-225, 228-232), and [Lan70](p.45-48). In [Art67] and [Lan70], the focus was to compute the index $[U : U^m]$. In [FV02], the focus was to study U_i/U_{i+1}.

Let $v_\pi : R \to \mathbb{Z} \cup \{\infty\}$ denote the valuation associated to π. Since π is the uniformizer therefore $v_\pi(\pi) = 1$. Hence $v_\pi(p) = e \geq 1$ and $s \in U$.

4.2 Prime powers of elements in R_π

Lemma 4.2.1. *Let $i \geq 0$ and let $\alpha \in R_\pi$.*

(1) If $\alpha^{p^i} \in U_1$, then $\alpha \in U_1$.

(2) $U_1^{p^i} = U^{p^i} \cap U_1$ for all $i \geq 0$.

Proof. (1) If $\alpha^{p^i} \in U_1$, then $\alpha \in U$. Let $\alpha \equiv b_0 \bmod \pi$. Then $1 \equiv \alpha^{p^i} \equiv b_0^{p^i} \bmod \pi$. Since char $R/(\pi) = p$, it follows that $b_0 \equiv 1 \bmod \pi$. Thus $\alpha \in U_1$.

(2) It is clear that $U_1^{p^i} \subseteq U^{p^i} \cap U_1$ for all $i \geq 0$. Let $\beta \in U^{p^i} \cap U_1$. Then $\beta = \alpha^{p^i}$ where $\alpha \in U$. Since $\alpha^{p^i} = \beta \in U_1$, it follows that $\alpha \in U_1$ by (1). Thus $\beta \in U_1^{p^i}$.

□

Lemma 4.2.2. *Let $i \geq 1$. Then*

(1) If $i \geq \frac{e}{p-1}$, then $U_i^p \subseteq U_{i+e}$.

(2) If $i < \frac{e}{p-1}$, then $U_i^p \subseteq U_{ip}$.

(3) If $i > \frac{e}{p-1}$, and $\alpha \in U_i \backslash U_{i+1}$, then $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$.

(4) If $i < \frac{e}{p-1}$, and $\alpha \in U_i \backslash U_{i+1}$, then $\alpha^p \in U_{ip} \backslash U_{ip+1}$. In particular $\alpha^p \notin U_{i+e}$.

Proof. Let $\alpha \in U_i$. Thus $\alpha = 1 + \pi^i \beta$ where $\beta \in R_\pi$. Then

$$\alpha^p = 1 + \left(\sum_{j=1}^{p-1} \binom{p}{j} \pi^{ij} \beta^j \right) + \pi^{ip} \beta^p.$$

Each of the terms in the inner sum has valuation at least $e + i$ because $p \mid \binom{p}{j}$ for $1 \leq j \leq p-1$ and $ij \geq i$. If $i \geq \frac{e}{p-1}$, then $e + i \leq ip$. Thus $\alpha^p \in U_{i+e}$. This proves (1).

If $i < e/(p-1)$, then $ip < e+i$ and again each of the terms in the inner sum has valuation at least $e+i$. Thus $\alpha^p \in U_{ip}$. This proves (2).

Now assume that $\alpha \in U_i \backslash U_{i+1}$. Then $\pi \nmid \beta$. The minimum of the valuations of each term in the inner sum is $e+i$ and this minimum valuation occurs when $j=1$.

If $i > e/(p-1)$, then $e+i < ip$, so $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$. If $i < e/(p-1)$, then $ip < e+i$, therefore $\alpha^p \in U_{ip} \backslash U_{ip+1}$. Since $ip+1 \le e+i$, if follows that $\alpha^p \notin U_{i+e}$.

□

Lemma 4.2.3. *Let $i \ge 1$ and let $\alpha \in R_\pi$.*

(1) If $i > e/(p-1), \alpha \in U_i$, and $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$, then $\alpha \notin U_{i+1}$.

(2) If $i \le e/(p-1)$ and $\alpha^p \in U_{ip} \backslash U_{ip+1}$, then $\alpha \in U_i \backslash U_{i+1}$.

Proof. For (1), since $\alpha \in U_i$, we may write $\alpha = 1 + \pi^j \beta$ where $\pi \nmid \beta$ and $i \le j$. Thus $\alpha \in U_j \backslash U_{j+1}$. Since $j \ge i > e/(p-1)$, it follows from Lemma 4.2.2(3) that $\alpha^p \in U_{j+e} \backslash U_{j+1+e}$. The assumptions imply that $j = i$, and thus $\alpha \notin U_{i+1}$. This proves (1).

For (2), we have $\alpha^p \in U_{ip} \subseteq U_1$. Thus $\alpha \in U_1$, by Lemma 4.2.1(1). Let $\alpha = 1 + \pi^j \beta$ where $\pi \nmid \beta$. Thus $\alpha \in U_j \backslash U_{j+1}$. If $j \ge e/(p-1)$, then $\alpha^p \in U_{j+e}$ by Lemma 4.2.2(1). Thus $j + e \le ip \le i + e$, so $j \le i < e/(p-1)$, a contradiction. Thus $j < e/(p-1)$. Then $\alpha^p \in U_{jp} \backslash U_{jp+1}$ by Lemma 4.2.2(4). Thus $j = i$, so $\alpha \in U_i \backslash U_{i+1}$. □

Proposition 4.2.4. *Let $i \ge 1$.*

(1) If $i > \frac{e}{p-1}$, then $U_i^p = U_{i+e}$.

(2) Suppose that $i = \frac{e}{p-1}$. Let $1 + \pi^{i+e}\beta \in U_{i+e}$ where $\beta \in R_\pi$. Then $1 + \pi^{i+e} \in U_i^p$ if and only if the congruence $x^p + sx - \beta \equiv 0 \bmod \pi$ has a solution in R.

Proof. If $i \ge \frac{e}{p-1}$, then $U_i^p \subseteq U_i + e$ by Lemma 4.2.2(1). First assume that $i \ge \frac{e}{p-1}$. Let $\beta \in R_\pi$ and let

$$f(x) = \frac{(1+\pi^i x)^p - (1 + \pi^{i+e}\beta)}{\pi^{i+e}}$$

Since $i \geq \frac{e}{p-1}$, it follows that $f(x) \in R_\pi[x]$. To see this, we observe as above that the valuation of each term in the numerator, after cancelling the 1's, is at least $e+i$. Since

$$f'(x) = \frac{p(1+\pi^i x)^{p-1}\pi^i}{\pi^{i+e}} = s(1+\pi^i x)^{p-1},$$

it follows that $f'(r) \not\equiv 0 \bmod \pi$ for all $r \in R$.

Now assume that $i > \frac{e}{p-1}$. Let $1+\pi^{i+e}\beta \in U_{i+e}$. We wish to find $\delta \in R_\pi$ such that $(1+\pi^i\delta)^p = 1+\pi^{i+e}\beta$. We will first find $\delta_0 \in R$ such that $f(\delta_0) \equiv 0 \bmod \pi$. Then $f'(\delta_0) \not\equiv 0\pi$ from above, so Hensel's lemma in Corollary 3.3.2 implies that there exists $\delta \in R_\pi$ such that $f(\delta) = 0$. This will imply that $(1+\pi^i\delta)^p = 1+\pi^{i+e}\beta$. We have

$$\begin{aligned}(1+\pi^i\delta_0)^p &= 1 + \left(\sum_{j=1}^{p-1}\binom{p}{j}\pi^{ij}\delta_0^j\right) + \pi^{ip}\delta_0^p \\ &\equiv 1 + p\pi^i\delta_0 + \pi^{ip}\delta_0^p \bmod \pi^{i+e+1} \\ &\equiv 1 + p\pi^i\delta_0 \equiv 1 + \pi^{i+e}s\delta_0 \bmod \pi^{i+e+1},\end{aligned}$$

because $i > e/(p-1)$ implies that $ip > i+e$. We choose $\delta_0 \in R$ such that $\delta_0 \equiv s^{-1}\beta \bmod \pi$. Then $\beta \equiv s\delta_0 \bmod \pi$, so

$$1+\pi^{i+e}\beta \equiv 1+\pi^{i+e}s\delta_0 \equiv (1+\pi^i\delta_0)^p \bmod \pi^{i+e+1}.$$

It follows that $f(\delta_0) \equiv 0 \bmod \pi$. This proves (1).

For (2), we follow the proof of (1) and note that the inequality $i > e/(p-1)$ was used in just one place. If $i = e/(p-1)$, then $ip = i+e$ and

$$\begin{aligned}(1+\pi^i\delta_0)^p &\equiv 1 + p\pi^i\delta_0 + \pi^{ip}\delta_0^p \bmod \pi^{i+e+1} \\ &\equiv 1 + \pi^{i+e}s\delta_0 + \pi^{ip}\delta_0^p \bmod \pi^{i+e+1} \\ &\equiv 1 + \pi^{i+e}(s\delta_0 + \delta_0^p) \bmod \pi^{i+e+1}.\end{aligned}$$

If δ_0 is a solution of $x^p + sx - \beta \equiv 0 \bmod \pi$, then $f(\delta_0) \equiv 0 \bmod \pi$. Conversely, if $1+\pi^{i+e}\beta = (1+\pi^i\delta)^p$, then δ is a solution of $x^p + sx - \beta \equiv 0 \bmod \pi$. This proves (2). $\square$

Proposition 4.2.5. *Let $i \geq 1$. Then the following statements hold.*

(1) If $i \leq e/(p-1)$, then $U^p \cap U_{ip} = U_i^p$.

(2) If $i \geq e/(p-1)$, then $U^p \cap U_{i+e} = U_i^p$.

Proof. First note that both statements are identical when $i = e/(p-1)$ because $i + e = ip$ in this case.

Assume that $i \leq e/(p-1)$. Then $U^p \cap U_{ip} \supseteq U_i^p$ by Lemma 4.2.2(2). Now let $\tau \in U^P \cap U_{ip}$. By Lemma 4.2.1(2), we have $\tau \in U_1^p$. Let $\tau = (1 + \pi^j\beta)^p$ where $\pi \nmid \beta$. Suppose that $j < i$. Then Lemma 4.2.2(4) implies that $\tau \in U_{jp} \backslash U_{jp+1}$. But $\tau \in U_{ip} \subseteq U_{jp+1}$ because $ip > jp + 1$. This is a contradiction, and thus $j \geq i$. Then $\tau \in U_j^p \subseteq U_i^p$. This proves (1).

If $i > e/(p-1)$, then $U_{i+e} = U_i^p$ by Proposition 4.2.4(1), so (2) follows easily in this case. The case $i = e/(p-1)$ was proved in (1). □

Proposition 4.2.6. *If $i > e/(p-1)$, then $U_i^{p^r} = U_{i+re}$ for all $r \geq 0$.*

Proof. The result is trivial for $r = 0$. For $r \geq 1$, we have by induction on r that

$$U_i^{p^r} = (U_i^{p^{r-1}})^p = U_{i+(r-1)e}^p = U_{i+re}$$

by Proposition 4.2.4(1) because $i + (r-1)e \geq i > e/(p-1)$. □

4.3 Arbitrary powers of elements in R_π

Proposition 4.3.1. *Let $m \geq 1$ be an integer. If $\gcd(m,p) = 1$, then $U_i^m = U_i$ for all $i \geq 1$.*

Proof. Clearly $U_i^m \subseteq U_i$. Now let $\alpha = 1 + \pi^i\beta \in U_i$. Let $f(x) = x^m - \alpha$. Then $f'(x) = mx^{m-1}$. Since $f(1) = -\pi^i\beta \equiv 0 \bmod \pi^i$ and $f'(1) = m \not\equiv 0 \bmod \pi$, Hensel's lemma in Corollary 3.3.2 implies that there exists $\eta \in R_\pi$ such that $0 = f(\eta) = \eta^m - \alpha$ and $\eta \equiv 1 \bmod \pi^i$. Thus $\eta \in U_i$, so $\alpha \in U_i^m$. Therefore $U_i = U_i^m$. □

Lemma 4.3.2. *Let G be an abelian group written multiplicatively. Let m, r, s be positive integers and let $m = rs$ where $\gcd(r, s) = 1$. Then $G^m = G^r \cap G^s$.*

Proof. It is clear that $G^m \subseteq G^r \cap G^s$ because $m = rs$. Now let $g \in G^r \cap G^s$. Then $g = g_1^r = g_2^s$ where $g_1, g_2 \in G$. Take integers k, l such that $kr + ls = 1$. Then

$$g = g^{kr+ls} = (g_2^s)^{kr}(g_1^r)^{ls} = (g_1^l g_2^k)^{rs} = (g_1^l g_2^k)^m.$$

Therefore $G^r \cap G^s \subseteq G^m$, so we have $G^m = G^r \cap G^s$. $\square$

Proposition 4.3.3. *Let m be a positive integer. Suppose that $m = p^\gamma s$ where $\gamma \geq 0$ and $p \nmid s$. Then $U_i \subseteq U^m$ for all $i > \frac{e}{p-1} + \gamma e$.*

Proof. We have $U_i = U_{i-\gamma e}^{p^\gamma} \subseteq U^{p^\gamma}$ by Proposition 4.2.6 because $i - \gamma e > \frac{e}{p-1}$. We also have $U_i = U_i^s \subseteq U^s$ by Proposition 4.3.1. Thus $U_i \subseteq U^{p^\gamma} \cap U^s = U^m$ by Lemma 4.3.2. $\square$

Theorem 4.3.4. *Let p be a prime number. Let $m = p^\gamma s$ where $\gamma \geq 0$ and $p \nmid s$. Consider the surjective group homomorphism*

$$f_i : U \to (R/\pi^i R)^*/((R/\pi^i R)^*)^m.$$

If $i > \frac{e}{p-1} + \gamma e$, then $\ker(f_i) = U^m$.

Proof. First we show that $\ker(f_i) = U_i U^m$ for all $i \geq 1$. It is obvious that $U_i U^m \subseteq \ker(f_i)$ for all $i \geq 1$. Now suppose that $b \in \ker(f_i)$. Then there exists $c \in R$ such that $\pi \nmid c$ and $b \equiv c^m \bmod \pi^i$. Let $\beta = b/c^m$. Then $\beta \equiv 1 \bmod \pi^i$, so $\beta \in U_i$. Thus $b = \beta c^m \in U_i U^m$ and it follows that $\ker(f_i) = U_i U^m$ for all $i \geq 1$. If $i > \frac{e}{p-1} + \gamma e$, then Proposition 4.3.3 implies that $U_i \subseteq U^m$ and thus $\ker(f_i) = U^m$. $\square$

We now present the main theorem of this section.

Theorem 4.3.5. *Keep the same notation from Theorem 4.3.4. Let $b \in R$ and assume that $\pi \nmid b$. Assume that $i > \frac{e}{p-1} + \gamma e$. If the congruence $x^m \equiv b \bmod \pi^i$ has a solution in R, then the equation $x^m = b$ has a solution in R_π.*

Proof. If the congruence $x^m \equiv b \bmod \pi^i$ has a solution in R, then $b \in \ker(f_i) = U^m$. $\square$

If $R/(\pi) \cong R_\pi/\pi R_\pi$ is finite, then $[U : U^m]$ can be computed easily as done in [Art67], pp. 209-211, and strengthened slightly in [Lan70], p. 47.

4.4 Primitive p^{th} roots of unity in R_π

It is clear that Lemma 4.2.2 doesn't seem to fully treat the case $i = e/(p-1)$. Also Lemma 4.2.3(1) seems to include an extra hypothesis ($\alpha \in U_i$). The statement in Proposition 4.2.4(2) deserves more development. In each case, this is better explained by knowing whether or not R_π contains a primitive p^{th} root of unity.

Lemma 4.4.1. *Suppose that R_π contains ζ, a primitive p^{th} root of 1. Then the following statements hold.*

(1) $p-1 \mid e$ and $\zeta \in U_{\frac{e}{p-1}} \backslash U_{\frac{e}{p-1}+1}$.

(2) $-p \in R_\pi^{p-1}$.

Proof. Let ζ be a primitive p^{th} root of 1. Let

$$h(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1 = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1}).$$

The $p = h(1) = (1 - \zeta) \cdots (1 - \zeta^{p-1})$. We have $(1 - \zeta^i)/(1 - \zeta^j) \in \mathbb{Z}[\zeta]$ for all $i, j \in \{1, 2, \ldots, p-1\}$. Thus $(1-\zeta^i)/(1-\zeta^j) \in U$. It follows that $v_\pi(1-\zeta^i) = v_\pi(1-\zeta^j)$, and thus $(p-1)v_\pi(1-\zeta) = v_\pi(p) = e$. Therefore $v_\pi(1-\zeta) = e/(p-1) \in \mathbb{Z}_{>0}$. Let $\alpha = 1 - \zeta$. Then $\zeta = 1 - \alpha \in U_{\frac{e}{p-1}} \backslash U_{\frac{e}{p-1}+1}$. This proves (1).

We have

$$\begin{aligned} p &= (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1}) \\ &= (1-\zeta)^{p-1}\left(\frac{1-\zeta^2}{1-\zeta}\right)\cdots\left(\frac{1-\zeta^{p-1}}{1-\zeta}\right) = (1-\zeta)^{p-1}A, \end{aligned}$$

where $A = (1+\zeta)(1+\zeta+\zeta^2)\cdots(1+\zeta+\zeta^2+\cdots\zeta^{p-2}) \in R_\pi$. We have $\zeta \equiv 1 \bmod \pi$ because $v_\pi(1-\zeta) \in \mathbb{Z}_{>0}$. It follows that

$$A \equiv 2 \cdot 3 \cdots (p-1) \equiv (p-1)! \equiv -1 \bmod \pi$$

because $\pi \mid p$. Since $\dfrac{p}{(1-\zeta)^{p-1}} = A \equiv -1 \bmod \pi$ and $\gcd(p, p-1) = 1$, it follows that $\dfrac{-p}{(1-\zeta)^{p-1}} \in U_1 = U_1^{p-1}$. Then $\dfrac{-p}{(1-\zeta)^{p-1}} = \eta^{p-1}$ where $\eta \in U_1$. Thus $-p = (\eta(1-\zeta))^{p-1} \in R_\pi^{p-1}$. This proves (2). □

Suppose that R_π contains a primitive p^{th} root of unity ζ. Then Lemma 4.2.2 does not contain a full statement for the case $i = \frac{e}{p-1}$ because $\zeta \in U_i \backslash U_{i+1}$ but $\zeta^p = 1 \in U_j$ for all $j \geq 1$. In Lemma 4.2.3(1), the hypothesis that $\alpha \in U_i$ is necessary because if $\alpha \in U_i$, where $i > \frac{e}{p-1}$, then $(\zeta\alpha)^p = \alpha^p$ but $\zeta\alpha \notin U_i$.

Let k denote the residue field $R/(\pi)$. If $a \in R_\pi$, let $\bar{a}$ denote the image of a in k. Let $\theta : k \to k$ be the additive homomorphism defined by $\theta(c) = c^p + sc$.

Proposition 4.4.2. *The following statements are equivalent.*

(1) R_π contains a primitive p^{th} root of unity.

(2) $p-1 \mid e$ and $-s \in U^{p-1}$.

(3) $p-1 \mid e$ and $\overline{-s} \in k^{p-1}$.

(4) $-p \in R_\pi^{p-1}$.

(5) θ is not injective.

Proof. The equivalence of (3) and (5) is immediate. We shall prove (4) ⇒ (2) ⇒ (3) ⇒ (1) ⇒ (4).

Assume that (4) holds. Let $-p = \tau^{p-1}$ where $\tau \in R_\pi$. Then $e = v_\pi(-p) = (p-1)v_\pi(\tau)$, so $(p-1) \mid e$. This gives

$$-s = \frac{-p}{\pi^e} = \left(\frac{\tau}{\pi^{e/(p-1)}}\right)^{p-1} \in U^{p-1}.$$

Thus (2) holds. It is obvious that (2) implies (3).

Assume that (3) holds. Then there exists $\beta \in U$ such that $\beta^{p-1} \equiv -s \bmod \pi$. Let $i = e/(p-1)$. Let $\alpha = 1 + \beta\pi^i$. Then $\alpha \in U_i \backslash U_{i+1}$. Since $ip = i + e$, we have

$$\alpha^p = (1 + \beta\pi^i)^p \equiv 1 + (s\beta + \beta^p)\pi^{i+e} \equiv 1 \bmod \pi^{i+e+1}.$$

Thus $\alpha^p \in U_{i+e+1} = U_{i+1}^p$ by Proposition 4.2.4(1). Then $\alpha^p = \delta^p$ where $\delta \in U_{i+1}$. Since $\alpha \notin U_{i+1}$, we have $\alpha/\delta \in U_1, \alpha/\delta \neq 1, (\alpha/\delta)^p = 1$. Thus α/δ is a primitive p^{th} root of unity in R_π. Thus (1) holds.

Finally, Lemma 4.4.1(2) shows that (1) implies (4). $\square$

Proposition 4.4.3. *Assume that $p - 1 \mid e$ and let $i = \frac{e}{p-1}$. Assume also that k is a finite field. Then the following statements are equivalent.*

(1) $U_i^p = U_{i+e}$

(2) The congruence $x^p + sx - \beta \equiv 0 \bmod \pi$ has a solution in R for all $\beta \in R$.

(3) θ is surjective.

(4) R_π does not contain a primitive p^{th} root of unity.

(5) $\overline{-s} \notin k^{p-1}$

(6) θ is injective.

Proof. The proof of Proposition 4.2.4(2) shows that (1) and (2) are equivalent. The equivalence of (2) and (3) is immediate. Proposition 4.4.2 implies that (4), (5), and (6) are equivalent. Finally, (3) and (6) are equivalent because k is finite. $\square$

We now obtain the following supplement to Lemmas 4.2.2 and 4.2.3.

Corollary 4.4.4. *Assume that R_π does not contain a primitive p^{th} root of unity.*

(1) If $i = e/(p-1) \in \mathbb{Z}_{>0}$ and $\alpha \in U_i \backslash U_{i+1}$, then $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$.

(2) *If* $i > e/(p-1)$ *and* $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$*, then* $\alpha \in U_i \backslash U_{i+1}$*.*

Proof. We refer to the proof of Lemma 4.2.2. Since $i = e/(p-1)$ and $\alpha \in U_i \backslash_{i+1}$, we have $\pi \nmid \beta$ and so

$$\alpha^p \equiv 1 + (\beta^p + s\beta)\pi^{i+e} \bmod \pi^{i+e+1}.$$

Then equivalence of (4) and (5) in Proposition 4.4.3 (or (1) and (3) in Proposition 4.4.2) implies that $\beta^p + s\beta \not\equiv 0 \bmod \pi$. Thus $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$. This proves (1).

Now assume that $i > e/(p-1)$ and $\alpha^p \in U_{i+e} \backslash U_{i+1+e}$. We have $\alpha \in U_1$ by Lemma 4.2.1(1). Assume that $\alpha \in U_j \backslash U_{j+1}$ where $j \geq 1$. First suppose that $j \leq e/(p-1)$. Then $\alpha^p \in U_{jp} \backslash U_{jp+1}$ by Lemma 4.2.2(4). Then $i+e = jp \leq e+j$, so $i \leq j \leq e/(p-1)$, which is impossible. Thus $j > e/(p-1)$. Then $\alpha^p \in U_{j+e} \backslash U_{j+e+1}$ by Lemma 4.2.2(3). It follows that $j = i$, so $\alpha \in U_i \backslash U_{i+1}$. □

4.5 Supplement to Section 2

In this section we use information of roots of unity from the previous section to extend Propositions 4.2.5 and 4.2.6. The first result concerns Proposition 4.2.6 for the case $i = e/(p-1)$.

Proposition 4.5.1. *Assume that* $i = e/(p-1)$*.*

(1) $U_i^{p^r} \subseteq U_{i+re}$ *for all* $r \geq 0$*.*

(2) *The following statements are equivalent.*

(a) $U_i^{p^r} = U_{i+re}$ *for all* $r \geq 0$*.*

(b) $U_i^{p^r} = U_{i+re}$ *for some value of* $r \geq 1$*.*

(c) $U_i^{p^r} = U_{i+re}$ *for* $r = 1$*. (That is,* $U_i^p = U_{i+e}$*.)*

Proof. (1) The statement is trivial for $r = 0$ and holds for $r = 1$ by Lemma 4.2.2 (1). Now assume that $r \geq 2$. The case $r = 1$ and Proposition 4.2.6 imply that

$$U_i^{p^r} = (U_i^p)^{p^{r-1}} \subseteq U_{i+e}^{p^{r-1}} = U_{i+e+(r-1)e} = U_{i+re}.$$

(2) It is trivial that (a) implies (b). Next we assume that (c) and prove (a). The case $r = 0$ in (a) is trivial. The case $r = 1$ in (a) follows from (c). Now assume that $r \geq 2$. Then (c) and Proposition 4.2.6 imply that

$$U_i^{p^r} = (U_i^p)^{p^{r-1}} = (U_{i+e})^{p^{r-1}} = U_{i+e+(r-1)e} = U_{i+re}.$$

Now we prove that (b) implies (c). We can assume that $r \geq 2$. We have $U_i^p \subseteq U_{i+e}$ by Lemma 4.2.2 (1). For the opposite inclusion, let $\beta \in U_{i+e}$. Then

$$\beta^{p^{r-1}} \in U_{i+e}^{p^{r-1}} = U_{i+e+(r-1)e} = U_{i+re} = U_i^{p^r}.$$

Then $\beta^{p^{r-1}} = \alpha^{p^r}$ where $\alpha \in U_i$. Let $\lambda = \beta/\alpha^p$. Then $\beta = \alpha^p\lambda$ and $\lambda^{p^{r-1}} = 1$. We have $\alpha^p \in U_{i+e}$ by Lemma 4.2.2 (1) and $\beta \in U_{i+e}$. Then $\lambda \in U_{i+e}$. If $\lambda \neq 1$, then for some j satisfying $1 \leq j \leq r-2$, we have $\lambda^{p^j} = \zeta$. It follows that $\zeta = \lambda^{p^j} \in U_{i+e}$, which contradicts Lemma 4.4.1 (1). Thus $\lambda = 1$, so $\beta = \alpha^p$. Therefore, $\beta \in U^p \cap U_{i+e} = U_i^p$ by Proposition 4.2.5 (2). This proves (c). $\square$

Next we consider Proposition 4.2.5 and try to extend the result to cover $(p^r)^{th}$ powers.

Proposition 4.5.2. *(1) If $i > e/(p-1)$, then $U^{p^r} \cap U_{i+re} = U_i^{p^r}$.*

(2) If $i = e/(p-1)$ and $U_{i+e} = U_i^p$, then $U^{p^r} \cap U_{i+re} = U_i^{p^r}$.

Proof. (1) Proposition 4.2.6 implies that

$$U^{p^r} \cap U_{i+re} = U^{p^r} \cap U_i^{p^r} = U_i^{p^r}.$$

(2) Proposition 4.5.1 (2) shows that the proof in (1) works again in this case. $\square$

Chapter 5 The Poincaré Series of a Diagonal Polynomial

It was mentioned in an earlier chapter that the work of Wang, Goldman and Han does not give us a complete picture of the Poincaré series of a diagonal polynomial due to restrictions on the diagonal polynomial itself. In this chapter we finally look into an arbitrary general diagonal polynomial without any restrictions and compute it's Poincaré series.

5.1 Preliminary Results

Let R denote a unique factorization domain (UFD) with maximal ideal generated by a prime element π and let R_π denote the completion of R with respect to this valuation. Assume that the residue field $R/(\pi)$ is finite with cardinality q. Let U denote the group of units of R_π and let char $R/(\pi) = p$.

Theorem 5.1.1. *Let $R/(\pi) = \{\bar{a} \mid a \in I \subset R\}$. Then*

$$R/(\pi^m) = \{\overline{a_0 + a_1\pi + \cdots + a_{m-1}\pi^{m-1}} \mid a_i \in I\}.$$

Proof. By induction on m. The case where $m = 1$ is trivial. We now assume that the theorem is true for $m = k$. Then any element a of R can be written as

$$a_0 + a_1\pi + \cdots + a_{k-1}\pi^{k-1} + \lambda\pi^k, \quad a_i \in I, \lambda \in R.$$

From the condition of the theorem, there exists $a_k \in I$ and $\mu \in R$ such that $\lambda = a_k + \mu\pi$. Thus

$$a = a_0 + a_1\pi + \cdots + a_k\pi^k + \mu\pi^{k+1}.$$

If we also have $a = b_0 + b_1\pi + \cdots + b_k\pi^k + \mu'\pi^{k+1},\ b_i \in I, \mu' \in R$, then $a_0 \equiv b_0 \bmod \pi$. So $a_0 = b_0$, since $a_0, b_0 \in I$. Therefore, $a_1 + \cdots + a_k\pi^{k-1} \equiv b_1 + \cdots + b_k\pi^{k-1} \bmod \pi^k$. By the inductive hypothesis, $a_i = b_i, i = 1, \ldots, k$. We therefore conclude that $R/(\pi^{k+1}) =$

$\{\overline{a_0 + a_1\pi + \cdots + a_k\pi^k} \mid a_i \in I\}$. This the theorem is valid for $m = k + 1$. This completes the proof. $\square$

Corollary 5.1.2. *If $R/(\pi)$ is finite and $\mid R/(\pi) \mid = q$, then $\mid R/(\pi^m) \mid = q^m$.*

Proof. Since $\mid R/(\pi) \mid = q$, hence each a_i in Theorem 5.1.1 has q choices, therefore $\mid R/(\pi^m) \mid = q^m$. $\square$

If char $R = 0$ and char $R/(\pi) = p$, then $p \in (\pi)$, and we let $p = \pi^e s$ where $e \in \mathbb{Z}_{>0}$ and $\pi \nmid s$.

The next proposition plays a crucial role in the proof of the rationality of the Poincaré series.

Proposition 5.1.3. *Assume that* char $R = 0$. *Let $b \in U$ and let $t \in \mathbb{Z}_{>0}$. Then there exists a positive integer M depending on t such that the following two statements hold.*

(1) If the congruence $x^t \equiv b \bmod \pi^M$ has a solution in R, then the congruence $x^t \equiv b \bmod \pi^m$ has a solution in R for all $m \geq M$. In particular, $b \in U^t$.

(2) If the congruence $x^t \equiv b \bmod \pi^M$ has solution in R, then the number of solutions in $R/(\pi^m)$ to the congruence $x^t \equiv b \bmod \pi^m$ is the same for all $m \geq M$. This number of solutions equals $[U : U^t]$.

Proof. Suppose that $t = p^\gamma d$ where $\gamma \geq 0$ and $d \in \mathbb{Z}_{>0}$ with $p \nmid d$. Then $\pi \nmid d$ in R_π. We will show that the positive integer $M = 2e\gamma + 1$ satisfies (1) and (2).

Let $G(x) = x^t - b$ and suppose that $G(a) \equiv 0 \bmod \pi^m$ where $a \in R$ and $m \geq M = 2e\gamma + 1$. Note that $a \in U$. Let $G(a) = \pi^m \beta$ where $\beta \in R$. Let $z \in R$, which will be determined below. Then

$$\begin{aligned} G(a+z\pi^{m-e\gamma}) &= (a+z\pi^{m-e\gamma})^t - b \\ &= a^t + ta^{t-1}z\pi^{m-e\gamma} + \pi^{2(m-e\gamma)}\eta - b, \text{ for some } \eta \in R_\pi, \\ &\equiv (a^t - b) + ta^{t-1}z\pi^{m-e\gamma} \bmod \pi^{m+1}, \text{ because } 2(m-e\gamma) \geq m+1, \\ &\equiv \pi^m\beta + a^{t-1}(\pi^e s)^\gamma d\pi^{m-e\gamma}z \bmod \pi^{m+1} \\ &\equiv \pi^m(\beta + a^{t-1}s^\gamma dz) \bmod \pi^{m+1}. \end{aligned}$$

Since $\pi \nmid a^{t-1}s^\gamma d$, there exists $z \in R$ such that $\pi \mid (\beta + a^{t-1}s^\gamma dz)$. With this value z, we have $G(a+z\pi^{m-e\gamma}) \equiv 0 \bmod \pi^{m+1}$. This argument gives a construction of a coherent sequence in R_π that converges to a solution of $G = 0$ in R_π. Thus $b \in U^t$ and (1) holds.

Since $R/(\pi^m) \cong R_\pi/\pi^m R_\pi$ by Theorem 4.1.1, we denote both rings by R_m to simplify our notation. Let $R_m^\times$ denote the group of units of R_m and let

$$\theta_m : U \to R_m^\times/(R_m^\times)^t$$

denote the composition of the surjective group homomorphisms

$$U \to R_m^\times \to R_m^\times/(R_m^\times)^t.$$

It follows from (1) that $\ker(\theta_m) = U^t$ for all $m \geq M$.

If $a \in R$, let $\bar{a}$ denote the image of a in $R_m^\times$. Let

$$\tau_m : R_m^\times \to R_m^\times$$

denote the group homomorphism given by $\tau_m(\bar{a}) = \bar{a}^t$. Then $\mathrm{im}(\tau_m) = (R_m^\times)^t$. If $x^t \equiv b \bmod \pi^M$ has a solution in R, then the number of solutions in R_m to $x^t \equiv b \bmod \pi^m$ is given by $\mid \ker(\tau_m) \mid$. Since

$$\mid \ker(\tau_m) \mid \; = \frac{\mid R_m^\times \mid}{\mid \mathrm{im}(\tau_m) \mid} = \; \mid R_m^\times/(R_m^\times)^t \mid \; = |U/U^t|$$

for all $m \geq M$, it follows that (2) holds. $\square$

It is clear that the value $M = 2e\gamma + 1$ in Proposition 5.1.3 is in general not the least integer satisfying (1) and (2). In this direction the result in Theorem 4.3.5, given by $M = \frac{e}{p-1} + \gamma e + 1$ serves as the least value of M for which Proposition 5.1.3 holds. It is interesting to find an analogous result to Proposition 5.1.3 when char $R = p$. If char $R = p$, then $R_\pi = K[[\pi]]$, the ring of formal power series in π.

Let $t \in \mathbb{Z}_{>0}$. For $m \geq 1$, let $h_m^{(t)}$ denote the number of solutions in $R/(\pi^m)$ to the congruence $x^t \equiv 1 \bmod \pi^m$. If $t = rs$ where $\gcd(r, s) = 1$, then $h_m^{(t)} = h_m^{(r)} h_m^{(s)}$. In particular, write $t = p^\gamma d$ where $p \nmid d$ and $\gamma \geq 0$. Then $h_m^{(t)} = h_m^{(p^\gamma)} h_m^{(d)}$.

If $p \nmid t$, then Proposition 5.1.3 and its proof remain valid without any change when char $R = p$. In this case, $t = p^\gamma d$ where $\gamma = 0$ and $d = t$. The proof shows that we may take $M = 1$.

Lemma 5.1.4. *If $m \geq 2$ and $\gamma \geq 0$, then $h_{m+p^\gamma}^{(p^\gamma)} = q^{p^\gamma - 1} h_m^{(p^\gamma)}$. If $m = 1$, then $h_m^{(p^\gamma)} = 1$ for all $\gamma \geq 0$.*

Proof. First assume that $m = 1$. If $a \in R_\pi$, then $a^{p^\gamma} \equiv 1 \bmod \pi$ if and only if $a \equiv 1 \bmod \pi$ because the residue field has characteristic p. Thus $h_m^{(p^\gamma)} = 1$ for all $\gamma \geq 0$.

If $\gamma = 0$, then it is easily checked that $h_m^{(p^\gamma)} = 1$ for all $m \geq 1$. In particular, the statement for $m \geq 2$ holds when $\gamma = 0$ because $q^{p^\gamma - 1} = 1$ in this case.

Now assume that $m \geq 2$ and $\gamma \geq 1$. Let $a \in R_\pi$ and suppose that $a^{p^\gamma} \equiv 1 \bmod \pi^m$. Then

$$a \equiv a_0 + a_1\pi + \cdots + a_{m-1}\pi^{m-1} \bmod \pi^m,$$

where $a_i \in K, 0 \leq i \leq m-1$, and

$$a^{p^\gamma} \equiv a_0^{p^\gamma} + a_1^{p^\gamma}\pi^{p^\gamma} + \cdots + a_{m-1}^{p^\gamma}\pi^{(m-1)p^\gamma} \bmod \pi^m.$$

Choose $k \in \mathbb{Z}$ such that $k - 1 < \dfrac{m}{p^\gamma} \leq k \leq m - 1$. This is possible because $\dfrac{m}{p^\gamma} \leq \dfrac{m}{2} \leq m - 1$ since $m \geq 2$ and $\gamma \geq 1$. Since $(k-1)p^\gamma < m \leq kp^\gamma$, it follows that $a_0 = 1, a_1 = \cdots = a_{k-1} = 0$, and $a_k, \ldots, a_{m-1}$ are arbitrary elements. Therefore $h_m^{(p^\gamma)} = q^{m-k}$.

Similarly, $k < \dfrac{m + p^\gamma}{p^\gamma} \leq k+1$ and $k+1 \leq (m+p^\gamma) - 1$ because $k \leq (m-1) + (p^\gamma - 1)$. Then

$$h_{m+p^\gamma}^{(p^\gamma)} = q^{(m+p^\gamma)-(k+1)} = q^{m-k} q^{p^\gamma - 1} = q^{p^\gamma - 1} h_m^{(p^\gamma)}.$$

□

Corollary 5.1.5. *Assume that* char $R = p$. *Let* $t \in \mathbb{Z}_{>0}$ *and write* $t = p^\gamma d$ *where* $p \nmid d$ *and* $\gamma \geq 0$. *If* $m \geq 2$, *then* $h_{m+p^\gamma}^{(t)} = q^{p^\gamma - 1} h_m^{(t)}$.

Proof. If $m \geq 1$, then $h_{m+p^\gamma}^{(d)} = h_m^{(d)} = [U : U^t]$. Then for $m \geq 2$, we have

$$h_{m+p^\gamma}^{(t)} = h_{m+p^\gamma}^{(p^\gamma)} h_{m+p^\gamma}^{(d)} = q^{p^\gamma - 1} h_m^{(p^\gamma)} h_m^{(d)} = q^{p^\gamma - 1} h_m^{(t)}.$$

□

5.2 Computing c_m

We let $f(x_1, \ldots, x_n) = \epsilon_1 x_1^{t_1} + \cdots + \epsilon_n x_n^{t_n} + b$ where $\epsilon_1, \ldots, \epsilon_n \in R_\pi, t_1, \ldots, t_n$ are positive integers, and $b \in R_\pi$.

Let $l = \mathrm{lcm}(t_1, \ldots, t_n)$, where lcm denotes the least common multiple. Let $l = t_i u_i,\ 1 \leq i \leq n$. We may assume that $t_1 \leq t_2 \leq \cdots \leq t_n$. Then $u_1 \geq u_2 \geq \cdots \geq u_n$. Let $C = u_1 + \cdots + u_n$.

For each $m \geq 1$, let c_m denote the number of solutions to the congruence $f(x_1, \ldots, x_n) \equiv 0 \bmod \pi^m$.

Let $(a_1, \ldots, a_n) \in R_m^{(n)}$ where $(a_1, \ldots, a_n) \not\equiv (0, \ldots, 0) \bmod \pi^m$. We say that $(a_1, \ldots, a_n)$ has *level* j in $R_m^{(n)}$ if j is the largest integer such that $\pi^{j u_i} \mid a_i$ in R_m for each i where $a_i \not\equiv 0 \bmod \pi^m$. We will say that $(0, \ldots, 0)$ has level m in $R_m^{(n)}$. Note that $j = 0$ always satisfies the condition so that $(a_1, \ldots, a_n)$ always has level ≥ 0 and level m in R_m.

Let $D_m^{(j)}$ denote the set of elements $(a_1, \ldots, a_n) \in R_m^{(n)}$ that have level j in $R_m^{(n)}$ and satisfy $f(a_1, \ldots, a_n) \equiv 0 \bmod \pi^m$. Let $d_m^{(j)} = \mid D_m^{(j)} \mid$.

Proposition 5.2.1. *$c_m = d_m^{(0)} + d_m^{(1)} + \cdots + d_m^{(m)}$ for each $m \geq 1$.*

Proof. The equation holds because each solution of $f(x_1, \ldots, x_n) \equiv 0 \bmod \pi^m$ has level j where $0 \leq j \leq m$, and $D_0^{(0)} \cup \cdots \cup D_m^{(m)}$ is a disjoint union. □

For $0 \leq j < m$, we now partition $D_m^{(j)}$ as follows. For $1 \leq k \leq n$ and $0 \leq \lambda < u_k$, let $D_m^{(j,k,\lambda)}$ denote the solutions $(a_1, \ldots, a_n) \in D_m^{(j)}$ satisfying

(1) $\pi^{(j+1)u_i} \mid a_i$ in R_m, where $1 \leq i \leq k-1$ and $a_i \not\equiv 0 \bmod \pi^m$,

(2) $\pi^{ju_k+\lambda} \mid a_k$ in R_m and $\pi^{ju_k+\lambda+1} \nmid a_k$ in R_m where $0 \leq \lambda < u_k$ and $a_k \not\equiv 0 \bmod \pi^m$.

Let $d_m^{(j,k,\lambda)} = \mid D_m^{(j,k,\lambda)} \mid$. This partition of $D_m^{(j)}$ shows that

$$d_m^{(j)} = \sum_{k=1}^{n} \sum_{\lambda=0}^{u_k-1} d_m^{(j,k,\lambda)}.$$

Let $v_\pi(\epsilon_i) = \delta_i,\ 1 \leq i \leq n$, and let M_i be the positive integer from Proposition 5.1.3 that is associated to $t_i,\ 1 \leq i \leq n$. Let $j \in \mathbb{Z}_{\geq 0}$ and let

$$M(j) = \max_{1 \leq i \leq n} \{M_i + \delta_i + jl + t_i(u_i - 1)\}.$$

Proposition 5.2.2. *Let $j \in \mathbb{Z}_{\geq 0}$. Assume that* char $R = 0$. *Then $d_{m+1}^{(j)} = q^{n-1} d_m^{(j)}$ for all $m \geq M(j)$.*

Proof. Note that $0 \leq j < M(j) \leq m$. It is sufficient to show that $d_{m+1}^{(j,k,\lambda)} = q^{n-1} d_m^{(j,k,\lambda)}$ for all $m \geq M(j),\ 1 \leq k \leq n,\ 0 \leq \lambda < u_k$.

Assume that $m \geq M(j)$ and suppose that

$$f(a_1, \ldots, a_n) \equiv 0 \bmod \pi^m$$

where $(a_1, \ldots, a_n) \in D_m^{(j,k,\lambda)}$.

Let $a_k = \pi^{ju_k+\lambda} b_k$, where $b_k \in R_m$ and $\pi \nmid b_k$. We have

$$\epsilon_k (\pi^{ju_k+\lambda} b_k)^{t_k} \equiv -\left(\sum_{i=1}^{k-1} \epsilon_i a_i^{t_i}\right) - \left(\sum_{i=k+1}^{n} \epsilon_i a_i^{t_i}\right) - b \bmod \pi^m.$$

Then

$$b_k^{t_k} \equiv \frac{-(\sum_{i=1}^{k-1} \epsilon_i a_i^{t_i}) - (\sum_{i=k+1}^{n} \epsilon_i a_i^{t_i}) - b}{\epsilon_k \pi^{jl+\lambda t_k}} \bmod \pi^{m-\delta_k-jl-\lambda t_k}.$$

For convenience, let

$$L = \frac{-(\sum_{i=1}^{k-1} \epsilon_i a_i^{t_i}) - (\sum_{i=k+1}^{n} \epsilon_i a_i^{t_i}) - b}{\epsilon_k \pi^{jl+\lambda t_k}}.$$

Since $\pi \nmid b_k$ and $m - \delta_k - jl - \lambda t_k \geq M_k > 0$, it follows that $L \in R_\pi$ and $\pi \nmid L$.

We now count solutions $f(a_1', \ldots, a_n') \equiv 0 \bmod \pi^{m+1}$ where $a_i' \equiv a_i \bmod \pi^m$ for all $1 \leq i \leq n$. Since

$$m \geq M_i + jl + t_i(u_i - 1) \geq M_i + ju_i + (u_i - 1) \geq (j+1)u_i$$

and

$$m > jl + t_k(u_k - 1) \geq ju_k + t_k\lambda \geq ju_k + \lambda,$$

we have $\pi^{(j+1)u_i} \mid a_i'$ in R_{m+1} for $1 \leq i \leq k-1$ and $\pi^{ju_k+\lambda}$ is the exact power dividing a_k' in R_{m+1}. There are q choices for each a_i' in R_{m+1} where $i \neq k$, for a total of q^{n-1} choices. For each choice, let

$$L' = \frac{-(\sum_{i=1}^{k-1} \epsilon_i (a_i')^{t_i}) - (\sum_{i=k+1}^{n} \epsilon_i (a_i')^{t_i}) - b}{\epsilon_k \pi^{jl+\lambda t_k}}.$$

Then $L' \in R_\pi, \pi \nmid L'$, and $L' \equiv L \bmod \pi^{M_i}$.

Let h denote the number of solutions to $x^{t_k} \equiv L \bmod \pi^{M_k}$. Proposition 5.1.3 implies that $x^{t_k} \equiv L' \bmod \pi^m$ has exactly h solutions for all $m \geq M_k$ and for all L' for which there is at least one solution to the congruence.

Given $a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n$ as above, there are h values of a_k as above that satisfy $f(a_1, \ldots, a_n) \equiv 0 \bmod \pi^m$. These h solutions give rise to $q^{n-1}h$ solutions to the congruence $f \equiv 0 \bmod \pi^{m+1}$. This finishes the proof. $\square$

5.3 The case $b \neq 0$

In this section we give an expression for c_m when $b \neq 0$.

Proposition 5.3.1. *Assume that $b \neq 0$ and let $v_\pi(b) = m_0$. Let $m \geq 1$ and suppose that $0 \leq j \leq m$. if $m_0 < m$ and $\dfrac{m_0}{l} < j$, then $d_m^{(j)} = 0$.*

Proof. Suppose that $d_m^{(j)} > 0$ and let $(a_1, \ldots, a_n) \in D_m^{(j)}$. Then

$$\epsilon_1 a_1^{t_1} + \cdots + \epsilon_n a_n^{t_n} + b \equiv 0 \bmod \pi^m.$$

Since $m_0 < jl$, we have either $m_0 < m < jl$ or $m_0 < jl \leq m$.

First assume that $m_0 < m < jl$. Since either $a_i \equiv 0 \bmod \pi$ or $\pi^{ju_i} \mid a_i$ in R_m, it follows that $\sum_{i=0}^{n} \epsilon_i a_i^{t_i} \equiv 0 \bmod \pi^m$ because $m < jl$. Then $b \equiv 0 \bmod \pi^m$, which is impossible because $m_0 < m$. Now assume that $m_0 < jl \leq m$. Then $\sum_{i=0}^{n} \epsilon_i a_i^{t_i} \equiv 0 \bmod \pi^{jl}$. Then $b \equiv 0 \bmod \pi^{jl}$, which is impossible because $m_0 < jl$. Thus $d_m^{(j)} = 0$ as stated. □

Corollary 5.3.2. *Assume that $b \neq 0$ and $v_\pi(b) = m_0$. If $m > m_0$, then*

$$c_m = \sum_{j=0}^{[\frac{m_0}{l}]} d_m^{(j)}.$$

Proof. This follows immediately from Propositions 5.2.1 and 5.3.1 □

5.4 The case $b = 0$

In this section we give an expression for c_m when $b = 0$. Lemma 5.4.1 below contains some simple computations that are needed to ensure that certain expressions make sense in Proposition 5.4.2.

Let $r \in \mathbb{Z}_{\geq 0}$ such that $r < \dfrac{m}{l} \leq r + 1$. Then $r \leq rl < m$ and so it follows that $r + 1 \leq m$.

Lemma 5.4.1. *Assume that $m \geq l$.*

(1) If $t_1 \geq 2$, then $m-(r+1)u_i \geq 0$ for $1 \leq i \leq n$.

(2) Suppose that $t_1 = \cdots = t_{k-1} = 1$ and $2 \leq t_k \leq \cdots \leq t_n$. Then $\max\{m-(r+1)u_i, 0\} = 0$ for $1 \leq i \leq k-1$, and $m-(r+1)u_i \geq 0$ for $k \leq i \leq n$.

Proof. (1) If $r = 0$, then $m \geq l \geq u_i$, so $m-(r+1)u_i \geq 0$. Now assume that $r \geq 1$. Then $u_i = \dfrac{l}{t_i} \leq \dfrac{l}{t_1} \leq \dfrac{l}{2}$. Thus

$$(r+1)u_i \leq (r+1)\frac{l}{2} = \frac{r+1}{2}l \leq rl < m,$$

so $m-(r+1)u_i > 0$.

(2) First assume that $1 \leq i \leq k-1$. Then $u_i = l$ and $m \leq (r+1)l = (r+1)u_i$. Thus $m-(r+1)u_i \leq 0$, so $\max\{m-(r+1)u_i, 0\} = 0$ for $1 \leq i \leq k-1$. The argument in (1) shows that $m-(r+1)u_i \geq 0$ for $k \leq i \leq n$. $\square$

Proposition 5.4.2. *Assume that $b = 0$. If $m \geq l$, then*

$$d_{m+l}^{(r+2)} + d_{m+l}^{(r+3)} + \cdots + d_{m+l}^{(m+l)} = (d_m^{(r+1)} + d_m^{(r+2)} + \cdots + d_m^{(m)})q^{nl-C}.$$

Proof. We first find a formula for $d_m^{(r+1)} + d_m^{(r+2)} + \cdots + d_m^{(m)}$. Let $(a_1, \ldots, a_n) \in R_m^{(n)}$. Then $(a_1, \ldots, a_n) \in D_m^{(r+1)} \cup \cdots \cup D_m^{(m)}$ if and only if $(a_1, \ldots, a_n)$ has level $\geq r+1$ in $R_m^{(n)}$, and this occurs if and only if $\pi^{(r+1)u_i} \mid a_i$ in R_m for each i where $a_i \not\equiv 0 \bmod \pi^m$. If $m-(r+1)u_i > 0$, then the number of possible a_i's equals $q^{m-(r+1)u_i}$. If $m-(r+1)u_i \leq 0$, then the number of possible a_i's equals 1. Namely, $a_i \equiv 0 \bmod \pi^m$ in this latter case. Thus the number of elements $(a_1, \ldots, a_n) \in R_m^{(n)}$ that have level $\geq r+1$ equals $\displaystyle\prod_{i=1}^{n} q^{\max\{m-(r+1)u_i, 0\}}$. We conclude that

$$d_m^{(r+1)} + d_m^{(r+2)} + \cdots + d_m^{(m)} = \prod_{i=1}^{n} q^{\max\{m-(r+1)u_i, 0\}}$$

$$= \prod_{i=k}^{n} q^{m-(r+1)u_i}, \quad \text{by Lemma 5.4.1 because } 2 \leq t_k.$$

Similarly, since $r+1 < \dfrac{m+l}{l} \leq r+2$, we have

$$
\begin{aligned}
&d_{m+l}^{(r+2)} + d_{m+l}^{(r+3)} + \cdots + d_{m+l}^{(m+l)} \\
&\qquad = \prod_{i=1}^{n} q^{\max\{m+l-(r+2)u_i,0\}} = \prod_{i=1}^{n} q^{\max\{m-(r+1)u_i+(l-u_i),0\}} \\
&\qquad = \prod_{i=k}^{n} q^{m-(r+1)u_i+(l-u_i)}, \text{ because } l = u_i \text{ for } 1 \le i \le k-1, \\
&\qquad = \prod_{i=k}^{n} q^{m-(r+1)u_i} \prod_{i=k}^{n} q^{l-u_i} = \prod_{i=k}^{n} q^{m-(r+1)u_i} \prod_{i=1}^{n} q^{l-u_i} \\
&\qquad = (d_m^{(r+1)} + d_m^{(r+2)} + \cdots + d_m^{(m)}) q^{nl-C}.
\end{aligned}
$$

□

Proposition 5.4.3. *Assume that $b = 0$. Assume that $0 \le j < \frac{m}{l}$. Then*

$$d_m^{(j)} = d_{m-jl}^{(0)} \cdot q^{j(nl-C)}.$$

Proof. Since

$$f(\pi^{ju_1} b_1, \ldots, \pi^{ju_n} b_n) = \pi^{jl} f(b_1, \ldots, b_n),$$

we must solve $f(b_1, \ldots, b_n) \equiv 0 \bmod \pi^{m-jl}$, where $(b_1, \ldots, b_n)$ has level 0. There are $d_{m-jl}^{(0)}$ such solutions and each b_i lifts in

$$q^{(m-ju_i)-(m-jl)} = q^{j(l-u_i)}$$

ways. Thus

$$d_m^{(j)} = d_{m-jl}^{(0)} \cdot q^{j(l-u_1)} \cdots q^{j(l-u_n)} = d_{m-jl}^{(0)} \cdot q^{j(nl-C)}.$$

□

Proposition 5.4.4. *Assume that $b = 0$. Then*

$$d_{m+l}^{(0)} + \cdots + d_{m+l}^{(r+1)} = d_{m+l}^{(0)} + (d_m^{(0)} + \cdots + d_m^{(r)}) q^{nl-C}.$$

Proof. Let $0 \le j < \frac{m}{l}$. Then $0 \le j \le r$ and $0 \le j+1 < \frac{m+l}{l}$. Applying Proposition 5.4.3 gives

$$
\begin{aligned}
d_{m+l}^{(j+1)} &= d_{(m+l)-(j+1)l}^{(0)} q^{(j+1)(nl-C)} = d_{m-jl}^{(0)} q^{(j+1)(nl-C)} \\
&= d_{m-jl}^{(0)} q^{j(nl-C)} q^{(nl-C)} = d_m^{(j)} q^{(nl-C)}.
\end{aligned}
$$

It follows that

$$d^{(0)}_{m+l} + \cdots + d^{(r+1)}_{m+l} = d^{(0)}_{m+l} + (d^{(0)}_{m} + \cdots + d^{(r)}_{m})q^{nl-C}.$$

$\square$

We now apply Propositions 5.2.1, 5.4.2, 5.4.4 to obtain the following result.

Proposition 5.4.5. *Assume that $b = 0$ and $m \geq l$. Then $c_{m+l} = d^{(0)}_{m+l} + c_m q^{nl-C}$.*

Proof.

$$\begin{aligned} c_{m+l} &= \sum_{i=0}^{r+1} d^{(i)}_{m+l} + \sum_{i=r+2}^{m+l} d^{(i)}_{m+l} \\ &= d^{(0)}_{m+l} + (d^{(0)}_{m} + \cdots + d^{(r)}_{m})q^{nl-C} + (d^{(r+1)}_{m} + d^{(r+2)}_{m} + \cdots + d^{(m)}_{m})q^{nl-C} \\ &= d^{(0)}_{m+l} + c_m q^{nl-C} \end{aligned}$$

$\square$

We are now in a position to construct the Poincaré series of our diagonal polynomial. We do this in the next section.

5.5 The Poincaré Series

Using results from the previous sections we can now finally compute the Poincaré series of our diagonal polynomial

$$f(x_1, \ldots, x_n) = \epsilon_1 x_1^{t_1} + \cdots + \epsilon_n x_n^{t_n} + b$$

where $\epsilon_1, \ldots, \epsilon_n \in R_\pi$, $t_1, \ldots, t_n$ are positive integers, and $b \in R_\pi$.

For each $m \geq 1$, if c_m denotes the number of solutions to the congruence $f(x_1, \ldots, x_n) \equiv 0 \bmod \pi^m$, then the Poincaré series of f is the formal power series

$$P_f(y) = 1 + \sum_{m=1}^{\infty} c_m y^m.$$

As was the case in the previous sections, we computed c_m separately for $b \neq 0$ and $b = 0$. Similarly here we first present the Poincaré series of f when $b \neq 0$ as out next theorem.

Theorem 5.5.1. *Assume that* char $R = 0, b \neq 0$*, and* $v_\pi(b) = m_0$*. Let*

$$M = \max_{0 \leq j \leq [\frac{m_0}{l}]} \{M(j)\}.$$

Let $m_1 = \max\{M, m_0\}$*. If* $m > m_1$*, then* $c_{m+1} = q^{n-1} c_m$*. In particular,*

$$P_f(y) = 1 + \left(\sum_{i=1}^{m_1} c_i y^i \right) + \frac{c_{m_1+1} y^{m_1+1}}{1 - q^{n-1} y}.$$

Proof. The formula for c_m follows from Proposition 5.2.2 and Corollary 5.3.2. Then

$$\begin{aligned} P_f(y) &= 1 + \sum_{i=1}^{m_1} c_i y^i + \sum_{i=0}^{\infty} c_{m_1+1+i} y^{m_1+1+i} \\ &= 1 + \left(\sum_{i=1}^{m_1} c_i y^i \right) + c_{m_1+1} y^{m_1+1} \sum_{i=0}^{\infty} (q^{n-1} y)^i \\ &= 1 + \left(\sum_{i=1}^{m_1} c_i y^i \right) + \frac{c_{m_1+1} y^{m_1+1}}{1 - q^{n-1} y}. \end{aligned}$$

□

In the next theorem the Poincaré series is constructed for $b = 0$.

Theorem 5.5.2. *Assume that* char $R = 0$*. Then* $P_f(y)$ *is a rational function when* $b = 0$*. In particular, if* $M = \max\{M(0), l\}$ *where* $M(0)$ *is defined just before Proposition 5.2.2, then*

$$P_f(y) = \frac{(1 - q^{n-1} y) \left(\left(\sum_{i=0}^{M+l-1} c_i y^i \right) - q^{nl-C} y^l \left(\sum_{i=0}^{M-1} c_i y^i \right) \right) + q^{l(n-1)} d_M^{(0)} y^{M+l}}{(1 - q^{n-1} y)(1 - q^{(nl-C)} y^l)}$$

Proof. Proposition 5.4.5 gives

$$\begin{aligned} P_f(y) &= \sum_{i=0}^{\infty} c_i y^i = \sum_{i=0}^{M+l-1} c_i y^i + \sum_{i=M+l}^{\infty} c_i y^i = \sum_{i=0}^{M+l-1} c_i y^i + \sum_{i=M}^{\infty} c_{i+l} y^{i+l} \\ &= \sum_{i=0}^{M+l-1} c_i y^i + \sum_{i=M}^{\infty} (d_{i+l}^{(0)} + q^{nl-C} c_i) y^{i+l} \end{aligned}$$

After setting $i = M + j$, Proposition 5.2.2 gives

$$\begin{aligned} \sum_{i=M}^{\infty} d_{i+l}^{(0)} y^{i+l} &= d_{M+l}^{(0)} y^{M+l} \sum_{j=0}^{\infty} (q^{n-1} y)^j = q^{l(n-1)} d_M^{(0)} y^{M+l} \sum_{j=0}^{\infty} (q^{n-1} y)^j \\ &= \frac{q^{l(n-1)} d_M^{(0)} y^{M+l}}{1 - q^{n-1} y}. \end{aligned}$$

Next, we have that

$$\sum_{i=M}^{\infty} q^{nl-C} c_i y^{i+l} = q^{nl-C} y^l \left(P_f(y) - \sum_{i=0}^{M-1} c_i y^i \right).$$

Combining the last three displayed equations gives

$$(1 - q^{nl-C} y^l) P_f(y) = \left(\sum_{i=0}^{M+l-1} c_i y^i \right) - q^{nl-C} y^l_{i=0}{}^{M-1} c_i y^i + \frac{q^{l(n-1)} d_M^{(0)} y^{M+l}}{1 - q^{n-1} y}.$$

Dividing both sides of this equation by $1 - q^{nl-C} y^l$ gives the result. $\square$

Chapter 6 A Different formulation for c_m

In this chapter we present a different formulation of the number of solutions c_m. The final expressions for c_m is different from the previous chapters and relies less on recurrence relations.

6.1 Preliminaries

Definition 6.1.1. *Let R denote a unique factorization domain (UFD) with maximal ideal generated by a prime element π, $f \in R[x_1, \ldots, x_n]$ and let l, m be positive integers, $l \leq m$, and $(x_1, \ldots, x_n), (x'_1, \ldots, x'_n) \in R^{(n)}$. If*

$$f(x_1, \ldots, x_n) \equiv 0 \bmod \pi^m, \;\; f(x'_1, \ldots, x'_n) \equiv 0 \bmod \pi^l$$

$$x_i \equiv x'_i \bmod \pi^l \textit{ for } 1 \leq i \leq n,$$

then we say that $(x_1, \ldots, x_n)$ is a descendant of $(x'_1, \ldots, x'_n)$ with respect to f. We also call $(x'_1, \ldots, x'_n)$ the ancestor of $(x_1, \ldots, x_n)$.

A solution of $f \equiv 0 \bmod \pi^m$ is a descendant of a unique solution of $f \equiv 0 \bmod \pi^l$. The notion of descendant yields a transitive property: if u is v's descendant and v is w's descendant, then u is w's descendant.

Theorem 6.1.2. *Let R be a discrete valuation ring, π a prime element in R which generates the unique maximal ideal, such that $|R/(\pi)| = q < \infty$. If $A \in R^{(n)}$ is a solution of $f \equiv 0 \bmod \pi^m$, then there are exactly λq^{n-1} solutions of $f \equiv 0 \bmod \pi^{m+1}$ which are descendants of A, where*

$$\lambda = \begin{cases} 1, & \textit{if } A \textit{ is nonsingular,} \\ P, & \textit{if } A \textit{ is singular and also a solution of } f \equiv 0 \bmod \pi^{m+1}, \\ 0, & \textit{else} \end{cases}$$

Proof. Assume $A = (a_1, \ldots, a_n)$. Let $B = (b_1, \ldots, b_n)$ be a solution of $f \equiv 0 \bmod \pi^{m+1}$ which is a descendant of A. From the definition of descendant, $b_i = a_i + \eta_i \pi^m$, $\eta_i \in R/(\pi), i = 1, \ldots, n$. So we can decide B as long as we know η_i. If $b_i' = a_i + \eta_i' \pi^m$, then

$$b_i \equiv b_i' \bmod \pi^{m+1} \Leftrightarrow (\eta_i - \eta_i')\pi^m \in (\pi^{m+1}) \Leftrightarrow \eta_i \equiv \eta_i' \bmod \pi.$$

So from the condition of the theorem, η_i has q different values. By Taylor's theorem,

$$0 \equiv f(B) \equiv f(A) + \sum_{i=1}^{n} \frac{\partial f(A)}{\partial x_i} \eta_i \pi^m \bmod \pi^{m+1}.$$

1. Assume $f(A) = c\pi^m, c \in R$. Then the above congruence is equivalent to $\sum_{i=1}^n \frac{\partial f(A)}{\partial x_i} \eta_i \equiv c \bmod \pi$. If A is nonsingular, then $\frac{\partial f(A)}{\partial x_i} \not\equiv 0 \bmod \pi$ for some i. So we can solve for some η_i since $R/(\pi)$ is a field. Therefore the number of B is q^{n-1}.

2. In the case when A is singular, the above congruence becomes $f(A) \equiv 0 \bmod \pi^{m+1}$. So the number of B is q^n if A is a solution of $f \equiv 0 \bmod \pi^{m+1}$ and there is no B otherwise.

$\square$

Corollary 6.1.3. *Let p denote the characteristic of the finite residue field $R/(\pi)$. If $\alpha \in R$ is a solution of $x^n \equiv b \bmod \pi^m$, $\pi \nmid b$ then,*

1. *If $p \nmid n$, then there is exactly one solution of $x^n \equiv b \bmod \pi^{m+1}$ which is a descendant of α.*

2. *If $p \mid n$, then there are exactly q solutions of $x^n \equiv b \bmod \pi^{m+1}$ which are descendants of α if α is also a solution of $x^n \equiv b \bmod \pi^{m+1}$.*

Proof. Consider $f(x) = x^n - b$. If $p \nmid n$, then $\pi \nmid n$. Therefore $\frac{\partial f(\alpha)}{\partial x} = n\alpha^{n-1} \not\equiv 0 \bmod \pi$. Therefore α is nonsingular and the result follows from Theorem 6.1.2.

If $p \mid n$, then $\pi \mid n$. Therefore $\frac{\partial f(\alpha)}{\partial x} = n\alpha^{n-1} \equiv 0 \bmod \pi$. Therefore α is singular and the result follows from Theorem 6.1.2. □

Theorem 6.1.4. *Let $c_m(> 0)$ denote the number of solutions of the congruence $x^n \equiv b \bmod \pi^m$ and let $p = \pi^e s, \pi \nmid s$. If $m \geq e\gamma + \frac{e}{p-1} + 1$ then $c_i = c_m$ for all $i \geq m$.*

Proof. It is not hard to show that if the congruence $x^n \equiv b \bmod \pi^m$ has a solution then it has the same number of solutions as the congruence $x^n \equiv 1 \bmod \pi^m$. Consider the homomorphism $\phi_m : R/\pi^m R^* \to R/\pi^m R^*$ which maps an element a to a^n. Now Im $\phi_m = (R/\pi^m R^*)^n$ and $|\text{Ker } \phi_m|$ is the number of solutions of the congruence $x^n \equiv 1 \bmod \pi^m$. Since ϕ_m is a homomorphism therefore by the second isomorphism theorem $|\text{Ker } \phi_m| = |R/\pi^m R^*/(R/\pi^m R^*)^n|$. By Theorem 4.3.4, $U/U^n \simeq R/\pi^m R^*/(R/\pi^m R^*)^n$ when $m \geq e\gamma + \frac{e}{p-1} + 1$ where U denotes the group of units in R_π. Since U/U^n is constant therefore $|\text{Ker } \phi_m|$ is also a constant and hence the result. □

Theorem 6.1.5. *Suppose c_m is the number of solutions to the congruence $x^n \equiv b \bmod \pi^m$. Let $n = p^\gamma s$. If $p \mid n$ and $m \geq e\gamma + \frac{e}{p-1} + 1$ then $\dfrac{c_m}{q}$ of these solutions lift, and each of them lift in q different ways. On the other hand if $p \nmid n$ then all c_m of these solutions lift, and each of them lift in exactly 1 way.*

Proof. Since $m \geq e\gamma + \frac{e}{p-1} + 1$, therefore by Theorem 6.1.4, c_m is a constant. We prove a small fact here.

Claim 1. *Every solution of $x^n \equiv b \bmod \pi^{m+1}$ is a descendant of a solution of $x^n \equiv b \bmod \pi^m$.*

Proof of claim. Consider C_{m+1} to be the set of solutions of the congruence $x^n \equiv b \bmod \pi^{m+1}$ and let C_m denote the set of solutions of the congruence $x^n \equiv b \bmod \pi^m$. Let $\alpha_{m+1} \in C_{m+1}$. Therefore $\alpha_{m+1} = \beta_m + \delta\pi^m$ after reduction modulo π^m. We have

$$(\beta_m + \delta\pi^m)^n \equiv b \bmod \pi^{m+1}$$

$$\beta_m^n + \beta_m^{n-1} n\delta\pi^m + \pi^{2m}\eta \equiv b \bmod \pi^{m+1}$$

for some $\eta \in R$. If $p \mid n$, then we have

$$\beta_m^n \equiv b \bmod \pi^{m+1}$$

Therefore $\beta_m \in C_{m+1}$ and hence $\beta_m \in C_m$. Therefore α_{m+1} is a descendant of β_m. By Corollary 6.1.3, there are exactly q descendants of β_m.

On the other hand if $p \nmid n$, then every $\beta_m \in C_m$ has exactly one descendant $\alpha_{m+1} \in C_{m+1}$ by Corollary 6.1.3. Since c_m is a constant for $m \geq e\gamma + \frac{e}{p-1} + 1$, and since every descendant comes from a unique solution in C_m, therefore every every solution of $x^n \equiv b \bmod \pi^{m+1}$ is a descendant of a solution of $x^n \equiv b \bmod \pi^m$. □

Now we shift our focus to proving the theorem. Consider the map $\theta_m : C_{m+1} \to C_m$, which maps α_{m+1} to its ancestor α_m. This map is well defined by the previous claim. Also $|C_{m+1}| = |C_m| = c_m$. If $p \mid n$ then by Corollary 6.1.3 since $\alpha_m \in C_{m+1}$, therefore α_m has q descendants. Therefore $|\theta_m^{-1}(\theta_m(\alpha_{m+1}))| = q$. If α_{m+1} runs through all the elements in C_{m+1}, then $\theta_m^{-1}(\theta_m(\alpha_{m+1}))$ will give us a partition of C_{m+1} into disjoint sets, where each set consists of the descendants of α_m. The sets are disjoint since every α_{m+1} has a unique ancestor α_m. Since $\mid \theta_m^{-1}(\theta_m(\alpha_{m+1})) \mid \; = q$ and $\mid C_{m+1} \mid \; = c_m$, therefore the number of such disjoint sets is $\dfrac{c_m}{q}$. Therefore $|\operatorname{Im}\theta_m| = \dfrac{c_m}{q}$ and hence the theorem is proved when $p \mid n$.

On the other hand if $p \nmid n$ then by Corollary 6.1.3, α_m has exactly 1 descendant. Therefore $|\operatorname{Im}\theta_m| = c_m$ and hence every α_m has exactly one descendant α_{m+1}. □

Proposition 6.1.6. *Let $n = p^\gamma s, p \nmid s, \pi \nmid b$. Suppose the congruence $x^n \equiv b \bmod \pi^{e\gamma+\frac{e}{p-1}+1}$ has a solution, then the congruence $x^n \equiv b \bmod \pi^\beta$ has a solution for every $\beta \geq e\gamma + \frac{e}{p-1} + 1$.*

Proof. Since $x^n \equiv b \bmod \pi^{e\gamma+\frac{e}{p-1}+1}$ has a solution, therefore from Theorem 4.3.5, $x^n = b$ has a solution in R_π, hence $x^n \equiv b \bmod \pi^\beta$ has a solution for every $\beta \geq e\gamma + \frac{e}{p-1} + 1$. □

6.2 The Main Theorem

We keep previous notations, but also introduce some new notations here.

- $F(x_1, \ldots, x_n) = \varepsilon_1 x_1^{t_1} + \ldots + \varepsilon_n x_n^{t_n}$.
- C_m = The set of all solutions of $F(x_1, \ldots, x_n) \equiv -b \bmod \pi^m$.
- D_m = The set of all primitive solutions of $F(x_1, \ldots, x_n) \equiv -b \bmod \pi^m$.
- B_m = The set of all non-primitive solutions of $F(x_1, \ldots, x_n) \equiv -b \bmod \pi^m$.
- $c_m = |C_m|, d_m = |D_m|, b_m = |B_m|$.
- $t_i = p^{\gamma_i} s_i, \gamma_i \geq 0, p \nmid s_i$.
- $\varepsilon_i = \pi^{\eta_i} l_i, \eta_i \geq 0, \pi \nmid l_i$.

Also let $M = \max\limits_{1\leq i\leq n}\{\eta_i + e\gamma_i\} + \dfrac{e}{p-1} + 1$.

Theorem 6.2.1. *Assume that $d_M \neq 0$ and let $t = \min\limits_{1\leq i\leq n}\{t_i\}$. If $m \geq M$ then the number of solutions, c_m of*

$$\varepsilon_1 x_1^{t_1} + \ldots + \varepsilon_n x_n^{t_n} \equiv -b \bmod \pi^m \tag{6.1}$$

is given by

$$c_m = \begin{cases} d_M q^{(m-M)(n-1)} + q^{(m-1)n}, & \textit{if } M \le m \le t, v_\pi(-b) \ge m \\ d_M q^{(m-M)(n-1)} + c^{(1)}_{m-t} \cdot q^{(t-1)n}, & \textit{if } m \ge t, v_\pi(-b) > t \\ d_M q^{(m-M)(n-1)}, & \textit{if } m \ge M \ \textit{and } v_\pi(-b) < m \ \textit{or } v_\pi(-b) \le t \end{cases}$$

where $c^{(1)}_{m-t}$ *is the number of solutions of the congruence*

$$\varepsilon_1 \pi^{t_1-t} {x_1}^{t_1} + \ldots + \varepsilon_n \pi^{t_n-t} {x_n}^{t_n} \equiv \frac{-b}{\pi^t} \bmod \pi^{m-t}$$

To prove our main theorem we first find out the number of primitive solutions, d_m of the congruence.

6.3 Finding d_m

Lemma 6.3.1. *Assume* $d_M \neq 0$*. Then* $d_m = d_M q^{(m-M)(n-1)}$ *for* $m \ge M$*.*

Proof. Let's start with a solution $(\alpha_1, \ldots, \alpha_n) \in D_m$. Let j be the smallest number such that $\pi \nmid \alpha_j$. Take a lifting $(\alpha_1 + \delta_1 \pi^m, \ldots, \alpha_n + \delta_n \pi^m)$ of $(\alpha_1, \ldots, \alpha_n), \delta_i \in K$. We want $(\alpha_1 + \delta_1 \pi^m, \ldots, \alpha_n + \delta_n \pi^m) \in D_{m+1}$. Therefore we solve the congruence for δ_i's.

$$\varepsilon_1 (\alpha_1 + \delta_1 \pi^m)^{t_1} + \cdots + \varepsilon_n (\alpha_n + \delta_n \pi^m)^{t_n} \equiv -b \bmod \pi^{m+1}$$

Denote $-b - (\sum_{i=1}^{j-1} \varepsilon_i (\alpha_i + \delta_i \pi^m)^{t_i} + \sum_{i=j+1}^{n} \varepsilon_i (\alpha_i + \delta_i \pi^m)^{t_i})$ by $A(\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n)$. Then

$$\begin{aligned} \varepsilon_j (\alpha_j + \delta_j \pi^m)^{t_j} &\equiv A(\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n) \bmod \pi^{m+1} \\ \pi^{\eta_j} l_j (\alpha_j + \delta_j \pi^m)^{t_j} &\equiv A(\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n) \bmod \pi^{m+1} \\ l_j (\alpha_j + \delta_j \pi^m)^{t_j} &\equiv \pi^{-\eta_j} A(\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n) \bmod \pi^{m-\eta_j+1} \\ (\alpha_j + \delta_j \pi^m)^{t_j} &\equiv {l_j}^{-1} \pi^{-\eta_j} A(\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n) \bmod \pi^{m-\eta_j+1} \end{aligned}$$

Let us choose arbitrary values $\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n \in R$. Therefore we have

$$x^{t_j} \equiv {l_j}^{-1} \pi^{-\eta_j} A(\delta_1, \ldots, \hat{\delta}_j, \ldots, \delta_n) \bmod \pi^{m-\eta_j+1}$$

α_j is a solution of the above congruence mod $\pi^{m-\eta_j}$ and since $\pi \nmid \alpha_j$ therefore $\pi \nmid$ ${l_j}^{-1}\pi^{-\eta_j}A(\delta_1,\ldots,\hat{\delta_j},\ldots,\delta_n)$. Now $m \geq M$ hence $m-\eta_j+1 \geq e\gamma_j + \frac{e}{p-1}+1$, therefore if $p \mid t_j$ then by Theorem 6.1.5, $\dfrac{d_m}{q}$ of these solutions lifts to a solution mod $\pi^{m-\eta_j+1}$. These give rise to solutions of congruence (6.1). Each of these solutions lift in q different ways. There are q^{n-1} different choices of ${l_j}^{-1}\pi^{-\eta_j}A(\delta_1,\ldots,\hat{\delta_j},\ldots,\delta_n)$.

Therefore the number of different solutions to the above equation with different ${l_j}^{-1}\pi^{-\eta_j}A(\delta_1,\ldots,\hat{\delta_j},\ldots,\delta_n)$'s is given by

$$d_{m+1} = \frac{d_m}{q}\cdot q\cdot q^{n-1} = d_m q^{n-1} \text{ for } m \geq M.$$

Solving the simple recurrence relation we have $d_m = d_M q^{(m-M)(n-1)}$ for $m \geq M$.

On the other hand if $p \nmid t_j$ then by Theorem 6.1.5, all d_m of these solutions lifts to a solution mod $\pi^{m-\eta_j+1}$. Each of them lifting in exactly one way. There are q^{n-1} different choices of ${l_j}^{-1}\pi^{-\eta_j}A(\delta_1,\ldots,\hat{\delta_j},\ldots,\delta_n)$.

Therefore the number of different solutions to the above equation with different ${l_j}^{-1}\pi^{-\eta_j}A(\delta_1,\ldots,\hat{\delta_j},\ldots,\delta_n)$'s is given by

$$d_{m+1} = d_m\cdot 1\cdot q^{n-1} = d_m q^{n-1} \text{ for } m \geq M.$$

Solving the simple recurrence relation we have $d_m = d_M q^{(m-M)(n-1)}$ for $m \geq M$.

Therefore

$$d_m = d_M q^{(m-M)(n-1)} \qquad \text{for } m \geq M.$$

$\square$

In the next section we find the number of non-primitive solutions, b_m of our congruence.

6.4 Finding b_m

Lemma 6.4.1. *Let* $t = \min_{1\le i\le n}\{t_i\}$. *If* $1 \le m \le t$ *then*

$$b_m = \begin{cases} (q^{m-1})^n, & \text{if } 1 \le m \le t \text{ and } v_\pi(-b) \ge m. \\ 0, & \text{if } 1 \le m \le t \text{ and } v_\pi(-b) < m. \end{cases}$$

Proof. Let's consider arbitrary $\alpha_1, \ldots, \alpha_n$ such that $\pi \mid \alpha_i, 1 \le i \le n$.

Claim 2. $(\alpha_1, \ldots, \alpha_n) \in B_m$ *iff* $v_\pi(-b) \ge m$.

Proof of Claim. Let $\alpha_i = \pi\gamma_i$. Therefore

$$F(\alpha_1, \ldots, \alpha_n) = \pi^t G(\gamma_1, \ldots, \gamma_n)$$

where $G(x_1, \ldots, x_n) = \varepsilon_1 \pi^{t_1 - t} {x_1}^{t_1} + \ldots + \varepsilon_n \pi^{t_n - t} {x_n}^{t_n}$. If $(\alpha_1, \ldots, \alpha_n) \in B_m$ then $\pi^t G(\gamma_1, \ldots, \gamma_n) \equiv -b \pmod{\pi^m}$ is solvable. But since $m \le t$ therefore $-b \equiv 0 \pmod{\pi^m}$ which implies $v_\pi(-b) \ge m$. On the other hand if $v_\pi(-b) \ge m$ then $\pi^m \mid -b$. Also since $m \le t$ therefore $\pi^m \mid F(\alpha_1, \ldots, \alpha_n)$. Therefore

$$F(\alpha_1, \ldots, \alpha_n) \equiv 0 \pmod{\pi^m}$$

□

Now if $v_\pi(-b) < m$, then since $m \le t$ therefore $\pi^m \mid F(\alpha_1, \ldots, \alpha_n)$, which implies $0 \equiv -b \bmod \pi^m$ but this contradicts the assumption that $v_\pi(-b) < m$. Therefore $b_m = 0$ if $v_\pi(-b) < m$. Each α_i has q^{m-1} choices , $1 \le i \le n$. Therefore the number of different choices for $(\alpha_1, \ldots, \alpha_n)$ is $(q^{m-1})^n$. Hence the result. □

Lemma 6.4.2. *Let* $t = \min_{1\le i\le n}\{t_i\}$. *If* $m \ge t$ *then*

$$b_m = \begin{cases} c^{(1)}_{m-t} \cdot q^{(t-1)n}, & \text{if } m \ge t, v_\pi(-b) \ge t \\ 0, & \text{if } m \ge t, v_\pi(-b) < t \end{cases}$$

Proof. Suppose $F(\alpha_1,\ldots,\alpha_n) \equiv -b \bmod \pi^m$. If $v_\pi(-b) < t$, then $m > v_\pi(-b)$, therefore $v_\pi(F(\alpha_1,\ldots,\alpha_n)+b) < m$. Hence $b_m = 0$ if $v_\pi(-b) < t$, therefore we consider $v_\pi(-b) \geq t$. Let $b' = \dfrac{-b}{\pi^t}$. Consider the congruence

$$G(x_1,\ldots,x_n) \equiv b' \bmod \pi^{m-t}$$

Let us denote the set of solutions of the above congruence by $C^{(1)}_{m-t}$. Let $(\sigma_1,\ldots,\sigma_n) \in C^{(1)}_{m-t}$. From $(\sigma_1,\ldots,\sigma_n)$ we want to construct a solution $(\alpha_1,\ldots,\alpha_n)$ such that $(\alpha_1,\ldots,\alpha_n) \in B_m$.

Claim 3. $B_m = \{(\alpha_1,\ldots,\alpha_n) \mid \alpha_i = \pi(\sigma_i + h_i\pi^{m-t}), 1 \leq i \leq n\}$ *for arbitrary* h_i*'s.*

Proof of Claim. $(\alpha_1,\ldots,\alpha_n) \in B_m$ since

$$\begin{aligned} F(\alpha_1,\ldots,\alpha_n) &= F(\pi(\sigma_1 + h_1\pi^{m-t}),\ldots,\pi(\sigma_n + h_n\pi^{m-t})) \\ &= \pi^t G(\sigma_1 + h_1\pi^{m-t},\ldots,\sigma_n + h_n\pi^{m-t}) \end{aligned}$$

Its easy to see that

$$G(\sigma_1 + h_1\pi^{m-t},\ldots,\sigma_n + h_n\pi^{m-t}) \equiv G(\sigma_1,\ldots,\sigma_n) \bmod \pi^{m-t}$$

Now $G(\sigma_1,\ldots,\sigma_n) \equiv b' \bmod \pi^{m-t}$. Therefore

$$\begin{aligned} G(\sigma_1 + h_1\pi^{m-t},\ldots,\sigma_n + h_n\pi^{m-t}) &\equiv \frac{-b}{\pi^t} \bmod \pi^{m-t} \\ \pi^t G(\sigma_1 + h_1\pi^{m-t},\ldots,\sigma_n + h_n\pi^{m-t}) &\equiv -b \bmod \pi^m \\ F(\alpha_1,\ldots,\alpha_n) &\equiv -b \bmod \pi^m \end{aligned}$$

This implies $(\alpha_1,\ldots,\alpha_n) \in B_m$. On the other hand given $(\alpha_1,\ldots,\alpha_n) \in B_m$, let $\alpha_i = \pi\sigma_i$. Substituting it in $F(x_1,\ldots,x_n)$ we get

$$\begin{aligned} F(\alpha_1,\ldots,\alpha_n) = \pi^t G(\sigma_1,\ldots,\sigma_n) &\equiv -b \bmod \pi^m \\ G(\sigma_1,\ldots,\sigma_n) &\equiv \frac{-b}{\pi^t} \bmod \pi^{m-t} \\ G(\sigma_1,\ldots,\sigma_n) &\equiv b' \bmod \pi^{m-t} \end{aligned}$$

This implies $(\sigma_1, \ldots, \sigma_n) \in C^{(1)}_{m-t}$ and any solution $(\alpha_1, \ldots, \alpha_n)$ is of the above form by taking $h_i = 0$. $\square$

Now $\alpha_i = \pi\sigma_i + h_i\pi^{m-t+1}$. Since the h_i's were chosen arbitrarily, there are P^{t-1} choices of h_i's for each α_i. Therefore there are $q^{(t-1)n}$ choices for $(\alpha_1, \ldots, \alpha_n)$. But we started with a solution $(\sigma_1, \ldots, \sigma_n) \in C^{(1)}_{m-t}$ and constructed a solution $(\alpha_1, \ldots, \alpha_n) \in B_m$. Therefore it's easy to see that $b_m = c^{(1)}_{m-t} \cdot q^{(t-1)n}$ for $v_\pi(-b) \geq t$. Hence the result. $\square$

Therefore combining results in Lemmas 6.4.1 and 6.4.2 we have the following result.

Lemma 6.4.3. *Let* $t = \min\limits_{1 \leq i \leq n}\{t_i\}$. *Then*

$$b_m = \begin{cases} (q^{m-1})^n, & \text{if } 1 \leq m \leq t,\ v_\pi(-b) \geq m \\ c^{(1)}_{m-t} \cdot q^{(t-1)n}, & \text{if } m \geq t, v_\pi(-b) \geq t \\ 0, & \text{if } m \geq t, v_\pi(-b) < t \text{ or } 1 \leq m \leq t, v_\pi(-b) < m \end{cases}$$

Now since $c_m = d_m + b_m$ therefore number of solutions c_m is given by

$$c_m = \begin{cases} d_M q^{(m-M)(n-1)} + q^{(m-1)n}, & M < m \leq t, v_\pi(-b) \geq m \\ d_M q^{(m-M)(n-1)} + c^{(1)}_{m-t} \cdot q^{(t-1)n}, & m \geq t, v_\pi(-b) \geq t \\ d_M q^{(m-M)(n-1)}, & \text{if } m \geq M \text{ and } v_\pi(-b) < m \text{ or } v_\pi(-b) < t \end{cases}$$

where $M = \max\limits_{1 \leq i \leq n}\{\eta_i + e\gamma_i\} + \dfrac{e}{p-1} + 1$ and $c^{(1)}_{m-t}$ is the number of solutions of the congruence

$$\varepsilon_1 \pi^{t_1 - t} {x_1}^{t_1} + \ldots + \varepsilon_n \pi^{t_n - t} {x_n}^{t_n} \equiv \frac{-b}{\pi^t} \bmod \pi^{m-t}$$

Chapter 7 A Simple Example

In this chapter we present a simple example which illustrates the results of the previous two chapters. We keep all the notations from the previous chapters. We start off with a very simple proposition.

7.1 Verifying previous results related to c_m

Proposition 7.1.1. *Let $f(x_1, \ldots, x_n) = \epsilon_1 x_1 + g(x_2, \ldots, x_n)$ where ϵ_1 is a unit and $g(x_2, \ldots, x_n)$ is a polynomial of $n-1$ variables. Let c_m denote the number of solutions of the congruence $f(x_1, \ldots, x_n) \equiv 0 \bmod \pi^m$ and b_m the number of non-primitive solutions of the same congruence. If $|R/(\pi)| = q$, then $c_m = q^{m(n-1)}$, $b_m = q^{(m-1)(n-1)}$.*

Proof. We fix x_1, then there are q^m choices for each $x_2, \ldots, x_n$. Since ϵ_1 is a unit therefore the congruence always has a solution and therefore $c_m = (q^m)^{n-1} = q^{m(n-1)}$. Now to find the number of non primitive solution every x_i's has to be divisible by π. Therefore there are q^{m-1} choices for each $x_2, \ldots, x_n$. Therefore $b_m = (q^{m-1})^{n-1} = q^{(m-1)(n-1)}$. $\square$

In this chapter we fix $g(x_2, \ldots, x_n) = \epsilon_2 x_2 + \cdots + \epsilon_n x_n + b$. Therefore

$$f(x_1, \ldots, x_n) = \epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_n x_n + b.$$

Here ϵ_1 is a unit, $\epsilon_2, \ldots, \epsilon_n \in R_\pi$ and $b \in R_\pi$. Now using the same notations from Section 5.2, we see that $l = \mathrm{lcm}(1, \ldots, 1) = 1$, $u_i = 1$, $1 \le i \le n$. Therefore $C = u_1 + \ldots + u_n = n$.

Since $c_m = d_m + b_m$, where d_m is the number of primitive solutions, therefore by Proposition 7.1.1, $d_m = q^{m(n-1)} - q^{(m-1)(n-1)}$.

Applying Theorem 6.2.1, we have $t = \min_{1 \le i \le n}\{t_i\} = 1$. Since $m \ge 1$, therefore if $b \neq 0, v_\pi(-b) < 1$, then

$$\begin{aligned} d_M q^{(m-M)(n-1)} &= (q^{M(n-1)} - q^{(M-1)(n-1)})q^{(m-M)(n-1)} \\ &= q^{m(n-1)} - q^{(m-1)(n-1)} \\ &= d_m \end{aligned}$$

By Lemma 6.4.2, $b_m = 0$ when $v_\pi(-b) < 1$. Therefore $c_m = d_m$ and hence the result of Theorem 6.2.1 is verified.

If $b \neq 0, v_\pi(-b) \ge 1$, then by Theorem 6.2.1 we have

$$\begin{aligned} d_M q^{(m-M)(n-1)} + c_{m-1}^{(1)} &= (q^{M(n-1)} - q^{(M-1)(n-1)})q^{(m-M)(n-1)} + c_{m-1}^{(1)} \\ &= q^{m(n-1)} - q^{(m-1)(n-1)} + c_{m-1}^{(1)} \end{aligned}$$

where $c_{m-1}^{(1)}$ is the number of solutions of the congruence

$$\epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_n x_n \equiv \frac{-b}{\pi} \bmod \pi^{m-1}$$

Applying Proposition 7.1.1 with $g(x_2, \ldots, x_n) = \epsilon_2 x_2 + \cdots + \epsilon_n x_n + \dfrac{b}{\pi}$, we see that $c_{m-1}^{(1)} = c_{m-1} = q^{(m-1)(n-1)}$.

Therefore

$$d_M q^{(m-M)(n-1)} + c_{m-1}^{(1)} = q^{m(n-1)} - q^{(m-1)(n-1)} + q^{(m-1)(n-1)} = q^{m(n-1)} = c_m.$$

which verifies Theorem 6.2.1.

Now when $b \neq 0$, then the result of Theorem 5.5.1 from Chapter 4, $c_{m+1} = q^{n-1}c_m$ is easily verified to be true when $c_m = q^{m(n-1)}$.

Now we verify the same results when $b = 0$. In this case $v_\pi(-b) = \infty$. Therefore $v_\pi(-b) \ge 1$ and by Theorem 6.2.1 we have

$$\begin{aligned} d_M q^{(m-M)(n-1)} + c_{m-1}^{(1)} &= (q^{M(n-1)} - q^{(M-1)(n-1)})q^{(m-M)(n-1)} + c_{m-1}^{(1)} \\ &= q^{m(n-1)} - q^{(m-1)(n-1)} + c_{m-1}^{(1)} \end{aligned}$$

Applying Proposition 7.1.1 with $g(x_2, \ldots, x_n) = \epsilon_2 x_2 + \cdots + \epsilon_n x_n$, we see that $c_{m-1}^{(1)} = c_{m-1} = q^{(m-1)(n-1)}$.

Therefore

$$d_M q^{(m-M)(n-1)} + c_{m-1}^{(1)} = q^{m(n-1)} - q^{(m-1)(n-1)} + q^{(m-1)(n-1)} = q^{m(n-1)} = c_m.$$

which verifies Theorem 6.2.1.

Now we verify the result from Chapter 4 when $b = 0$. By Proposition 5.4.5

$$\begin{aligned} d_{m+l}^{(0)} + c_m q^{nl-C} &= d_{m+1}^{(0)} + c_m q^{n-n} \\ &= d_{m+1}^{(0)} + q^{m(n-1)} \end{aligned}$$

If $j = 0$, then by the definition of $M(j)$ just before Proposition 5.2.2, we have $M(0) = \max_{1 \le i \le n} \{M_i + \delta_i + t_i(u_i - 1)\}$. By Proposition 5.2.2, we have $d_{m+1}^{(j)} = q^{n-1} d_m^{(j)}$ for all $m \ge M(j)$. Therefore $d_{m+1}^{(0)} = d_m^{(0)} q^{n-1}$. By looking at the definition of $d_m^{(0)}$ in Section 5.2, it can be easily seen that $d_m^{(0)} = d_m$, the number of primitive solutions.

But $d_m = q^{m(n-1)} - q^{(m-1)(n-1)}$. Hence

$$\begin{aligned} d_{m+l}^{(0)} + c_m q^{nl-C} &= d_{m+1}^{(0)} + q^{m(n-1)} \\ &= d_m^{(0)} q^{n-1} + q^{m(n-1)} \\ &= (q^{m(n-1)} - q^{(m-1)(n-1)}) q^{n-1} + q^{m(n-1)} \\ &= q^{(m+1)(n-1)} - q^{m(n-1)} + q^{m(n-1)} \\ &= q^{(m+1)(n-1)} \\ &= c_{m+1} \end{aligned}$$

Therefore $c_{m+1} = d_{m+1}^{(0)} + q^{m(n-1)}$ and hence the result from Proposition 5.4.5 is verified. At last we compute the Poincaré series and compare it with our results from previous chapters.

7.2 Verifying the Poincaré series

The Poincaré series, $P_f(y)$ is the formal power series $1+\sum_{i=1}^{\infty} c_i y^i$. Therefore

$$\begin{aligned} P_f(y) &= 1+\sum_{i=1}^{\infty} q^{i(n-1)} y^i \\ &= \frac{1}{1-q^{n-1}y} \end{aligned}$$

Now if $b \neq 0$, by Proposition 5.5.1 we have

$$\begin{aligned} P_f(y) &= 1+\left(\sum_{i=1}^{m_1} c_i y^i\right)+\frac{c_{m_1+1} y^{m_1+1}}{1-q^{n-1}y} \\ &= 1+\left(\sum_{i=1}^{m_1} q^{i(n-1)} y^i\right)+\frac{q^{(m_1+1)(n-1)} y^{m_1+1}}{1-q^{n-1}y} \\ &= \frac{1-(q^{n-1}y)^{m_1+1}}{1-q^{n-1}y}+\frac{q^{(m_1+1)(n-1)} y^{m_1+1}}{1-q^{n-1}y} \\ &= \frac{1}{1-q^{n-1}y} \end{aligned}$$

Now if $b=0$ then by Proposition 5.5.2 we have

$$P_f(y) = \frac{(1-q^{n-1}y)\left(\left(\sum_{i=0}^{M+l-1} c_i y^i\right)-q^{nl-C} y^l\left(\sum_{i=0}^{M-1} c_i y^i\right)\right)+q^{l(n-1)} d_M^{(0)} y^{M+l}}{(1-q^{n-1}y)(1-q^{(nl-C)} y^l)}$$

Due to our choice of the polynomial g, we have $l = 1, C = n$ and $d_M^{(0)} = q^{M(n-1)} - q^{(M-1)(n-1)}$. Therefore

$$\begin{aligned}
P_f(y) &= \frac{(1-q^{n-1}y)\left(\left(\sum_{i=0}^{M} q^{i(n-1)}y^i\right) - y\left(\sum_{i=0}^{M-1} q^{i(n-1)}y^i\right)\right) + q^{n-1}d_M^{(0)}y^{M+l}}{(1-q^{n-1}y)(1-y)} \\
&= \frac{(1-q^{n-1}y)\left(\left(\frac{1-(q^{n-1}y)^{M+1}}{1-q^{n-1}y}\right) - y\left(\frac{1-(q^{n-1}y)^{M}}{1-q^{n-1}y}y^i\right)\right) + q^{n-1}d_M^{(0)}y^{M+l}}{(1-q^{n-1}y)(1-y)} \\
&= \frac{1-q^{(n-1)(M+1)}y^{M+1} - y + q^{(n-1)M}y^{M+1} + q^{n-1}(q^{M(n-1)} - q^{(M-1)(n-1)})y^{M+1}}{(1-q^{n-1}y)(1-y)} \\
&= \frac{1-y}{(1-q^{n-1}y)(1-y)} \\
&= \frac{1}{1-q^{n-1}y}
\end{aligned}$$

Both of these expressions match with our findings at the beginning of the section and hence the Poincaré series is verified.

7.3 Future Directions

Even though the work in this dissertation gives a complete picture of the Poincaré series for a diagonal polynomial, there are still several unanswered questions which could be tackled in the future. We next outline some of them.

- *Geometric Properties* - In our work we explicitly computed the Poincaré Series for a general diagonal polynomial by finding the number of solutions to congruences modulo powers of a prime. An interesting question to look at is whether the expression for the Poincaré series gives us any insight into the variety defined by our general diagonal polynomial. Can something be said about the geometric properties of the variety.

- *Char $R = p$* - The proof of Denef and Igusa assume that char $R = 0$. It is an interesting question to ask whether the Poincaré series is rational when char $R = p$, for a prime p. In this direction our method still holds when f is a diagonal polynomial with the coefficients $\epsilon_1, \ldots, \epsilon_n$ and b being arbitrary and the exponents $t_1, \ldots, t_n$ being relatively prime to p. Is the same true when all the parameters are arbitrary?

- *Extending results of Goldman* - Another problem of interest to me would be extending results of Goldman that I stated in Theorem 2.1.3. In his theorem Goldman restricts to strongly non-degenerate forms. Now suppose that for some fixed k we have $F(\alpha_1, \ldots, \alpha_n) \equiv 0 \bmod \pi^{2k+1}$, such that there exists at least one i for which $\frac{\partial F}{\partial x_i}(\alpha_1, \ldots, \alpha_n) \not\equiv 0 \bmod \pi^{k+1}$ for every solution $(\alpha_1, \ldots, \alpha_n)$ of F. It would be interesting to find c_m for $m \geq 2k + 1$ in this case. This would extend Goldman's result, which is the special case when $k = 0$.

- *Other types of polynomials* - In this dissertation we looked at diagonal polynomials and computed their Poincaré series explicitly. Can we do this for any other types of polynomials and give explicit computations for their Poincaré series?

Bibliography

[Art67] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.

[BS66] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[Den84] J. Denef, *The rationality of the Poincaré Series associated to the p-adic points on a variety*, Invent. math. **77** (1984), 1–23.

[FV02] I.B. Fesenko and S.V. Vostokov, *Local Fields and Their Extensions*, Amer. Math. Soc., 2002.

[Gol83] J. R. Goldman, *Number of solutions of congruences: Poincaré Series for strongly nondegenerate forms*, Proc. Amer. Math. Soc. **87** (1983), 586–590.

[Gol86] ______, *Number of solutions of congruence: Poincaré Series for algebraic curves*, Adv. in Math. **62** (1986), 68–83.

[Han99] Q. Han, *Numbers of Solutions of Congruences and Rationality of Generating Functions*, Finite Fields and Their Applications **5** (1999), 266–284.

[Has80] H. Hasse, *Number Theory*, Springer Verlag, Grund. math. Wiss., 1980.

[Igu77] J. Igusa, *Some observations on higher degree characters*, Amer. J. Math. **99** (1977), 393–417.

[Igu79] ______, *Complex Powers and asymptotic expansions II*, J. Reine Angew. Math. **278/279** (1979), 307–321.

[Lan70] S. Lang, *Algebraic Number Theory*, Springer Verlag, 1970.

[Meu81] D. Meuser, *On the rationality of certain generating functions*, Math. Ann. **256** (1981), 303–310.

[Wan92] J. Wang, *On the Poincaré Series of Diagonal Forms*, Proc. Amer. Math. Soc. **116** (1992), 607–611.

[Wan93] ———, *On the Poincaré Series of Diagonal Forms over Algebraic Number Fields*, Acta Arithmetica **63** (1993), 97–101.

[Wei74] A. Weil, *Basic Number Theory*, 3rd ed., Springer Verlag, Grund. math. Wiss., 1974.

Vita

- Personal Information:
  - Born 27th August 1983 in Agartala, India.
- Education:
  - 2010(Expected), Ph.D., University of Kentucky.
  - 2006, M.A., University of Kentucky.
  - 2004, B.S., Chennai Mathematical Institute, India.
- Scholastic and Professional Honors:
  - 2009, Summer Research Fellowship.
  - 2008, Edgar Enochs scholarship for outstanding student in algebra.
- Publications:
  - *The Poincaré series of a diagonal polynomial*, with David Leep, preprint.
  - *Powers of elements in complete discrete valuation rings*, with David Leep, preprint.