HOMOGENEOUS INTEGER-VALUED POLYNOMIALS OF THREE VARIABLES

by

Marie-Andrée B.Langlois

Submitted in partial fulfillment of the requirements
for the degree of PhD. in Mathematics

at

Dalhousie University
Halifax, Nova Scotia
June 2018

“No, a proof is a proof. What kind of a proof? It’s a proof. A proof is a proof, and when you have a good proof, it’s because it’s proven.”

Jean Chrétien

Table of Contents

List of Tables

List of Figures

Abstract

A polynomial f in $\mathbb{Q}[x, y, z]$ is integer-valued if $f(x, y, z) \in \mathbb{Z}$, whenever x, y, z are integers. This work will look at the case where f is homogeneous and construct polynomials such that the denominators are divisible by the highest prime power possible and find bases for the modules of homogeneous integer-valued polynomials (IVPs). We will present computational methods for constructing such bases and an algebraic method to construct these. We explain the connection between 3-variable homogeneous IVPs of degree m and 3-variable IVPs of degree m, as well as with 2-variable IVPs of degree m evaluated at odd values only, then use linear algebra to calculate bases in both cases. In order to obtain polynomials written as a product of linear factors, we will look into extending the construction of finite projective planes to rings and explain a connection between line coverings of those planes and homogeneous IVPs.

List of Abbreviations and Symbols Used

IVP	Integer-valued polynomial	viii
$\mathrm{Int}(E, D)$	Ring of integer-valued polynomials on the subset E	1
$\alpha_{E,p}(n)$	Characteristic sequence of E	6
$\nu_p(n)$	p-adic valuation	6
$d(\mathbb{Z}, f)$	Fixed divisor of f	8
$k!_S$	Generalized factorial on the subset S	9
$\mathfrak{I}_n(\mathbb{B})$	ICharacteristic ideal of $\mathbb{B}$	12
$\mathrm{Int}_m(S, \mathbb{Z})$	Integer-valued polynomials of degree less than or equal to m	26
$\mathrm{Int}^m(S, \mathbb{Z})$	Homogeneous integer-valued polynomials degree m	26
$\left\lfloor \frac{n}{k} \right\rfloor$	Floor function	28
D_n	n-th diagonal of M	31
$T_{(a_1,b_1,a_2,b_2)}$	Triangular region in M	33
$\gamma(n)$	Number of times n is in M	35
$A \approx B$	Equivalent matrices	42
$\mathbb{Z}^m[x, y, z]$	Homogeneous polynomials of degree m with integer coefficients	47
$S(i, j)$	Stirling number of the second kind	47
$\mathcal{L}(B)$	Lattice generated by the matrix B	62
Λ^*	Dual of a lattice	63
HNF	Hermite normal form	63
$[B\|B']$	Adjoining the matrices B and B'	64
f_{sym}	Symmetrization of f	75

$\mathbb{F}_q\mathbf{P}^n$	Finite projective n space	78
$L_{(a,b,c)}$	Set of points incident to the line (a, b, c)	79
$\mathbb{Z}/(p^k)\mathbf{P}^2$	Projective H-plane over $\mathbb{Z}/(p^k)$	81

Acknowledgements

I would like to express my profound gratitude for my supervisor Prof. Keith Johnson, for his knowledge, guidance and patience. Also, for caring about my work and pushing my limits to attain my goals. There is simply no way I could have had better support.

I would like to thank my thesis committee Prof. Karl Dilcher and Dr. Rob Noble whose insightful comments and questions helped me get the best possible version of this manuscript. I would like to thank Prof. David Welhau who travelled to Halifax in order to make my thesis richer and for motivating further research in this area. I would also like to thank Prof. Peter Selinger, who ended up giving me advice that went beyond teaching and enlightened me about so many beautiful applications of mathematics.

I would like to thank everyone in the Chase building, my four years spent in the department were amazing from mathematical and personal perspectives. I have laughed a lot and made many friends, by trying to list them all I would forget someone for sure. I do want to mention Ben Cameron for his incredible patience and wisdom and Kira Scheibelhut who took the time to read this thesis and improved its quality.

Je tiens particulièrement à remercier ma famille qui, malgré la distance, m'a encouragé dans mon parcours atypique. I would like to thank my friends, especially Gen, Katherine, Marie-Claude and Sam for keeping me motivated and sane throughout this degree. Finally, I would like to thank Jayce for his support and believing in my dreams.

Chapter 1

Introduction

Rings of the form $\mathrm{Int}(S, D)$ *"have many remarkable properties, and are a source of examples and counterexamples in commutative algebra".* W. Narkiewicz

The results we describe below have been obtained over different rings, but they can be adapted to $\mathbb{Z}$, $\mathbb{F}_p$ and $\mathbb{Z}_{(p)}$, the rings of interest in this work, as we will explain for the appropriate cases.

This work is about IVPs on a set $S \subseteq \mathbb{Z}^n$. These are polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ that return an integer when evaluated at any value in S. The set of IVPs on S forms a ring and a $\mathbb{Z}$-module denoted by

$$\mathrm{Int}(S, \mathbb{Z}) = \{f \in \mathbb{Q}[x_1, \ldots, x_n] \mid f(S) \subseteq \mathbb{Z}\}.$$

Since we are considering $\mathbb{Z}$-modules, we are interested in finding bases for $\mathrm{Int}(S, \mathbb{Z})$.

For example, when $n = 1$ and $S = \mathbb{Z}$, we have that $f(x) = \frac{x(x-1)}{2}$ is integer-valued, since for any two consecutive integers there is always an even one. Generalizing this gives the set of polynomials

$$\left\{\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}\right\}_{n\geq 0}$$

which is, in fact, a $\mathbb{Z}$-basis for $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$. This basis contains one polynomial of each degree, and so it is what will be referred to as a regular basis.

This work will focus mainly on homogeneous IVPs, which, for a given degree m, are polynomials of the form

$$f(x_1, \dots, x_n) = \sum_{i_1+i_2+\cdots+i_n=m} c_{i_1,i_2,\dots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

where the coefficients $c_{i_1,i_2,\dots,i_n}$ are rational numbers and f satisfies the integrality condition described above. Note that the polynomial where all coefficients are zero, will be included in all modules we work with.

In addition to the nice number theoretical results one may obtain, further motivation to study IVPs in general and the homogeneous case in particular is their connection to algebraic topology, which will be explained in Chapter 3. Integer-valued polynomials tend to appear in homotopy theory, as described in [Joh14] and summarized in the next chapter.

The connection between IVPs and topology has been studied for much longer. One of the first instances is from 1971 when Adams, Harris and Switzer [AHS71] explained some of the K-theory of BU through IVPs. Building on these results, Clarke showed that the complex K-theory homology of the infinite complex projective space, $K_0(\mathbb{C}P^\infty)$, is isomorphic to $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$, and this can be extended to $K_0(BT^n) \simeq \mathrm{Int}(\mathbb{Z}^n, \mathbb{Z})$. The connection to homogeneous polynomials was made by Baker, Clarke, Ray and Schwartz [BCRS89] who identified the primitive elements of $K_0(BU(n))$ as the symmetric homogeneous IVPs in n-variables.

The goal of this work is to identify homogeneous IVPs, focusing on the 3-variable case. We start by localizing at a prime. Usually $p = 2$ since it will allow us to divide by higher powers of p within computational limits, but our methods extend to odd primes. When constructing these polynomials, we are interested in how big a denominator we can get, i.e., we are looking for basis elements of the form $f_i = \frac{q_i}{p^{e_i}}$ with $q_i \in \mathbb{Z}_{(p)}[x]$. We are concerned with finding maximal e_i such that f_i is an IVP.

The 2-variable case was described by Johnson and Patterson's work [JP11], hence our results will build on this work. Note that, given the topological correspondence, the 3-variable case will not behave like the previous one, so we need to develop new tools, but we will often refer to the 2-variable case to test our methods.

Our work is done over $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$, but many of the results in the next chapter are given in much greater generality. We have explored two different strategies to obtain homogeneous 3-variable IVPs. The first is through computational methods and the second is by direct construction.

For the computational part, we used tools from linear algebra to calculate the polynomials for a restricted range of degrees. We started by using the Smith normal form of a matrix that writes a homogeneous basis through a known (non-homogeneous) integer-valued one. This method produced results, but calculating the necessary Smith normal form becomes computationally impossible beyond degree 22, given the memory required for such calculations. Our next approach was to use the Hermite normal form, where we focused on finding the intersection of three submodules of the homogeneous 3-variable IVPs whose regular bases we can compute completely. This allowed us to calculate a basis up to degree 25 when localized at $p = 2$ and even further for other primes.

Even though the two previous methods produced IVPs with largest denominators possible, the polynomials are irreducible and tend to have many terms, which makes if difficult to find a general pattern for their construction. This is what the second part of our explorations addresses. How can we construct such polynomials more generally? Ideally, we want to write these as a product of linear factors, as is the case of the polynomials in the basis for $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$.

Since we are interested in the 3-variable case and wonder how large k can p^k be in the denominator of an IVP, our approach is to find these using generalized projective planes. These were first introduced by Klingenberg in [Kli54]. The connection between evaluating IVPs and finite projective planes is as follows: for $f(x, y, z)$ homogeneous of degree m we have $f(\lambda x, \lambda y, \lambda z) = \lambda^m f(x, y, z)$. Thus when evaluating at any triple (x', y', z'), where p divides all three of x', y', z', $f(x', y', z')$ will always be divisible by p^m. Similarly when working locally we are interested in dividing by p^h but not in the remaining result, so multiplication by units in $\mathbb{F}_p$ will not affect our results. This corresponds to how finite projective planes are built, and so we have a correspondence between polynomials with linear factorizations and union of lines in projective planes. Since we are interested in how large a power of p can be present in the denominator, we will need to work over the ring $\mathbb{Z}/(p^k)$, for $k \leq h$, instead of the field $\mathbb{F}_p$ which will have us work with projective Hjelmslev planes. The polynomials constructed from these unfortunately did not admit as large a denominator as the ones obtained from the computational methods, but are much simpler to understand.

This thesis is structured as follows: in Chapter 2 we will set up the basic definitions for studying IVPs and motivate why we study these. Then Chapter 3 will explain how homogeneous IVPs connect to algebraic topology. We then restrict the situation to the simpler case of looking at polynomials that are integer-valued at odd values only in Chapter 4. The next two chapters are on the computational data we have for homogeneous 3-variable polynomials. Lastly, we use projective H-planes to construct high degree homogeneous 3-variable IVPs in Chapter 7.

Chapter 2

Background and a Survey of Known Results

The goal of research in this area is to develop methods for computing a basis and the valuative capacity (an invariant) of the ring of IVPs in one or several variables, in both the homogeneous and general cases.

This is an expository chapter that reviews the work that has been done on integer-valued polynomials (IVPs) and that is used as a basis of this project. The chapter starts with general single variable results, then generalizes to the multivariable case where we look at the existing results on the homogeneous case. The chapter ends by summarizing results for the 2-variable homogeneous case.

In general, the ring of IVPs on a domain D is a free D-module [CC97, I.1]. In certain cases, we can not only obtain that our module has a basis but also that the basis is regular (i.e., that there is one polynomial of each degree in the basis). But knowing this does not guarantee that we can find the basis, so this work will look into finding some of these. Since the results from this thesis are over $\mathbb{Z}$, $\mathbb{Z}/(p)$ and $\mathbb{Z}_{(p)}$, the results from the background section have been restricted to $\mathbb{Z}$.

2.1 Integer-valued Polynomials

For the rest of this chapter let $S \subseteq \mathbb{Z}$.

Definition 1. [CC97, I.1] *For any subset S, the ring of integer-valued polynomials on S is defined to be*

$$\mathrm{Int}(S, \mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(S) \subseteq \mathbb{Z}\}.$$

Definition 2. [CC97, II.1] *The sequence of characteristic ideals of S is given by $(I_n \mid n = 0, 1, 2, \ldots)$ where I_n is the fractional ideal of $\mathbb{Q}$ formed by 0 and the leading coefficients of the elements of $\operatorname{Int}(S, \mathbb{Z})$ of degree no more than n. The characteristic sequence of S with respect to a fixed prime p is the sequence of negatives of the p-adic valuations of these ideals, denoted by $\alpha_{S,p}(n)$.*

In 1997, Bhargava introduced the following definition which is very important when studying IVPs:

Definition 3. [Bha97, 2] *For $S \subseteq \mathbb{Z}$, and p a fixed prime, a p-ordering of S is a sequence $(a_n)_{n\geq 0}$, such that for each n, $a_n \in S$ is chosen to minimize*

$$\nu_p((a_n - a_{n-1}) \cdots (a_n - a_0)).$$

a_0 can be chosen to be any element of S, and $\nu_p(m)$ is the p-adic valuation of m, that is, the largest k such that p^k divides m.

Definition 4. [Bha97] *Define*

$$\operatorname{Int}_m(S, \mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(S) \subseteq \mathbb{Z},\ \deg(f) \leq m\},$$

that is the set of IVPs over $\mathbb{Z}$ of degree less than or equal to m.

Bhargava proved the following proposition that links IVPs to p-orderings by using the characteristic sequence (Definition 2):

Proposition 5. [Bha97, Th. 19] *Let $(a_n)_{n\geq 0}$ be a sequence of distinct elements of S. Then, $(a_n)_{n\geq 0}$ is a p-ordering of S if and only if for all m, ($0 \leq n \leq m$), the polynomials*

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}$$

form a basis for the $\mathbb{Z}_{(p)}$-module $\operatorname{Int}_m(S, \mathbb{Z}_{(p)}) = \{f(x) \in \mathbb{Q}[x] \mid f(S) \subseteq \mathbb{Z}_{(p)},\ \deg(f) \leq m\}$. In this case we have that $\nu_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \alpha_{S,p}(n)$ for $0 \leq n \leq m$.

2.1.1 Significance of Integer-valued Polynomials

In their monograph [CC97, Introduction] Cahen and Chabert introduce the study of IVPs, which are beautiful and interesting to study from a number theory perspective. They give answers to the classic problem of how much can we divide? By writing a polynomial as a product of linear factors we get more control of the divisibility after input values, and ideally we obtain high divisibility for all elements in the set of interest. Below are some interesting algebraic properties of IVPs.

For a domain D, it is worth studying the ring $\operatorname{Int}(S, D)$ (denoted $\operatorname{Int}(D)$ in the special case $S = D$) on its own, since it has nice properties and relates to various mathematical areas. This subsection shows some interesting known results about IVPs. These will not be proved in this thesis, but they demonstrate many of the interesting connections between IVPs and other areas of mathematics. The connections between topology and IVPs will be explored in Chapter 3.

They study $\operatorname{Int}(D)$ and its connection to D itself. Localizations of these rings have been studied, and IVPs behave well with respect to localization. For example, if D is Noetherian, given a multiplicative subset S of D we get that $S^{-1}\operatorname{Int}(D)$ and $\operatorname{Int}(S^{-1}D)$ are equal [CC97, Prop I.2.7].

Taking D to be local with unique maximal ideal $\mathfrak{m}$, we can consider the $\mathfrak{m}$-adic topology and prove that IVPs are uniformly continuous from $\hat{D}$ to $\hat{D}$, where $\hat{D}$ denotes the completion of D with respect to the $\mathfrak{m}$-adic topology. Using this, Mahler's results on p-adic continuous functions can be extended, proving an $\mathfrak{m}$-adic version of the Stone-Weierstrass approximation theorem. Although $\operatorname{Int}(\mathbb{Z})$ is not Noetherian, thus not a Dedekind domain, it is a two-dimensional Prüfer domain that is not an intersection of rank one valuation domains [Cha14, §2].

2.2 Known Results: General Cases

2.2.1 Bhargava's Work

Manjul Bhargava [Bha00] has contributed to many areas of mathematics. In this section we introduce some of his work that relates to IVPs, that is, results about factorials and p-orderings. A good introduction to this topic is [Bha00], where the author does not aim to prove one main result, but, instead, gives information about the factorial function from a number theoretic perspective, which is often forgotten given all the combinatorial attention that the factorial gets. The most well-know number theoretical result about the factorial is that $k!$ divides the product of any k consecutive integers. An equivalent statement of this is

Theorem 6. [Bha00, Th. 1] *For any non-negative integers k and ℓ, $(k+\ell)!$ is a multiple of $k!\ell!$.*

Proof.

$$\frac{(k+\ell)!}{k!\ell!} = \binom{k+\ell}{k} \in \mathbb{Z}.$$

□

We now look into less trivial applications of the factorial in number theory, and discuss the close relationship between the factorial function and the sets of possible values taken on by a polynomial.

Definition 7. [Bha00, 2] *Given an integral non-zero polynomial f, that is a polynomial with integer coefficients, the fixed divisor of f over $\mathbb{Z}$, $d(\mathbb{Z}, f)$ is the greatest common divisor of all the elements in the image of f on $\mathbb{Z}$, that is*

$$d(\mathbb{Z}, f) = gcd\{f(a) \mid a \in \mathbb{Z}\}.$$

Definition 8. *For an integral polynomial f, if all of the coefficients of f are relatively prime, then f is said to be primitive.*

Theorem 9. [Bha00, Th. 2] *Let f be a primitive polynomial of degree k, and let $d(\mathbb{Z}, f) = gcd\{f(a) \mid a \in \mathbb{Z}\}$. Then $d(\mathbb{Z}, f)$ divides $k!$. (This is sharp, i.e., there are cases where $d(\mathbb{Z}, f) = k!$.)*

Theorem 10. [Bha00, Th. 3] *Let $a_0, a_1, \dots, a_n \in \mathbb{Z}$ be any $n+1$ integers. Then the product of their pairwise differences $\prod_{i<j}(a_i - a_j)$ is a multiple of $0!1!2!\cdots n!$. (This is sharp.)*

Bhargava discusses the relationship between the number of functions from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ and the number of functions from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ that can be represented by polynomials, which is equivalent to the number of functions from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ that can be represented by polynomials.

Theorem 11. [Bha00, Th. 4] *The number of functions from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ that can be represented by polynomials is given by*

$$\prod_{k=0}^{n-1} \frac{n}{gcd(n, k!)}.$$

Note that when n is prime there are n^n such functions.

Then p-orderings are introduced, as in Definition 3 and following this we define:

Definition 12. [Bha00, 4] *Given $(a_n)_{n\geq 0}$ a p-ordering of a subset S of $\mathbb{Z}$, let $\alpha_n(S,p) = v_p((a_n - a_{n-1})\cdots(a_n - a_0))$. Then $(\alpha_n(S,p))$ is the associated p-sequence of S.*

Theorem 13. [Bha00, Th. 5] *The associated p-sequence of S is independent of the choice of p-ordering.*

Example 14. $\mathbb{Z}_{\geq 0}$ in increasing order is a p-ordering of $\mathbb{Z}$ at all primes.

Using this we can get a definition of the factorial function for subsets of $\mathbb{Z}$.

Definition 15. [Bha00, Def. 7] *Let S be any subset of $\mathbb{Z}$. Then the factorial function on S, denoted by $k!_S$. is defined by*

$$k!_S = \prod_p p^{\alpha_k(S,p)}.$$

This definition allows us to revisit the four previous theorems about the factorial for any $S \subseteq \mathbb{Z}$.

Theorem 16. [Bha00, Th. 8] *For any non-negative integers k and ℓ, $(k+\ell)!_S$ is still a multiple of $k!_S\ell!_S$.*

Theorem 17. [Bha00, Th. 9] *Let f be a primitive polynomial of degree k, and let $d(S,f) = gcd\{f(a) \mid a \in S\}$. Then $d(S,f)$ divides $k!_S$. (This is sharp.)*

Theorem 18. [Bha00, Th. 10] *Let $a_0, a_1, \ldots, a_n \in S$ be any $n+1$ integers. Then the product of their pairwise differences $\prod\limits_{i<j}(a_i - a_j)$ is a multiple of $0!_S 1!_S 2!_S \cdots n!_S$. (This is sharp.)*

Theorem 19. [Bha00, Th. 11] *The number of polynomials from S to $\mathbb{Z}/n\mathbb{Z}$ is given by*

$$\prod_{k-0}^{n-1} \frac{n}{gcd(n, k!_S)}.$$

The author proves these statements, which we will omit here. We next look into definitions that come into play quite often when studying this topic.

Definition 20. [Bha00, 7] *Given an integer n, the falling factorial is $x^{(n)} = x(x-1)\cdots(x-n+1)$ and if S is a subset of $\mathbb{Z}$, with p-ordering (a_i), then $x^{(n)_{S,p}} = (x-a_0)(x-a_1)\cdots(x-a_{n-1})$.*

The theorem below forms the foundation for this thesis.

Theorem 21. [CC97, Prop. I.1.1] *A polynomial is integer-valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the binomial polynomials*

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!},$$

for $k = 0, 1, 2, \ldots$. The binomial polynomials with $\binom{x}{0} = 1$ actually form a basis of $\mathrm{Int}(\mathbb{Z})$.

Proof. The polynomials form a $\mathbb{Q}$-basis of $\mathbb{Q}[x]$, since there is one of each degree and one can see that the polynomials are integer-valued. Thus a $\mathbb{Z}$-linear combination of these polynomials is in $\mathrm{Int}(\mathbb{Z})$.

Conversely, let $f \in \mathrm{Int}(\mathbb{Z})$, and write $f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_n \binom{x}{n}$, where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Q}$. Then $\lambda_0 = f(0) \in \mathbb{Z}$. Suppose by induction on $k < n$ that $\lambda_i \in \mathbb{Z}$ for $i \leq k$. Then $g_k = f - \sum_{i=0}^{k} \lambda_i \binom{x}{i}$ is integer-valued and $g_k = \lambda_{k+1}\binom{x}{k+1} + \cdots + \lambda_n \binom{x}{n}$. Therefore $\lambda_{k+1} = g_k(k+1) \in \mathbb{Z}$, since for all $i \geq k+1$, $\binom{x}{i} = 0$. □

Note that various forms of this result existed before the monograph [CC97], which describes them in its Historical introduction.

Theorem 22. [Bha00, Th. 23] *A polynomial is integer-valued on a subset S of $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials*

$$\frac{B_{k,S}}{k!_S} = \frac{(x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k})}{k!_S},$$

for $k = 0, 1, 2, \ldots$, where $(a_{i,k})_{i=0}^{\infty}$ is a sequence in $\mathbb{Z}$ that is term-wise congruent modulo $\nu_k(S,p)$ to a p-ordering of S, for each prime p dividing $k!_S$.

The author then discusses the multivariable case, but we will review this in a later section. He then explores other applications of generalized factorial functions, one of these being p-adic interpolation. Using the previous and generalizing to the subset of a local field, one can obtain:

Theorem 23. [Bha00, Th. 4] *Let S be any compact subset of a local field K. Then every continuous map $f\colon S \to K$ can be expressed uniquely in the form*

$$f(x) = \sum_{n=0}^{\infty} c_n \frac{B_{n,S}(x)}{n!_S},$$

where the sequence c_n tends to 0 as $n \to \infty$.

2.2.2 Single Variable: Summary of [Cha14]

This paper surveys the research area of IVPs, and presents most approaches that have been used so far, includng generalizations. One of the goals of this paper is to identify, for a domain D, when $\mathrm{Int}(D)$ has a regular basis, and, when possible to find that basis. This paper focuses on the additive properties of $\mathrm{Int}(D)$ and we will use these for $\mathrm{Int}(\mathbb{Z})$.

For example, some polynomials in $\mathrm{Int}(\mathbb{Z})$ are $\binom{x}{n}$ for $n \geq 2$, and $F_p(x) = \frac{x^p - x}{p}$ for p a prime by Fermat's Little Theorem ([DF04, pg. 96]).

Proposition 24. [CC97, II.2] *The set* $\{1, x\} \cup \{(x^p - x)/p \mid p \in \mathbb{P}\}$*, where* $\mathbb{P}$ *is the set of all primes, is a minimal system of polynomials in which every element of* $\mathrm{Int}(\mathbb{Z})$ *may be constructed by means of sums, products and compositions, i.e., the removal of any of these polynomials will not give* $\mathrm{Int}(\mathbb{Z})$*.*

Proposition 25. [Cha14, 2.3] *For every integer-valued polynomial* g *of degree* n*,* $n! \cdot g(x) \in \mathbb{Z}[x]$*.*

Proposition 26. [Cha14, 3.2] *The subset formed by the leading coefficients of the integer-valued polynomials of degree* $\leq n$*, that is, the characteristic ideal of* $\mathrm{Int}(\mathbb{Z})$*, is* $\frac{1}{n!}\mathbb{Z}$*.*

For $S \subseteq \mathbb{Z}$ we have defined $\mathrm{Int}(S, \mathbb{Z})$ and we have the following inclusions:

$$\mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z}) \subseteq \mathrm{Int}(S, \mathbb{Z}) \subseteq \mathbb{Q}[x].$$

Now we consider a $\mathbb{Z}$-algebra $\mathbb{B}$ such that $\mathbb{Z}[x] \subseteq \mathbb{B} \subseteq \mathbb{Q}[x]$.

Definition 27. *A basis of the* $\mathbb{Z}$*-module* $\mathbb{B}$ *is said to be a regular basis if it contains exactly one polynomial of degree* n*, for all non-negative integers* n*.*

Definition 28. *Two subsets* E *and* F *of* $\mathbb{Z}$ *are said to be polynomially equivalent if* $\mathrm{Int}(E, \mathbb{Z}) = \mathrm{Int}(F, \mathbb{Z})$*.*

Similar to the characteristic sequence (see Definition 2), we get:

Definition 29. *The characteristic ideal of index* n *of the* $\mathbb{Z}$*-module* $\mathbb{B}$ *is the fractional ideal* $\mathfrak{J}_n(\mathbb{B})$ *formed by 0 and the leading coefficients of the polynomials in* $\mathbb{B}$ *of degree less than or equal to* n *for all* $n \geq 0$*.*

Clearly, $(\mathfrak{J}_n(\mathbb{B}))_{n \in \mathbb{N}}$ is an increasing sequence of $\mathbb{Z}$-modules such that: for all $k, \ell \in \mathbb{N}$, $\mathbb{Z} \subseteq \mathfrak{J}_k(\mathbb{B}) \subseteq \mathbb{Q}$ and $\mathfrak{J}_k(\mathbb{B}) \cdot \mathfrak{J}_\ell(\mathbb{B}) \subseteq \mathfrak{J}_{k+\ell}(\mathbb{B})$.

Lemma 30. [Cha14, Prop. II.3.1] *Let f be a polynomial in $\mathbb{Q}[x]$ with degree n. Assume that $x_0, x_1, \ldots, x_n$ are distinct elements of $\mathbb{Q}$ such that $f(x_i) \in \mathbb{Z}$ for $0 \leq i \leq n$, then df belongs to $\mathbb{Z}[x]$ where $d = \prod\limits_{0 \leq i < j \leq n} (x_j - x_i)$.*

Proposition 31. [Cha14, Prop. II.1.4] *A sequence of polynomials $(f_n)_{n \geq 0}$, where $deg(f_n) = n$, is a regular basis of $\mathbb{B}$ if and only if, for every $n \geq 0$, the ideal generated by the leading coefficients of the $f_n s$ is $\mathfrak{J}_n(\mathbb{B})$. In particular, the $\mathbb{Z}$-algebra* $\mathrm{Int}(\mathbb{B})$ *admits a regular basis as a $\mathbb{Z}$-module if and only if all the $\mathfrak{J}_n(\mathbb{B})s$ are principal.*

Example 32. When $S = \mathbb{Z}$, $\mathfrak{J}_n(\mathbb{Z}) = \frac{1}{n!}\mathbb{Z}$.

The inverse of a nonzero fractional ideal $\mathfrak{J}$ of $\mathbb{Z}$ is the fractional ideal $\mathfrak{J}^{-1} = \{x \in \mathbb{Q} \mid x\mathfrak{J} \subseteq \mathbb{Z}\}$.

Definition 33. *The factorial ideal $n!_S^{\mathbb{Z}}$ of index n of the subset S with respect to the domain D is the inverse of the fractional ideal $\mathfrak{J}_n(S, \mathbb{Z})$, i.e., $n!_S^{\mathbb{Z}} = \mathfrak{J}_n(S, \mathbb{Z})^{-1}$.*

The sequence $(n!_S^{\mathbb{Z}})_{n \in \mathbb{N}}$ is a decreasing sequence of integral ideals of $\mathbb{Z}$.

Proposition 34. [CC97, II.3.7] *Given the factorial ideals $n!_S^{\mathbb{Z}} = d_n\mathbb{Z}$, the polynomials $\frac{1}{d_n} g_n(x)$ then form a regular basis of the $\mathbb{Z}$-module* $\mathrm{Int}(S, \mathbb{Z})$.

Proposition 35. [CC97, II.3.7] *The $\mathbb{Z}$-module* $\mathrm{Int}(S, \mathbb{Z})$ *is free.*

2.2.3 Multivariable Integer-valued Polynomials

We can now look into the ring of IVPs for the multivariable case as in [Cha14] and [Evr12] and generalize some of the previous results, which gets us closer to our goal of studying homogeneous 3-variable polynomials. Let m be a positive integer, let $\underline{S}$ be a subset of $\mathbb{Z}^m$ and let $m_0, m_1, \ldots$ be any ordering of the monomials of $\mathbb{Z}^m[\underline{x}]$, and consider the $\mathbb{Z}$-algebra

$$\mathrm{Int}(\underline{S}, \mathbb{Z}) = \{f(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m] \mid f(\underline{S}) \subseteq \mathbb{Z}\}.$$

Let $\mathfrak{J}_n(\underline{S}, \mathbb{Z})$ be the $\mathbb{Z}$-module generated by all the coefficients of the polynomials of total degree less than or equal to n in $\text{Int}(\underline{S}, \mathbb{Z})$ and let

$$n!_{\underline{S}}^{D} = \mathfrak{J}_n(\underline{S}, \mathbb{Z})^{-1} = \{x \in \mathbb{Z} \mid xf \in \mathbb{Z}[x_1, \ldots, x_m] \forall f \in \text{Int}(\underline{S}, \mathbb{Z}), deg(f) \leq n\}.$$

For $\ell \geq 1$ and any sequence $(\underline{x}_0, \ldots, \underline{x}_{\ell-1})$ of elements of $\mathbb{Z}^m$, let

$$\Delta(\underline{x}_0, \ldots, \underline{x}_{\ell-1}) = \det(m_j(\underline{x}_i))_{0 \leq i,j < \ell}.$$

Before looking into bases for the multivariable case, we generalize p-ordering, and, therefore factorials. In Definition 3 of p-ordering, choosing a_k to minimize the power of p dividing the product of differences is equivalent to choosing a_k such that it minimizes the p-adic valuation of the following Vandermonde determinant [Bha00]:

$$\begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^k \\ 1 & a_1 & a_1^2 & \cdots & a_1^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_k & a_k^2 & \cdots & a_k^k \end{vmatrix} = \prod_{i<j} (a_i - a_j).$$

Before generalizing p-orderings to many variables, we need to assume that no non-zero polynomial $f \in \mathbb{Q}[\underline{x}]$ is such that $f(\underline{S}) = 0$. We will assume that we have a sequence of monomials $(m_j)_{j \geq 0}$ that have an order which is compatible with the total degree, so that for $i < j$ we have $\deg(m_i) \leq \deg(m_j)$.

Definition 36. [Evr12, 4] *Let $\underline{S}$ be a subset of $\mathbb{Z}^n$. Then for a fixed ordering $m_0, m_1, \ldots$ of the monomials of $\mathbb{Z}[x_1, \ldots, x_n]$, a p-ordering of $\underline{S}$ is a sequence $\underline{a}_0, \underline{a}_1, \ldots$ of the elements in $\underline{S}$ inductively chosen so that $\underline{a}_k$ minimizes $\nu_p(\Delta(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_k))$ where*

$$\Delta(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_k) = \begin{vmatrix} m_0(\underline{a}_0) & m_1(\underline{a}_0) & m_2(\underline{a}_0) & \cdots & m_k(\underline{a}_0) \\ m_0(\underline{a}_1) & m_1(\underline{a}_1) & m_2(\underline{a}_1) & \cdots & m_k(\underline{a}_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_0(\underline{a}_k) & m_1(\underline{a}_k) & m_2(\underline{a}_k) & \cdots & m_k(\underline{a}_k) \end{vmatrix}.$$

The associated p-sequence of $\underline{S}$ is then given by

$$\alpha_k(\underline{S}, p) = \nu_p\left(\frac{\Delta(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_k)}{\Delta(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{k-1})}\right),$$

and the generalized factorial $k!_{\underline{S}}$ is

$$k!_{\underline{S}} = \prod_p \alpha_k(\underline{S}, p).$$

When $\underline{S}$ is a Cartesian product, its factorials are easy to compute, since they can be obtained as in the single variable case. This is still the case when $\underline{S}$ is polynomially equivalent (recall Definition 28) to a Cartesian product. It would be interesting to compute factorials for subsets that are not polynomially equivalent to a Cartesian product [Evr12]. This thesis will look at some of these cases.

Below is a proposition found in [Cha14] that summarizes the results from [Evr12]:

Proposition 37. [Cha14][Evr12, 19,20] *Let $(\underline{a}_k)_{k\geq 0}$ be a sequence of elements of $\underline{S}$ such that, for every $k \geq 0$, $\Delta(\underline{a}_0, \dots, \underline{a}_k) \neq 0$. Furthermore, consider the associated polynomials*

$$F_k(\underline{x}) = \frac{\Delta(\underline{a}_0, \dots, \underline{a}_{k-1}, \underline{x})}{\Delta(\underline{a}_0, \dots, \underline{a}_k)}.$$

The following assertions are equivalent:

1. *$(\underline{a}_k)_{k\geq 0}$ is a p-ordering of $\underline{S}$.*

2. *For every $k \geq 0$, $F_k \in \mathrm{Int}(\underline{S}, \mathbb{Z})$.*

3. *$\{F_k(\underline{x})\}_{k\geq 0}$ is a basis if the $\mathbb{Z}$-module $\mathrm{Int}(\underline{S}, \mathbb{Z})$.*

4. *For every $f(\underline{x}) \in \mathbb{Q}[\underline{x}]$, if the indices of the monomials of f are less than k, then $f(\underline{x}) \in \mathrm{Int}(\underline{S}, \mathbb{Z}) \Leftrightarrow f(\underline{a}_0), \dots, f(\underline{a}_{k-1}) \in \mathbb{Z}$.*

We now look into a case where we can construct a basis:

Proposition 38. *The polynomials $\{\binom{x}{r}\binom{y}{s} \mid r, s \in \mathbb{Z},\ r, s \geq 0\}$ form a basis of the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z}^2, \mathbb{Z})$.*

Proof. $\binom{x}{r}\binom{y}{s}$ form a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[x,y]$, since we can obtain all monomials, i.e., $\binom{x}{r}\binom{y}{s}$ has leading term $x^r y^s$. Since $\binom{x}{r}$ and $\binom{y}{s}$ are integer-valued, their product is as well, and any $\mathbb{Z}$-linear combination of these polynomials is integer-valued.

Conversely, let $f \in \mathrm{Int}(\mathbb{Z}^2,\mathbb{Z})$ be a polynomial of degree $n+m$ and

$$f(x,y) = \sum_{\substack{r,s\geq 0,\\ r\leq n,\ s\leq m}}^{n+m} a_{r,s}\binom{x}{r}\binom{y}{s},$$

with $a_{r,s} \in \mathbb{Q}$. It suffices to show $a_{r,s} \in \mathbb{Z}$. We first order the terms by increasing degree of $r+s$, then for a given $r+s=k$, we order by increasing degree of r. Suppose by induction on $k \leq n+m$ that $a_{r,s} \in \mathbb{Z}$ for $r+s \leq k$. For $r+s=k+1$, there can be up to $k+2$ terms of this degree, since the are at most $k+2$ distinct pairs such that $r+s=k+1$, so we proceed by induction on these terms. Suppose that for all $j < k+1$, $a_{j,s} \in \mathbb{Z}$. When $j+s=k+1$, we need to show that $a_{j+1,s} \in \mathbb{Z}$. In order to use our induction hypothesis we work with

$$g_{k,j} = f - \sum_{\substack{r+s\leq k\\ r\leq j}} a_{r,s}\binom{x}{r}\binom{y}{s}$$

then $g_{k,j} = a_{j+1,s}\binom{x}{j+1}\binom{y}{s} + \cdots + a_{n,m}\binom{x}{n}\binom{y}{m}$. Therefore $a_{j+1,s} = g_{k,j}(j+1,s)$, since for all i such that $i \geq j+1$ we have $\binom{x}{i} = 0$. □

This result will be used in Chapter 4 to connect the homogenous 3-variable case to the general 2-variable case. Induction can be used to obtain the following, which will be proven in the next section:

Corollary 39. *The polynomials* $\left\{\binom{x_1}{r_1}\binom{x_2}{r_2}\cdots\binom{x_n}{r_n} \mid r_1,\ldots,r_n \in \mathbb{Z},\ r_1,\ldots,r_n \geq 0\right\}$ *form a basis of the* $\mathbb{Z}$*-module* $\mathrm{Int}(\mathbb{Z}^n,\mathbb{Z})$.

2.3 Integer-valued Homogeneous Polynomials

2.3.1 Numerical Forms [Hub97]

In his paper Numerical Forms [Hub97], which is the term the author uses for homogeneous IVPs, Hubbuck gives a bound for the coefficients of a numerical form. The goal of that paper is to show:

Proposition 40. [Hub97, Prop. 1.3] *For a fixed prime p, there exist monotonic increasing polynomials $u_n(z)$ and $v_n(z)$ such that the coefficients $a_{i_1,i_2,\ldots,i_n}$ of any numerical M-form, a form, hence a polynomial, of degree M, in n variables satisfy*

$$\nu(a_{i_1,i_2,\ldots,i_n}) > \frac{M - u_n(t)}{v_n(t)}.$$

Here t is the integer such that $p^{t+1} - 1 > M - n + 1 \geq p^t - 1$ and ν is the valuation such that $\nu(\frac{s}{r \cdot p^u}) = u$, where $p \nmid r$ and $p \nmid s$.

The construction of the single variable polynomials $u_n(z)$ and $v_n(z)$ can be found at the end of the paper. A consequence of this result is the following:

Proposition 41. [Hub97, Abstract] *If I is the graded ring of homogeneous rational polynomials in n-variables which are numerical over $\mathbb{Z}$, then I is a subring of Γ, the divided polynomial algebra over $\mathbb{Z}$ in n-variables. For any positive integer k, the image of the induced homomorphism $I \otimes (\mathbb{Z}/k\mathbb{Z}) \to \Gamma \otimes (\mathbb{Z}/k\mathbb{Z})$ is a finite graded ring.*

2.3.2 2-Variable Homogeneous IVPs [JP11]

Keith Johnson and Donald Patterson have determined a basis for homogeneous IVP in degree two. This section will summarize their work and then indicate where the case of 3-variables differs given the computational results obtained in further chapters. In this paper the idea of p-orderings is extended to $\mathbb{Z}^2$ or $\mathbb{Z}^2_{(p)}$ in such a way as to give a construction of a basis for the $\mathbb{Z}_{(p)}$-module of p-local integer-valued homogeneous polynomials in 2-variables.

Definition 42. [JP11, Def. 4] *Let S be a subset of $\mathbb{Z}_{(p)}^2$. A projective p-ordering of S is a sequence $((a_i, b_i) \mid i = 0, 1, 2, \ldots)$ in S with the property that for each $i > 0$ the element (a_i, b_i) minimizes $\nu_p\left(\prod_{j<i}(sb_j - ta_j)\right)$ over all pairs $(s, t) \in S$. The sequence $(d_i \mid i = 0, 1, 2, \ldots)$ with $d_i = \nu_p\left(\prod_{j<i}(a_i b_j - b_i a_j)\right)$ is the p-sequence of the p-ordering.*

Lemma 43. [JP11, Lem. 5]

1. *If $((a_i, b_i) \mid i = 0, 1, 2, \ldots)$ is a projective p-ordering of $\mathbb{Z}_{(p)}^2$, then for each index i either $\nu_p(a_i) = 0$ or $\nu_p(b_i) = 0$.*
2. *If $((a_i, b_i) \mid i = 0, 1, 2, \ldots)$ is a projective p-ordering of $\mathbb{Z}_{(p)}^2$, then there is another projective p-ordering $((a_i', b_i') \mid i = 0, 1, 2, \ldots)$ with the property that for each index i either $a_i' = 1$ and $p \mid b_i'$, or $b_i' = 1$ and $((a_i', b_i') \mid i = 0, 1, 2, \ldots)$ has the same p-sequence as $((a_i, b_i) \mid i = 0, 1, 2, \ldots)$.*

Definition 44. [JP11, Def. 6] *Let S denote the subset of $\mathbb{Z}_{(p)}^2$ consisting of pairs (a, b) with either $a = 1$ and $p \mid b$, or $b = 1$ and let $S_0 = ((a, 1) \mid a \in \mathbb{Z}_{(p)})$ and $S_1 = ((1, pb) \mid b \in \mathbb{Z}_{(p)})$.*

Lemma 45. [JP11, Lem. 7] *The set S is the disjoint union of S_0 and S_1, and if $(a, b) \in S_0$ and $(c, d) \in S_1$, then $\nu_p(ad - bc) = 0$.*

Definition 46. *The shuffle S of two sequences S_i and S_j is obtained by arranging the elements ofS_i and S_j in non-decreasing order in S such that the elements of each sequence are in the same order. That is, if you ignore the elements of S_j in S, you obtain S_i and vice versa.*

Proposition 47. [JP11, Prop. 8] *Any projective p-ordering of S is the shuffle of projective p-orderings of S_0 and S_1 into nondecreasing order. The shuffle of any pair* *of p-sequences of S_0 and S_1 into nondecreasing order gives a p-sequence of S and the corresponding shuffle of the projective p-orderings of S_0 and S_1 that gave rise to these p-sequences gives a projective p-ordering of S.*

Proposition 48. [JP11, Prop. 10]

1. *A projective p-ordering of $\mathbb{Z}^2_{(p)}$ is given by the periodic shuffle of the sequences $((i,1) \mid i = 0,1,2,\ldots)$ and $((1,pi) \mid i = 0,1,2,\ldots)$ which takes one element of the second sequence after each block of p elements of the first. The corresponding p-sequence is $\left(\nu_p\left(\lfloor \frac{pi}{p+1} \rfloor\right) \mid i = 0,1,2,\ldots\right)$.*

2. *The p-sequence of $\mathbb{Z}^2_{(p)}$ is independent of the choice of projective p-ordering used to compute it.*

Proposition 49. [JP11, Prop. 11] *If $((a_i,b_i) \mid i = 0,1,2,\ldots)$ is a projective p-ordering of $\mathbb{Z}^2_{(p)}$, then the polynomials*

$$f_n(x,y) = \prod_{i=0}^{n-1} \frac{xb_i - ya_i}{a_nb_i - b_na_i}$$

are homogeneous and $\mathbb{Z}_{(p)}$-valued on $\mathbb{Z}^2_{(p)}$.

The following will help us actually find a basis for the homogeneous 2-variable polynomials and will be illustrated with an example.

Definition 50. [JP11, Def. 12] *For $0 \leq n \leq m$ and $((a_i,b_i) \mid i = 0,1,2,\ldots)$, the projective p-ordering of $\mathbb{Z}^2_{(p)}$ constructed in Proposition 48, let*

$$g_n^m(x,y) = \begin{cases} y^{m-n} \displaystyle\prod_{i=0}^{n-1} \frac{xb_i - ya_i}{a_nb_i - b_na_i} & \text{if } (a_n,b_n) \in S_0 \\[2em] x^{m-n} \displaystyle\prod_{i=0}^{n-1} \frac{xb_i - ya_i}{a_nb_i - b_na_i} & \text{if } (a_n,b_n) \in S_1. \end{cases}$$

Lemma 51. [JP11, Lem. 13] *The polynomials $g_n^m(x,y)$ have the properties*

$$g_n^m(a_i,b_i) = \begin{cases} 0 & \text{if } i < n \\ 1 & \text{if } i = n. \end{cases}$$

Proposition 52. [JP11, Prop. 14] *The set of polynomials $\{g_n^m(x,y) \mid n = 0,1,2,\ldots,m\}$ form a basis for the $\mathbb{Z}_{(p)}$-module of homogeneous polynomials in $\mathbb{Q}[x,y]$ of degree m which take values in $\mathbb{Z}_{(p)}$ when evaluated at points of $\mathbb{Z}^2_{(p)}$.*

Example 53. [JP11, Ex. 15] Let $p = 2$ and $m = 3$. By Proposition 48 the following is a projective 2-ordering of $\mathbb{Z}^2_{(p)}$:

$$\begin{array}{lll} (0,1), & (1,1), & (1,0), \\ (2,1), & (3,1), & (1,2), \\ (4,1), & (5,1), & \ldots \quad . \end{array}$$

With this projective 2-ordering we construct $g_n^3(x,y)$ for $n = 0,1,2,3$ and obtain the following basis:

$$\left\{ y^3, xy^2, x^2(x-y), \frac{xy(x-y)}{2} \right\}.$$

This method will be helpful to obtain basis elements in the 3-variable case by either using some of these polynomials or multiplying by other homogeneous polynomials to obtain an explicit 3-variable polynomial. More details about the connection between the 2-variable and 3-variable case can be found in Section 5.2.

Chapter 3

The Connection with Algebraic Topology

The goal of this chapter is to describe the connections between algebraic topology and IVPs, especially the homogeneous ones. This chapter will assume some familiarity with algebraic topology, since that subject would require more than a chapter of explanations by itself. This chapter will show how elements of certain groups arising in topology are isomorphic to IVPs.

One motivation for studying homogeneous IVPs is their application to topology. This can be established by starting with the Adams-Novikov spectral sequence, more details about this subject can be found in [Rav86], which gives a tool for computing homotopy groups of a topological space or spectrum X with the help of generalized homology or cohomology theory. From a topological perspective this sequence is useful for calculating stable homotopy groups of spheres. The spectral sequence is known to converge, in many cases, to $\pi_*^S(X)$, the stable homotopy groups of X.

For a space X the Adams spectral sequence [Ada58] is based on $H^*(X, \mathbb{Z}/(p))$ and an important part of this sequence is the E_2-term which can be defined and computed in strictly algebraic terms. The Adams-Novikov [Nov67] sequence, which is also called the E_*-Adams sequence, is the analogous sequence based on a general cohomology or homology theory, $E^*(\ )$ or $E_*(\ )$.

For the study of IVPs the homology theory of interest is $K_*(\ )$, complex K-theory. Recall, from [Rav86, 2.1], that $E_*(X)$ is a comodule over the $\pmod p$ commutative Hopf algebra $A = E_*E$.

Theorem 54. [Rav86, Th. 2.1.1] *Let X be a topological space. There is a spectral sequence converging to $\pi_*^S(X)$ with $E_*^{**}(X)$ and differentials $d_r \colon E_r^{s,t} \to E_r^{s+r,t+r-1}$ such that* *(a)* $E_2^{s,t} = Ext_A^{s,t}(E_*(X, \mathbb{Z}/(p)), E_*(X, \mathbb{Z}/(p)))$*, with* $A = E_*E$*.*

(b) If X *is of finite type,* E_∞^{**} *is the bigraded group associated with a certain filtration of* $\pi_*^S(X) \otimes \mathbb{Z}_p$*, where* $\mathbb{Z}_p$ *denotes the ring of* p*-adic integers.*

In this theorem we have that E_* is a homology theory and Ext is the algebraic object. The idea behind the Adams spectral sequence is to use our knowledge of $\pi_*^S(E)$ and $E_*(X)$ to get information about $\pi_*^S(X)$.

Using this tool to go from topology to algebra, in 1989 Baker, Clarke, Ray and Schwartz [BCRS89] studied the K-homology of an n-torus BT^n, and showed a connection between homology and homogeneous IVPs, (which are referred to as numerical polynomials in that paper). In this case X is the space BU and E is complex K-theory. Their main focus is on describing the K-homology of CP^∞, the infinite complex projective space, and BT^n, which makes the coaction of the cooperation algebra $K_*(K)$, and hence the primitive submodule, easy to understand.

A previous paper from Adams, Harris and Switzer [AHS71], that had described $K_*(BU)$ and $KO_*(BSp)$, achieves this by mapping elements of $K_0(K)$ and $KO_*(KO)$ to $K_{2n}(K) \otimes \mathbb{Q}$ and $K_{4n}(K) \otimes \mathbb{Q}$ respectively, where KO_* is homology theory for the BO-spectrum which comes from the real Bott periodicity that is described in [AGP02]. The main interest for us is that these elements are mapped to homogeneous 2-variable IVPs, which are of the form

$$\begin{aligned} p_n'(u,v) &= \frac{1}{n!} v(v-u)(v-2u)\cdots(v-(n-1)) \\ q_n'(u,v) &= \frac{2}{(2n+2)!}(v^2-u^2)(v^2-2^2u^2)\cdots(v^2-n^2u^2). \end{aligned}$$

The paper from Baker et al. uses a similar process to give a description of K_*BT^n and K_*BU. They make use of the result from [Cla81]:

Proposition 55. [Cla81, Th. 11] *The ring* $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$ *is isomorphic to* $K_0(CP^\infty)$*, where* $K_0(CP^\infty)$ *has the ring structure induced by the map* $CP^\infty \times CP^\infty \to CP^\infty$ *which classifies the tensor product of line bundles.*

Proposition 56. [BCRS89, Prop. 1.6] *The ring $A_n = \mathrm{Int}(\mathbb{Z}^n, \mathbb{Z})$ is isomorphic to the iterated tensor product $A^{\otimes n}$ and hence has a basis consisting of the elements*

$$\binom{w_1}{k_1}\binom{w_2}{k_2}\cdots\binom{w_n}{k_n}, \quad k_1, k_2, \ldots, k_n \geq 0.$$

Corollary 57. [BCRS89, Cor. 1.7] *If $BT^n = (CP^\infty)^n$ denotes the classifying space of an n-torus then $K_0(BT^n)$ is isomorphic to the ring A_n. The coaction*

$$\psi\colon K_0(BT^n) \to K_0(K) \otimes K_0(BT^n)$$

is the ring homomorphism determined by $\psi(w_i) = w_i \otimes w_i$.

The following two propositions are of interest to us, since they give us a connection to homogeneous IVPs and a way to construct these. By primitive elements here we mean elements x such that $\psi(x) = 1 \otimes x + x \otimes 1$, under the coaction map ψ defined in the above corollary.

Proposition 58. [BCRS89, Prop. 1.8] *The group of primitive elements $P_m K_0(BT^n)$ is isomorphic to the $\mathbb{Z}$-module of IVPs in n-variables which are homogeneous of degree m.*

Thus, studying 3-variable homogeneous IVPs, is another way of studying the primitive elements of the K_*-homology of the 3-torus.

Proposition 59. [BCRS89, Prop. 1.9] *Suppose that $f(w_1, \ldots, w_{n-1}) \in A_{n-1}$ has total degree k and denominator M, so $Mf(w_1, \ldots, w_{n-1})$ has integer coefficients. Then for sufficiently large j,*

$$w_n^{k+j} f(w_1 w_n^{-1}, \ldots, w_{n-1} w_n^{-1})$$

is a homogeneous IVP of degree $k + j$.
In fact $w_n^{k+j} f(w_1 w_n^{-1}, \ldots, w_{n-1} w_n^{-1})$ is integer valued if j is greater than or equal to the maximum exponent of any prime occurring in M.

The estimate for j in that proposition, and in general, is not the best, which motivates our desire to find bases for homogeneous IVPs. The remainder of that section goes over the non-trivial nature of the ring of homogeneous IVPs by exploring the 2-variable case localized at a prime p, (which was continued in the paper from Johnson and Patterson [JP11]) which fully solves the 2-variable case for homogeneous 2-variable IVPs.

In the second section of [BCRS89], the authors explore further the relationship between the homotopy of BU and homogeneous IVPs, which is displayed in the next two statements:

Theorem 60. [BCRS89, Th. 2.1] *As a $K_0(K)$-comodule, $K_0(BU(n))$ may be identified with the submodule of $\mathbb{Q}[x_1, \ldots, x_n]$ consisting of those symmetric polynomials $f(x_1, \ldots, x_n)$ satisfying*

$$\frac{n!}{n_1! \cdots n_r!} f(k_1, \ldots, k_n) \in \mathbb{Z}$$

where the sequence of integers $k_1, \ldots k_n$ contains r distinct elements repeated $n_1, \ldots, n_r$ times, respectively. Here $\mathbb{Q}[x_1, \ldots, x_n]$ has the multiplicative comodule structure given by $\psi(x_i) = \omega \otimes x_i$. The map $A_n = K_0(BT^n) \to K_0(BU(n))$ sends an IVP $f(w_1, \ldots, w_n)$ to the symmetrization

$$\left(\frac{1}{n!}\right) \sum_{\sigma \in S_n} f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Where S_n is the symmetric group of permutations of n elements.

Proposition 61. [BCRS89, Cor. 2.2] *The group of primitive elements $P_m K_0(BU(n))$ may be identified with the $\mathbb{Z}$-module of homogeneous symmetric polynomials of degree m satisfying the integrality condition of the theorem.*

Since symmetric homogeneous IVPs give us primitive elements, we will try to also find the symmetrizations of our IVPs in the next sections.

Chapter 4

Polynomials Integer-valued at Odd Values

We begin this project by focusing on the prime $p = 2$, since over $\mathbb{Z}_{(2)}$ odd numbers are invertible. By this we mean we will look into taking $f(x) \in \mathbb{Z}[x]$ and finding a maximal i such that $\frac{f(x)}{2^i}$ is an IVP. In this chapter we restrict our attention to evaluating our polynomials at odd values only. We will start by looking into the 2-variable case, and then establish an isomorphism between the 2-variable IVPs at odd values of degree less than or equal to m and the homogenous 3-variable IVPs at odd values of degree m.

Lemma 62. $\operatorname{Int}(1 + 2\mathbb{Z}, \mathbb{Z})$ *has as basis* $\left\{\binom{(x-1)/2}{n}\right\}_{n \geq 0}$.

Proof. We use the basis for $\operatorname{Int}(\mathbb{Z})$ from Theorem 21, the map

$$\begin{aligned} \mu\colon \operatorname{Int}(\mathbb{Z}, \mathbb{Z}) &\to \operatorname{Int}(1 + 2\mathbb{Z}, \mathbb{Z}) \\ x &\mapsto \frac{x-1}{2} \end{aligned}$$

produces an isomorphism so maps bases to bases, as illustrated below

$$\begin{tikzcd} \mathbb{Z} \arrow[d, "u"'] \arrow[dr, dashed, "\tilde{f}"] & \\ 1 + 2\mathbb{Z} \arrow[r, "f"'] & \mathbb{Z}. \end{tikzcd}$$

□

Proposition 63. $\operatorname{Int}((1 + 2\mathbb{Z})^2, \mathbb{Z})$ *has basis* $\left\{\binom{(x-1)/2}{i}\binom{(y-1)/2}{j}\right\}_{i,j \geq 0}$*, where the denominators of the basis elements are* $2^{i+j} i! j!$.

Proof. This is Lemma 62 applied to Proposition 38. □

This case will allow our polynomials to have bigger denominators and permits us to draw some important conclusions for the general case. We start with definitions that will be useful for the remainder of this work:

Definition 64. $\mathrm{Int}_m(\mathbb{Z}^k, \mathbb{Z})$ *is the submodule of* $\mathrm{Int}(\mathbb{Z}^k, \mathbb{Z})$ *of IVPs of degree less than or equal to m, and* $\mathrm{Int}_m((1+2\mathbb{Z})^k, \mathbb{Z})$ *is the submodule of* $\mathrm{Int}_m(\mathbb{Z}^k, \mathbb{Z})$ *of IVPs at odd values.*

The above is a multivariable generalization of Definition 4.

Definition 65. $\mathrm{Int}^m(\mathbb{Z}^k, \mathbb{Z})$ *is the submodule of* $\mathrm{Int}(\mathbb{Z}^k, \mathbb{Z})$ *consisting of homogeneous IVPs of degree m and* $\mathrm{Int}^m((1+2\mathbb{Z})^k, \mathbb{Z})$ *is the submodule of* $\mathrm{Int}^m(\mathbb{Z}^k, \mathbb{Z})$ *of IVPs at odd values.*

We connect the 3-variable case to the 2-variable one:

Proposition 66. $\mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$ *and* $\mathrm{Int}^m((1+2\mathbb{Z})^3, \mathbb{Z})$ *both have rank* $\frac{(m+1)(m+2)}{2}$.

Proof. In the first case we are counting all non-negative pairs (i, j) such that $i+j \leq m$ and, in the second, all non-negative triples (i, j, k) such that $i + j + k = m$. Both quantities are equal to $\frac{(m+1)(m+2)}{2}$. □

Proposition 67. *We have the isomorphism*

$$\mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z}) \simeq \mathrm{Int}^m((1+2\mathbb{Z})^3, \mathbb{Z}).$$

The isomorphism is given by the maps:

$$\begin{aligned} G\colon \mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z}) &\to \mathrm{Int}^m((1+2\mathbb{Z})^3, \mathbb{Z}) \\ g(x,y) &\mapsto z^m g\left(\frac{x}{z}, \frac{y}{z}\right), \end{aligned}$$

$$\begin{aligned} F\colon \mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z}) &\leftarrow \mathrm{Int}^m((1+2\mathbb{Z})^3, \mathbb{Z}) \\ f(x,y,1) &\leftarrow\!\shortmid f(x,y,z). \end{aligned}$$

Proof. (1) We show that if $g \in \mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$ then $G(g) \in \mathrm{Int}^m((1+2\mathbb{Z})^3, \mathbb{Z})$. First we show that $G(g)$ is homogeneous:

$$\begin{aligned} G(g)(x,y,z) &= z^m g\left(\frac{x}{z}, \frac{y}{z}\right) \\ G(g)(hx,hy,hz) &= (hz)^m g\left(\frac{hx}{hz}, \frac{hy}{hz}\right) \\ &= h^m(G(g)(x,y,z)) \end{aligned}$$

Thus $G(g)$ is homogeneous. It remains to show that if $x, y, z \in (1+2\mathbb{Z})$, then $G(g)(x,y,z) \in \mathbb{Z}$. We know that $\frac{x}{z}, \frac{y}{z} \in 1 + 2\mathbb{Z}_{(2)}$ and $\frac{x}{z} \equiv x' \pmod{2^k}$, $\frac{y}{z} \equiv y' \pmod{2^k}$, for some sufficiently large k (larger than m), and $x', y' \in (1+2\mathbb{Z})$. We then have that

$$G(g)(x,y,z) = z^m g\left(\frac{x}{z}, \frac{y}{z}\right) \equiv z^m g(x', y') \pmod{2^k}$$

and $g(x', y') \in \mathbb{Z}_{(2)}$. Hence $G(g)(x,y,z) \in \mathbb{Z}_{(2)}$ and $G(g)(x,y,z)$ can be represented in $\mathbb{Z}/(2^k)$ for a sufficiently large k.

(2) Lastly, we show that if $f \in \mathrm{Int}^m((1+2\mathbb{Z})^3, \mathbb{Z})$ then $F(f) \in \mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$. We know that for all $a, b, c \in (1+2\mathbb{Z})$, $f(a,b,c) \in \mathbb{Z}$ and therefore $f(a,b,1) \in \mathbb{Z}$. Thus $g = f(a,b,1) \in \mathbb{Z}$ for all $a, b \in (1+2\mathbb{Z})$, and $f(x,y,1)$ is a polynomial where each term is of degree at most m.

(3) The homomorphism property holds from standard homogenization. Lastly, we show that the functions are inverses of each other, i.e. $F(G(g)) = g$ and $G(F(f)) = f$. Let $g(x,y) = \sum_{i+j \leq m} a_{ij} x^i y^j$, then

$$\begin{aligned} G(g) &= \sum_{i+j \leq m} a_{ij} z^m \left(\frac{x}{z}\right)^i \left(\frac{y}{z}\right)^j, \\ F(G(g)) &= \sum_{i+j \leq m} a_{ij} 1^m \left(\frac{x}{1}\right)^i \left(\frac{y}{1}\right)^j \\ &= g(x,y). \end{aligned}$$

Let $f(x,y,z) = \sum_{i+j+k=m} b_{ijk} x^i y^j z^k$, then

$$\begin{aligned}
F(f) &= \sum_{i+j+k=m} b_{ijk} x^i y^j 1^k = \sum_{i+j\leq m} b_{ijk} x^i y^j, \\
G(F(f)) &= \sum_{i+j\leq m} b_{ijk} z^m \left(\frac{x}{z}\right)^i \left(\frac{y}{z}\right)^j = \sum_{i+j\leq m} b_{ijk} z^m \frac{x^i}{z^i} \frac{y^j}{z^j} \\
&= \sum_{i+j\leq m} b_{ijk} z^{m-i-j} x^i y^j = \sum_{i+j+k=m} b_{ijk} z^k x^i y^j \\
&= f(x,y,z).
\end{aligned}$$

□

Remark 68. *Note that in the previous proposition we could just as easily have used $f(x,1,y)$ or $f(1,x,y)$ in the definition of F, with appropriate changes to G.*

We present some properties of $\nu_p(n!)$ which will be very useful for this chapter.

Lemma 69. [Leg30][Mol12, Th. 2.6.1] *(Legendre's Formula) For p a prime and n having the p-adic expansion $n = \sum_{i\geq 0} n_i p^i$, for $n_i \in \mathbb{Z}/(p)$, we have*

$$\nu_p(n!) = \sum_{k\in\mathbb{N},\ p^k\leq n} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - \sum n_i}{p-1}.$$

Proof. For p a prime, $\nu_p(n!) = \sum_{\ell\in\mathbb{N},\ p^\ell\leq n} \left\lfloor \frac{n}{p^\ell} \right\rfloor$, because the number of integers k in the range 1 to n for which $\nu_p(k) \geq \ell$ is $\left\lfloor \frac{n}{p^\ell} \right\rfloor$.

Write $n = \sum_{i\geq 0} n_i p^i$, for i such that $0 \leq i \leq \ell$, $p^\ell \leq n$ and $n_i \in \mathbb{Z}/(p)$. Let k being the greatest integer such that $p^k \leq n$. Then for any $0 \leq r < k$ we have

$$\left\lfloor \frac{n}{p^r} \right\rfloor = n_k p^{k-r} + n_{k-1} p^{k-1-r} + \cdots + n_r.$$

Combining this with the first inequality yields

$$\begin{aligned}\nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= n_k p^{k-1} + n_{k-1} p^{k-2} + \cdots + n_2 p + n_1 \\ &+ n_k p^{k-2} + n_{k-1} p^{k-3} + \cdots + n_2 \\ &\vdots \\ &+ n_k \\ &= n_1 + n_2(p+1) + n_3(p^2+p+1) + \cdots + n_k(p^{k-1} + \cdots + 1) \\ &= \frac{n_1(p-1) + n_2(p^2-1) + n_3(p^3-1) + \cdots + n_k(p^k-1)}{p-1} \\ &= \frac{(n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k) - (n_0 + n_1 + n_2 + \cdots + n_k)}{p-1} \\ &= \frac{n - \sum n_i}{p-1}.\end{aligned}$$

□

Lemma 70. *For an integer n we have*

$$\nu_2((2n)!) = n + \nu_2(n!) = \nu_2(2^n(n!)).$$

Proof. From the definition of the 2-adic valuation we have $\nu_2(2^n(n!)) = n + \nu_2(n!)$. We use Legendre's Formula, Lemma 69, if

$$n = n_i 2^i + n_{i_1} 2^{i-1} + \cdots + n_1 2 + n_0,$$

then $\nu_2(n!) = n - \sum_{0 \leq j \leq i} n_j$. We also have that

$$2n = n_i 2^{i+1} + n_{i_1} 2^i + \cdots + n_1 2^2 + n_0 2,$$

where the sum of the coefficients of the 2-adic expansion is the same as for n. Using Legendre's Formula $\nu_2((2n)!) = 2n - \sum_{0 \leq j \leq i} n_j = n + \nu_2(n!)$. □

Lemma 71. *Given any integer n with 2-adic expansion $n = \sum n_i 2^i = 2^k + n'$, where $n' < 2^k$, we have*

$$\nu_2(n!) = 2^k - 1 + \nu_2(n'!).$$

Proof. By Legendre's Formula, (Lemma 69),

$$\begin{aligned}\nu_2(n!) &= \sum_{i>0} \left\lfloor \frac{2^k + n'}{2^i} \right\rfloor \\ &= \sum_{i>0}^{k} 2^{k-i} + \sum_{i>0} \left\lfloor \frac{n'}{2^i} \right\rfloor.\end{aligned}$$

Since the first sum is a geometric series, this becomes

$$\nu_2(n!) = 2^k - 1 + \nu_2(n'!).$$

□

We next show how to count the number of basis elements with denominator of 2-adic valuation n, for $n < m$ in $\mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$. From Proposition 5 the sequence of 2-adic valuations of the denominators of $\mathrm{Int}(1 + 2\mathbb{Z}, \mathbb{Z})$ is the 2-sequence (recall Definition 12) of $S = (1+2\mathbb{Z})$. Note that for any n we actually have that $\alpha_n(1+2\mathbb{Z}, 2)$ can be calculated using Lemma 70 and is

$$\alpha_n(1 + 2\mathbb{Z}, 2) = n + \alpha_n(\mathbb{Z}, 2) = n + \nu_2(n!) = \nu_2(2^n n!) = \nu_2(2n!).$$

Below we display the 2-sequence of $\mathrm{Int}(1 + 2\mathbb{Z}, \mathbb{Z})$:

degree n	0	1	2	3	4	5	6	7	8	9	10
$\alpha_n(1 + 2\mathbb{Z}, 2)$	0	1	3	4	7	8	10	11	15	16	18

Table 4.1: 2-Sequence for $\mathrm{Int}(1 + 2\mathbb{Z}, \mathbb{Z})$

For $\mathrm{Int}_m((1 + 2\mathbb{Z})^2, \mathbb{Z})$ the basis elements are obtained as products of basis elements for each variable x, y, thus we add exponents in a square array. Each i, j-entry in the table is

$$i + j + \alpha_{\mathbb{Z}}(i) + \alpha_{\mathbb{Z}}(j) = (i + j) + \nu_2(i!j!) = \nu_2(2i!2j!) = \nu_2(2^{i+j} i!j!).$$

From here on, the matrix representation of Table 4.2 will be called M.

		degree of x													
		0	1	2	3	4	5	6	7	8	9	10	11	12	13
	0	0	1	3	4	7	8	10	11	15	16	18	19	22	23
	1	1	2	4	5	8	9	11	12	16	17	19	20	23	24
	2	3	4	6	7	10	11	13	14	18	19	21	22	25	26
	3	4	5	7	8	11	12	14	15	19	20	22	23	26	27
	4	7	8	10	11	14	15	17	18	22	23	25	26	29	30
degree of y	5	8	9	11	12	15	16	18	19	23	24	26	27	30	31
	6	10	11	13	14	17	18	20	21	25	26	28	29	32	33
	7	11	12	14	15	18	19	21	22	26	27	29	30	33	34
	8	15	16	18	19	22	23	25	26	30	31	33	34	37	38
	9	16	17	19	20	23	24	26	27	31	32	34	35	38	39
	10	18	19	21	22	25	26	28	29	33	34	36	37	40	41
	11	19	20	22	23	26	27	29	30	34	35	37	38	41	42
	12	22	23	25	26	29	30	32	33	37	38	40	41	44	45
	13	23	24	26	26	30	31	33	34	38	39	41	42	45	46

Table 4.2: $M[i,j] = \nu_2(2^{i+j} i! j!) = \nu_2((2i)!(2j)!)$

In order to get the 2-sequence of $\mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$, our goal is to find a formula for $\gamma(n)$, where for a given n, $\gamma(n)$ counts the number of times n appears in M. We look into the properties of M to construct $\gamma(n)$.

Definition 72. *Given the matrix M, with $i, j \geq 1$. The n-th diagonal D_n of M is*

$$D_n = \{M[i,j] \mid i + j = n\}.$$

Proposition 73. *If $i + j = 2^{k-1} - 1$, then $M[i,j] = 2^k - k - 1$.*

Proof. Since we are looking at elements on the diagonal D_n we have that these elements $M[i,j]$ satisfy $i + j = 2^{k-1} - 1$. We want to show that

$$M[i,j] = i + j + \nu_2(i!) + \nu_2(j!) = 2^k - k - 1. \tag{4.1}$$

We proceed by induction on k. If $k = 2$, $n = 1$, and from calculations we get $D_2 = \{(1,1)\}$, with $1 = 2^2 - 2 - 1$.

Suppose equation 4.1 holds for k, that is, for $i+j=2^{k-1}-1$. Then we have that $i+j+\nu_2(i!)+\nu_2(j!)=2^k-k-1$. That is,

$$\begin{aligned}\nu_2(i!)+\nu_2(j!)&=2^k-k-1-2^{k-1}+1\\&=2^{k-1}(2-1)-k\\&=2^{k-1}-k.\end{aligned}$$

Hence for $i+j=2^k-1$ we are reduced to showing that $\nu_2(i!)+\nu_2(j!)=2^k-(k+1)$. Without loss of generality suppose $i>2^{k-1}$ and $j\leq 2^{k-1}$. Let $i=2^{k-1}+i'$. Then by Lemma 71,

$$\nu_2(i!)+\nu_2(j!)=2^{k-1}-1+\nu_2(i'!)+\nu_2(j!).$$

Since $i'+j=(i-2^{k-1})+j=2^k-1-2^{k-1}=2^{k-1}$, we get by induction hypothesis that $\nu_2(i'!)+\nu_2(j!)=2^k-k-1$ and

$$\nu_2(i!)+\nu_2(j!)=2^{k-1}-1+2^k-k=2^k-(k+1).$$

□

Corollary 74. *When $n=2^{k-1}-1$, the diagonals D_n act as bounds for the values in M, in the sense that if $i+j>n$ then $M[i,j]>2^k-k-1$, and if $i+j<n$ then $M[i,j]<2^k-k-1$.*

Proof. Above D_n we have that $i+j<n=2^{k-1}-1$. Thus

$$\begin{aligned}M[i,j]=i+j+\nu_2(i!)+\nu_2(j!)&<n+1+\nu_2(i!)+\nu_2(j!)\\&=2^{k-1}-1+\nu_2(i!)+\nu_2(j!)\\&\leq 2^{k-1}-1+2^{k-1}-k\\&=2^k-k-1,\end{aligned}$$

where the last inequality comes from the proof of Proposition 73. Below D_n we have that $i + j > n + 1 = 2^{k-1} - 1$, thus

$$\begin{aligned} M[i,j] = i + j + \nu_2(i!) + \nu_2(j!) &> n + 1 + \nu_2(i!) + \nu_2(j!) \\ &= 2^{k-1} - 1 + \nu_2(i!) + \nu_2(j!) \\ &\geq 2^{k-1} - 1 + 2^{k-1} - k \\ &= 2^k - k - 1, \end{aligned}$$

where the last inequality comes from the proof of Proposition 73. □

If we look at the section of M represented below:

		degree of x							
		0	1	2	3	4	5	6	7
degree of y	0	0	1	3	4	7	8	10	11
	1	1	2	4	5	8	9	11	12
	2	3	4	6	7	10	11	13	14
	3	4	5	7	8	11	12	14	15
	4	7	8	10	11	14	15	17	18
	5	8	9	11	12	15	16	18	19
	6	10	11	13	14	17	18	20	21
	7	11	12	14	15	18	19	21	22

Table 4.3: Symmetry

We notice that if you take a value in red and reflect it about D_7, the diagonal made of $11 = 2^4 - 4 - 1$, then adding the reflected value in blue will always yield 22. This type of pattern will always occur and is demonstrated in Corollary 76.

Definition 75. *We define the triangle $T_{(a_1,b_1,a_2,b_2)}$ in M, where $b_1 - a_1 = b_2 - a_2$, to be the following set:*

$$T_{(a_1,b_1,a_2,b_2)} = \{(i,j) \mid a_1 \leq i \leq b_1,\ a_2 \leq j \leq b_2,\ \textit{and } i + j \leq b_1 + a_2\}.$$

For example, the following section of M is $T_{(0,7,0,7)}$, the green section is $T_{(0,3,0,3)}$, the red section is $T_{(4,7,0,3)}$, and the blue section is $T_{(0,3,4,7)}$:

		degree of x							
		0	1	2	3	4	5	6	7
degree of y	0	0	1	3	4	7	8	10	11
	1	1	2	4	5	8	9	11	
	2	3	4	6	7	10	11		
	3	4	5	7	8	11			
	4	7	8	10	11				
	5	8	9	11					
	6	10	11						
	7	11							

Table 4.4: Triangular Regions and Translations

You can see that every value in red or blue is 7 plus the value in the same position in the green triangle. This is demonstrated in Proposition 77.

We look into counting how many basis elements of $\text{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$ have a certain 2-adic valuation in their denominator. Corollary 74 shows that for degree m, where $2^k - k - 1 \leq m < 2^{k+1} - k - 2$, it is enough to search in the region $i + j \leq 2^k - 1$, where $i + j$ will make up the total degree of a given polynomial. For example, for $m = 3$ we would consider the following values:

	0	1	2	3
0	0	1	3	4
1	1	2	4	
2	3	4		
3	4			

Table 4.5: Denominators for $\text{Int}_3((1+2\mathbb{Z})^2, \mathbb{Z})$

That is for degree m, we find the diagonal that acts as an upper bound for the denominators, and count the entries $M[i, j]$ such that $i + j < 2^k$. We can count that there is one basis element with a 2^0 in its denominator, two with a 2^1, one with a 2^2, two with a 2^3 and four with a 2^4.

We can recursively use this method, in this case, when know the number of denominators for $\text{Int}_{m-1}(((1+2\mathbb{Z})^2, \mathbb{Z})$, one only needs to consider $M[i, j]$ such that

$2^{k-1} \leq i+j \leq 2^k - 1$. Doing this up to $m = 10$ gives a table where we count the number of basis elements with a certain denominator of each degree $0 \leq m \leq 10$. That is, in the table below the entries (m,n), record the number of entries $M[i,j]$ of size n for which $i+j \leq m$. In this case $i+j$ is the total degree and n is the 2-adic valuation of the denominators of the basis elements of degree m. This type of table will be very important for this project.

		n, for denominators of size 2^n																		
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Total degree m	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	1	2	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	1	2	1	2	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	1	2	1	2	4	2	1	2	0	0	0	0	0	0	0	0	0	0	0
	5	1	2	1	2	4	2	1	4	4	0	0	0	0	0	0	0	0	0	0
	6	1	2	1	2	4	2	1	4	5	2	4	0	0	0	0	0	0	0	0
	7	1	2	1	2	4	2	1	4	5	2	4	8	0	0	0	0	0	0	0
	8	1	2	1	2	4	2	1	4	5	2	4	8	4	2	1	0	0	0	0
	9	1	2	1	2	4	2	1	4	5	2	4	8	4	2	5	2	4	0	0
	10	1	2	1	2	4	2	1	4	5	2	4	8	4	2	5	2	5	4	4

Table 4.6: Number of Basis Elements in $\mathrm{Int}_m((1+2\mathbb{Z})^2, \mathbb{Z})$ Having $\nu_2 = n$

The column values eventually stabilize because of Corollary 74, since the diagonals bound the values n can take on. This matrix has its rows stabilizing to

$$(\gamma(n)) = 1, 2, 1, 2, 4, 2, 1, 4, 5, 2, 4, 8, 4, \ldots$$

This sequence stores in each entry n,the number of pairs (i,j) for which $\nu_2(2^{i+j} i! j!) = \nu_2((2i)!(2j)!) = n$. We know how to construct a table to get values for this sequence, but it would be very useful to have a formula for $\gamma(n)$. We will use the number theoretical properties of M to derive a recursive way of counting how many times a value x will appear in M.

Proposition 76. (Reflection.) *Consider D_n, for $n = 2^{k-1} - 1$. For all $M[a,b]$ and $M[c,d]$ such that $a+d = n = b+c$, we have*

$$M[a,b] + M[c,d] = 2(2^k - k - 1).$$

Proof.

$$\begin{aligned} M[a,b]+M[c,d] &= a+b+\nu_2(a!)+\nu_2(b!)+c+d+\nu_2(c!)+\nu_2(d!) \\ &= a+d+\nu_2(a!)+\nu_2(c!)+b+c+\nu_2(b!)+\nu_2(d!) \\ &= (2^k-k-1)+(2^k-k-1) \quad \text{by Proposition 73} \\ &= 2(2^k-k-1). \end{aligned}$$

□

Proposition 77. (Translation.) *Let $n = 2^{k-1}$. If $(i,j) \in T_{(0,n-1,0,n-1)}$, then*

$$M[i,j]+(2^k-1) = M[i+n,j] = M[i,j+n].$$

Proof. For $0 \le i \le n-1$ and $0 \le j \le n-1$, we have by Lemma 70

$$\begin{aligned} M[i,j] &= \nu_2(2^i i! 2^j j!) = \nu_2((2i)!(2j)!) \\ M[i+n,j] &= \nu_2(2^{i+n}(i+n)! 2^j j!) = \nu_2((2(i+n))!(2j)!) \\ M[i,j+n] &= \nu_2(2^i i! 2^{j+n}(j+n)!) = \nu_2((2i)!(2(j+n))!). \end{aligned}$$

Furthermore,

$$\begin{aligned} M[i+n,j] &= \nu_2((2(i+n))!)+\nu_2((2j)!) \\ &= \nu_2((2(i+2^{k-1}))!)+\nu_2((2j)!) \\ &= \nu_2((2i+2^k)!)+\nu_2((2j)!) \\ &= (2^k-1)+\nu_2((2i)!)+\nu_2((2j)!) \quad \text{by Lemma 71} \\ &= (2^k-1)+M[i,j]. \end{aligned}$$

A similar argument can be used to show that $M[i,j+n] = 2^k-1+M[i,j]$ and to prove our claim. □

Given a value n, we will calculate $\gamma(n)$ using the following:

(1) If $n = 2^k-k-1$, for some k, then n is on the diagonal $D_{2^{k-1}-1}$, and appears 2^{k-1} times in M.

(2) If n is a value that appears between the diagonals $D_{2^{k-1}-1}$ and D_{2^k-1}, thus $2^{k-1}-k < n < 2^k-k-1$, then the number of times n appears in M depends on the values of the smaller triangle below $D_{2^{k-1}-1}$ that is values in $T_{(0,2^{k-1}-1,0,2^{k-1}-1)}$.

   (i) By symmetry (Corollary 76), for each $m \in T_{(0,2^k-1,0,2^k-1)}$ such that $n+m = 2(2^k-k-1)$, there will be a corresponding n between $D_{2^{k-1}}$ and D_{2^k}.

   (ii) By translation (Corollary 77), for each $m \in T_{(0,2^{k-1}-1,0,2^{k-1}-1)}$ such that $m + 2^{k-1} - 1 = n$, there will be two corresponding n; one from the horizontal translation of $T_{(0,2^{k-1}-1,0,2^{k-1}-1)}$, and the other from the vertical translation.

Proposition 78. *We have the following recursive formula for* $\gamma(n)$*:* $\gamma(0) = 1$*,* $\gamma(1) = 2$*,* $\gamma(2) = 1$*,* $\gamma(3) = 2$*,* $\gamma(4) = 4$ *and*

$$\gamma(n) = \begin{cases} 2^{k-1} & \textit{if } n = 2^k-k-1 \\ \gamma(2(2^k-k-1)-n) & \textit{if } \ 2^k-k-1 < n < 2^k-1 \\ \gamma(2(2^k-k-1)-n) + 2\gamma(n-2^k+1) & \textit{if } \ 2^k-1 \leq n \leq 2(2^k-k-1) \\ 2\gamma(n-2^k+1) & \textit{if } \ 2(2^k-k-1) < n < 2^{k+1}-k-2 \end{cases}$$

where k *is the largest integer such that* $2^k-k-1 \leq n$.

Proof. We have $\gamma(0) = 1$, $\gamma(1) = 2$, $\gamma(2) = 1$ and $\gamma(3) = 2$ by counting in M, which is partially represented by Table 4.2.

Let k be such that $2^k-k-1 \leq n < 2^{k+1}-k-2$. We proceed by induction on k. Our base case will be $k = 3$ and we will calculate $\gamma(n)$ for

$$2^3-3-1 \leq n < 2^4-3-2$$
$$4 \leq n < 11$$

Given the formula in the statement we look at four sections of this interval, and show that the formula works for $k = 3$

Interval	$\gamma(n)$
$n = 2^k - k - 1 = 4$	$\gamma(4) = 2^{3-1} = 4$
$2^k - k - 1 < n < 2^k - 1$ $4 < n < 7$	$\gamma(5) = \gamma(2(2^3 - 3 - 1) - 5) = \gamma(8 - 5) = \gamma(3) = 2$ $\gamma(6) = \gamma(8 - 6) = \gamma(2) = 1$
$2^k - 1 \leq n \leq 2(2^k - k - 1)$ $7 \leq n \leq 8$	$\gamma(7) = \gamma(8 - 7) + 2\gamma(7 - 8 + 1) = \gamma(1) + 2\gamma(0) = 2 + 2$ $\gamma(8) = \gamma(8 - 8) + 2\gamma(8 - 8 + 1) = \gamma(0) + 2\gamma(1) = 5$
$2(2^k - k - 1) < n < 2^{k+1} - k - 2$ $8 < n < 11$	$\gamma(9) = 2\gamma(9 - 8 + 1) = 2\gamma(2) = 2$ $\gamma(10) = 2\gamma(10 - 8 + 1) = 2\gamma(3) = 4$

Table 4.7: $\gamma(n)$ for $4 \leq n < 11$

Now suppose the result holds for all $n < 2^k - k - 1$. To prove the formula is correct, we also need to show that the bounds of the formula are correct. Given the values n between the diagonals $D_{2^{k-1}-1}$ and D_{2^k-1} in M, that is, for

$$2^k - k - 1 \leq n \leq 2^{k+1} - k - 2,$$

we split these into three disjoint regions:

I This region in M will be $T_{(2^k,2(2^k-1)+1,0,2^k-1)}$, which in Table 4.4 corresponds to the region in red.

II This region in M will be $T_{(0,2^k-1,2^k,2(2^k-1)+1)}$, which in Table 4.4 corresponds to the region in blue.

III This region in M will be $T_{(0,2(2^k-1)+1,0,2(2^k-1)+1)} \backslash \{I, II\}$, which in Table 4.4 corresponds to the region in black.

Note that if $n = 2^k - k - 1$, then n is on a diagonal and $\gamma(n) = 2^{k-1}$ by Proposition 73. We then divide the interval $2^k - k - 1 \leq n < 2^{k+1} - k - 2$ into three subintervals where we want to show the following.

The values in the interval $2^k - k - 1 < n < 2^k - 1$ will be in region II only.

The values in the interval $2^k - 1 \leq n \leq 2(2^k - k - 1)$ will be in regions I, II and III.

The values in the interval $2(2^k - k - 1) < n < 2^{k+1} - k - 2$ will be in regions I and III only.

We proceed to prove this by showing that

(i) The elements in the interval $I_1\colon 2^k - k - 1 < n \leq 2(2^k - k - 1)$ are the only ones having the reflection property.

(ii) The elements in the interval $I_2\colon 2^{k-1} \leq n < 2^{k+1} - k - 2$ are the only ones having the translation property.

(i) For $n \in I_1$, we want to show that there exist $0 \leq \ell < 2^k - k - 1$ such that $n + \ell = 2(2^k - k - 1)$ as in Proposition 76, which gives that

$$\ell = (2^{k+1} - 2k - 2) - n.$$

For ℓ to be in the allowed interval we need $n \leq 2^{k+1} - 2k - 2$, which gives $\ell = 0$. Since $2^k - k - 1 < n$, we have that $\ell < 2^k - k - 1$, which is positive for $k \geq 3$. This completes the proof of (i).

(ii) For $n \in I_2$, we want to show that n has the translation property as in Proposition 77. That is, we want to show that $n - (2^k - 1)$ produces a value in the triangle $T_{(0,2^{k-1},0,2^{k-1})}$. In this case we need

$$0 \leq n - (2^k - 1) < 2^k - k - 1,$$
$$2^k - 1 \leq n < 2^{k+1} - k - 2,$$

which is exactly I_2, and it proves (ii).

Combining these bounds we get that, on the interval $2^k - k - 1 < n < 2^k - 1$, the values only have the reflection property and by induction $\gamma(n) = \gamma(2(2^k - k - 1) - n)$.

On the interval $2^k - 1 \leq n \leq 2(2^k - k - 1)$, the values have both the reflection and translation property thus, by induction $\gamma(n) = \gamma(2(2^{k+1} - k - 2) - n) + 2\gamma(n - 2^k + 1)$.

On the interval $2(2^k - k - 1) < n < 2^{k+1} - k - 2$, the values only have the translation property and by induction $\gamma(n) = 2\gamma(n - 2^k + 1))$.

□

Note: When writing n as $n = \sum n_i 2^i$, k described above is either the largest i in this expansion, or it is $i + 1$, i.e. $k = \lfloor \log_2 n \rfloor$ or $k = \lfloor \log_2 n \rfloor + 1$.

Implementing the recursive formula from Proposition 78 allows us to quickly calculate $\gamma(n)$. The first values in the sequence are:

	$\gamma(n)$									
n and column index	0	1	2	3	4	5	6	7	8	9
$0 \leq n < 10$	1	2	1	2	4	2	1	4	5	2
$10 \leq n < 20$	4	8	4	2	5	6	5	4	8	10
$20 \leq n < 30$	5	4	9	10	4	8	16	8	4	10
$30 \leq n < 40$	9	6	9	12	12	12	9	8	13	12
$40 \leq n < 50$	8	16	20	10	9	14	13	12	12	18
$50 \leq n < 60$	21	12	9	18	20	8	16	32	16	8
$60 \leq n < 70$	20	18	9	14	25	20	16	20	17	16
$70 \leq n < 80$	17	20	24	24	24	20	17	18	21	22
$80 \leq n < 90$	20	28	29	16	17	28	24	16	32	40
$90 \leq n < 100$	20	18	29	22	17	28	32	28	29	24

Table 4.8: $\gamma(n)$ for $0 \leq n < 100$

Note the sequence $(\gamma(n))$ cannot be found on the On-Line Encyclopedia of Integer Sequences [OEIS], it will be added to the website and is currently waiting for the approval of an Editor-in-Chief.

4.1 Why the Seven?

If we multiply $\gamma(n)$ by 7 we obtain the following sequence

$$7, 14, 7, 14, 28, 14, 7, 28, 35, 14, 28, 56, 28, \ldots$$

which is a 2-sequence that will appear in Matrix 5.4 in Section 5.2, and will be of major interest to us, since it is related to the 2-sequence of homogeneous 3-variable IVPs.

The columns of Table 5.4 stabilize to 7 times the 2-sequence of $\mathrm{Int}_m((1+2\mathbb{Z})^2,\mathbb{Z})$, showing a connection between $\mathrm{Int}_m((1+2\mathbb{Z})^2,\mathbb{Z})$ and $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$.

The table M is for $\mathrm{Int}_m((1+2\mathbb{Z})^2,\mathbb{Z}) \simeq \mathrm{Int}^m((1+2\mathbb{Z})^3,\mathbb{Z})$, hence evaluated at triples that have only odd values, i.e., that are congruent to $(1,1,1) \pmod 2$. There are six other triples of interest, namely

$$(1,0,0),\ (0,1,0),\ (0,0,1), (1,1,0),\ (1,0,1),\ (0,1,1),$$

since for a homogeneous polynomial of degree m, we can always divide by 2^m when evaluating at $(0,0,0) \pmod 2$. The seven basis elements arising from one element in $\mathrm{Int}^m((1+2\mathbb{Z})^3,\mathbb{Z})$ possibly comes from deciding from which triple the IVP is built, and the inconsistent “diagonal” might be explained by the lack of polynomials with a certain denominator at a given triple. We will generalize the case of evaluating at odd variables in Chapter 6.

Chapter 5

Computational Data and the Smith Normal Form

In this chapter we will develop computational methods to use our knowledge of 3-variable IVPs of degree less than or equal to m, to obtain bases for the homogenous case. We will use a tool from linear algebra, namely the Smith normal form of a matrix, which will be a matrix that satisfies a divisibility criterion. This will allow us, for a given degree m, to count the number of elements with a certain denominator and to produce basis elements. We end the chapter by discussing these results.

5.1 Algebraic Background: The Smith Normal Form

For different parts of this project we will use the Smith normal form of a matrix. In this section we recall the basic definitions and theorems, first over $\mathbb{Z}$, then over general rings, to ensure that the Smith normal form will exist over the rings we are working with. For the following let R be a commutative ring.

Definition 79. [Bro93, Def. 15.6] *Two $m \times n$ matrices A and B over R are said to be equivalent, which we will denote $A \approx B$, if B can be obtained by performing invertible elementary row and column operations, invertible with respect to the ring R, on A.*

Definition 80. [Bro93, Def. 15.7] *A commutative ring R is called an elementary divisor ring if for all $m, n \geq 1$ and for every $m \times n$ matrix A over R, there exists a diagonal matrix $diag(d_1, \dots, d_r)$ of size $m \times n$ over R such that*

(a) $A \approx diag(d_1, \dots, d_r)$, and

(b) $d_i | d_{i+1}$ for all $i = 1, \dots, r-1$. (Here $r = \min\{m, n\}$.)

Definition 81. [Nor12, Def. 1.6] *Let D be an $m \times n$ matrix over $\mathbb{Z}$ such that*

(a) *the (i, j)-entries in D are zero for $i \neq j$, that is, D is a diagonal matrix,*

(b) *each (i, i)-entry d_i in D is non-negative, and*

(c) *for each i with $1 \leq i < \min\{m, n\}$ there is an integer q_i with $d_{i+1} = q_i d_i$, that is, $d_i | d_{i+1}$.*

Then D is said to be in Smith normal form and we write $D = diag(d_1, d_2, \ldots, d_{\min\{m,n\}})$.

In general the Smith normal form for an $m \times n$ matrix looks like

$$\begin{bmatrix} d_1 & & & & & & & & \\ & d_2 & & & & & & & \\ & & \ddots & & & & & & \\ & & & d_r & & & & & \\ & & & & 0 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 0 & & \end{bmatrix}$$

Notice that d_1 is the gcd of the st entries in D. Also $d_1 d_2$ is the gcd of the 2-minors of D (the determinants of the 2×2 sub-matrices of D).

Theorem 82. [Nor12, Th. 1.11] (The existence of the Smith normal form over $\mathbb{Z}$) *Every $m \times n$ matrix A over $\mathbb{Z}$ can be reduced to an $s \times t$ matrix D in Smith normal form using invertible elementary row and column operations over $\mathbb{Z}$. For any matrix A of size $m \times n$ over $\mathbb{Z}$ we can obtain $A = UDV$, where U is of size $m \times m$ and V is of size $n \times n$. Moreover, since U, V are obtained from elementary row operations, they are unimodular.*

The previous theorem guarantees a Smith normal form for matrices over $\mathbb{Z}$. We need this for other rings, also, since we will be interested, for example, in $\mathbb{Z}/(p)$ for this project.

Definition 83. [Bro93, Def. 15.1] *A 1×2 matrix $\begin{bmatrix} a & b \end{bmatrix} \in M_{1\times 2}(R)$ admits a diagonal reduction if $\begin{bmatrix} a & b \end{bmatrix} \approx \begin{bmatrix} d & 0 \end{bmatrix}$ over R, for some $d \in R$.*

Definition 84. [Bro93, 2, page 181] *A ring R over which every 1×2 matrix admits a diagonal reduction is called a Hermite ring.*

Calculations later in this chapter and in further chapters will be over $\mathbb{Z}/(2^k)$, for $k \geq 1$. Hence it is useful to have that any row matrix $[a\ b]$, where $a \neq 0, b \in \mathbb{Z}/(2^k)$, we can always multiply by the following invertible matrix

$$\begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & -a \end{bmatrix} = \begin{bmatrix} a & 0 \end{bmatrix}$$

and if $a = 0$ one can multiply by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Thus $\mathbb{Z}/(2^k)$ is a Hermite ring.

Theorem 85. [Bro93, Th. 15.8] *Any Noetherian, Hermite ring is an elementary divisor ring.*

Theorem 86. [Bro93, Th. 15.9] *Any principal ideal ring (PIR) is an elementary divisor ring.*

Definition 87. [Bro93, Def. 15.10] *Let A be an $m \times n$ matrix over R. A matrix in Smith normal form $D = diag(d_1, \ldots, d_r)$ of size $m \times n$ over R is called a Smith normal form of A if $A \approx D$ and $d_1 | d_2 | \cdots | d_r$ in R.*

Recall that two elements $a,\ b$ of a PIR are said to be associates if $a = ub$ and u is a unit in the PIR, in which case we write $a \sim b$.

Theorem 88. [Bro93, Th. 15.24] (The existence of the Smith normal form.) *Let R be a PIR. Then R is an elementary divisor ring. Furthermore, if $D_1 = diag(d_1, \ldots, d_r)$ and $D_2 = diag(s_1, \ldots, s_r)$ are two Smith normal forms of A, then $d_i \sim s_i$ for all $i = 1, \ldots, r$.*

Since the Smith normal form can be obtained through elementary row operations, we can write for an $m \times n$ matrix A, matrix $S = UAV$ where S is also of size $m \times n$, U is of size $m \times m$ and V is of size $n \times n$. Note that both U and V are invertible over R.

The results above hold for PIRs hence for $\mathbb{Z}/(2^k)$, which will be needed for Proposition 126 in Chapter 7. Theorem 89 below is for the stricter case of PIDs, where we cannot have zero divisors but is sufficient to prove Proposition 90.

Theorem 89. [DF04, 12.1 Th. 4] *Let R be a principal ideal domain, let M be a free R-module of finite rank n and let N be a submodule of M. Then*

(1) N is free of rank m, $m \leq n$ and

(2) there exists a basis $y_1, y_2, \ldots, y_n$ of M so that $a_1y_1, a_2y_2, \ldots, a_my_m$ is a basis of N where $a_1, a_2, \ldots, a_m$ are non-zero elements of R with divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

Calculating the Smith normal form, will allow us to find the a_i's such that $a_1 \mid a_2 \mid \cdots \mid a_m$, in the previous theorem. Note that since $m \leq n$, $m = r$ in the earlier definitions and theorems.

Proposition 90. *For M and N as above, if $\{z_i\}$ is a basis of M, $\{x_i\}$ is a basis of N, A is the matrix expressing $\{x_i\}$ in terms of $\{z_i\}$, and $S = UAV$ is the Smith normal form of A, then $UA[z_1, \ldots, z_n]^T$ is the basis $\{y_i\}$ as in Theorem 89, and the diagonal elements of S are the a_i's in Theorem 89.*

Proof. Suppose we know that M has for basis $\{z_1, z_2, \ldots, z_n\}$ and N has for basis $\{x_1, x_2, \ldots, x_m\}$. Since N is a submodule of M, each x_j can be written as an R-linear combination of the z_i's. Let A be an $m \times n$ matrix that stores in each row j the coefficients of the z_i's.

Taking the Smith normal form of A yields $S = UAV$, where S is diagonal such that $d_i \mid d_{i+1}$ for $d_i = S[i, i]$. Since U and V are unimodular matrices, S is unique.

More precisely, we get the following commutative diagram:

$$\begin{tikzcd}
N \arrow[r, "A"] & M \\
\{x_i\} \arrow[d, shift left, "V^{-1}"] & \{z_i\} \arrow[d, "U"] \\
N \arrow[u, shift left, "V"] \arrow[r, "S"] & M \\
\{x_i'\} & \{y_i\}
\end{tikzcd}$$

in which the maps represent matrix multiplication. We have that we can write the basis elements of N as linear combinations of the ones of M, by doing the matrix multiplication

$$A \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} \sum a_{1j}z_j \\ \sum a_{2j}z_j \\ \vdots \\ \sum a_{mj}z_j \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}.$$

Now if multiply by U as well:

$$UA \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} \sum u_{1j}z_j \\ \sum u_{2j}z_j \\ \vdots \\ \sum u_{mj}z_j \end{bmatrix}$$

we additionally get that the coefficients u_{ij} respect the same divisibility properties as the diagonal of S. Hence we get a representation of the basis elements of N using the ones of M respecting the desired divisibility criteria from Theorem 89.

Since $UA = SV^{-1}$, the d_i's are the invariant factors.

□

5.2 Computational Results for $p = 2$

We will look at the case $n = 3$ here and present some computational results. Since the case $n = 2$ was described in [JP11] we often use it to test our methods. We will make great use of the fact that a basis for $\mathrm{Int}(\mathbb{Z}^3, \mathbb{Z})$ is given by $\left\{ \binom{x}{r}\binom{y}{s}\binom{z}{t} \;\middle|\; r, s, t \geq 0 \right\}$ as seen in Corollary 39. We will also use the fact that for the $\mathbb{Z}$-module of polynomials in $\mathrm{Int}_3(\mathbb{Z}^3,\mathbb{Z})$, that is, the polynomials of degree less than or equal to 3, we get an upper bound on indices, that is $\mathrm{Int}_3(\mathbb{Z}^3,\mathbb{Z})$, is generated by $\left\{ \binom{x}{r}\binom{y}{s}\binom{z}{t} \;\middle|\; 0 \le r+s+t \le 3 \right\}$.

We have that the $\mathbb{Z}$-module $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$ of polynomials in $\mathrm{Int}(\mathbb{Z}^3,\mathbb{Z})$ that are homogeneous of degree m is a proper submodule, hence is a free $\mathbb{Z}$-module.

Definition 91. *Let $\mathbb{Z}^m[x,y,z]$ denote the $\mathbb{Z}$-module of homogeneous polynomials of degree m with integer coefficients.*

$\mathbb{Z}^m[x,y,z]$ is a submodule of $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$, and we have the following inclusions:

$$\mathbb{Z}^m[x,y,z] \subseteq \mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z}) \subseteq \mathrm{Int}_m(\mathbb{Z}^3,\mathbb{Z}) \subseteq \mathrm{Int}(\mathbb{Z}^3,\mathbb{Z}).$$

We have that $\mathbb{Z}^m[x,y,z]$ has for basis the monomials $\{x^i y^j z^k \mid i+j+k=m\}$. Furthermore $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$ is a pure submodule of $\mathrm{Int}(\mathbb{Z}^3,\mathbb{Z})$, i.e. if $f \in \mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$ is such that $f = kg$ with $k \in \mathbb{Z}$, $g \in \mathrm{Int}(\mathbb{Z}^3,\mathbb{Z})$ then $g \in \mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$. Thus, the invariant factors of $\mathbb{Z}^m[x,y,z]$ in $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$ are the same as those in $\mathrm{Int}(\mathbb{Z}^3,\mathbb{Z})$.

Proposition 92. [GKP98, 6.1, page 262] *For any i the polynomial x^i can be expressed in terms of the polynomials $\binom{x}{r}_{0\le r\le i}$ by*

$$x^i = \sum_{r=0}^{i} r!S(i,r)\binom{x}{r},$$

where $S(i,r)$ are the Stirling numbers of the second kind. These are defined by

$$S(i,r) = \frac{1}{r!}\sum_{j=0}^{r}(-1)^{r-j}\binom{k}{j}j^n.$$

By writing each of x, y and z using the above proposition and multiplying them, we obtain:

Corollary 93. *The monomials $x^i y^j z^k$ have the expression*

$$x^i y^j z^k = \sum r!s!t!S(i,r)S(j,s)S(k,t)\binom{x}{r}\binom{y}{s}\binom{z}{t},$$

where the sum ranges over all (r, s, t) such that $r + s + t \leq m = i + j + k$.

Here is the information about bases we have so far:

$\mathbb{Z}$-modules	Basis
$\mathbb{Z}^m[x, y, z]$	$\{x^i y^j z^k \mid i + j + k = m\}$
$\text{Int}^m(\mathbb{Z}^3, \mathbb{Z})$	???
$\text{Int}_m(\mathbb{Z}^3, \mathbb{Z})$	$\left\{\binom{x}{r}\binom{y}{s}\binom{z}{t} \mid r + s + t \leq m\right\}$

Table 5.1: What We Know About Bases

We are looking for bases for the middle row. For a given m we want to find $d \in \mathbb{Z}$ and $\{a_{ijk}\} \subseteq \mathbb{Z}$ such that for $f \in \text{Int}^m(\mathbb{Z}^3, \mathbb{Z})$, we have

$$f = \sum a_{ijk} x^i y^j z^k$$

and $\frac{f}{d} \in \text{Int}(\mathbb{Z}^3, \mathbb{Z})$.

By Theorem 89, we can find a basis for $\text{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ written as scalars respecting a divisibility condition times a basis for $\text{Int}_m(\mathbb{Z}^3, \mathbb{Z})$. With the previous formula using Stirling numbers we can represent the basis elements of $\mathbb{Z}^m[x, y, z]$ using the basis elements of $\text{Int}_m(\mathbb{Z}^3, \mathbb{Z})$, which allows us to go from one basis to another.

This gives a linear system expressing the basis elements of $\mathbb{Z}^m[x, y, z]$ in terms of those of $\text{Int}^m(\mathbb{Z}^3, \mathbb{Z})$. To do so we will express $x^i y^j z^k$ as a vector of coefficients of $\binom{x}{r}\binom{y}{s}\binom{z}{t}$. That is for a given m, we get a matrix of coefficients for each row represents a triple such that $i + j + k = m$. Prior to building these matrix of coefficients we define the following ordering.

Definition 94. *Given all monomials $x^i y^j z^k$ such that $i + j + k = m$, the decreasing lexicographical ordering of these according to the triples (i, j, k) is obtained by first ordering them by decreasing order of k. Then, for a fixed value of k, the triples* *are ordered by decreasing order of j. Lastly, for a fixed j, the triples are ordered by decreasing order of i.*

For example, in the case $m = 3$, the monomials in decreasing lexicographical order are

z^3,	yz^2,	xz^2,	y^2z,	xyz,	x^2z,	y^3,	xy^2,	x^2y,	x^3
1	2	3	4	5	6	7	8	9	10
(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300) .

Using decreasing lexicographical order, we can order the triples (r, s, t), such that $r + s + t \leq m$ in the following way, first order the triples in increasing order of m' such that $r + s + t = m'$. Then, for a fixed m' order the triples in decreasing lexicographical order. For $m = 3$ the ordered triples (r, s, t) are

(000)	(001)	(010)	(100)	(002)	(011)	(101)	(020)	(110)	(200)
(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300) .

For $1 \leq m \leq 22$ and $p = 2$, in the case of three variables we have a MAPLE program which returns information about the denominators, d, of the basis elements of $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$.

First we create an $\frac{(m+1)(m+2)}{2} \times \frac{(m+1)(m+2)(m+3)}{6}$ matrix, where $\frac{(m+1)(m+2)}{2}$ is the number of monomials such that $i+j+k = m$, and is therefore the rank of $\mathbb{Z}^m[x, y, z]$. Also $\frac{(m+1)(m+2)(m+3)}{6}$ is the number of monomials such that $r + s + t \leq m$, hence the rank of $\mathrm{Int}_m(\mathbb{Z}^3, \mathbb{Z})$. We order both bases as described above. Our matrix M has for entries

$$M[a, b] = i!j!k!S(i, r)S(j, s)S(k, t),$$

which are the coefficients of the monomials $x^i y^j z^k$, in the representation above, (Corollary 93), for all $(r, s, t) \leq (i, j, k)$, ordered as described above, where $S(\ell, u)$ are the Stirling numbers of the second kind. Each row of M represents a triple (i, j, k) such that $i + j + k = m$, and these are in decreasing lexicographical order as in Definition 94. Each column of M represents a triple (r, s, t) such that $r + s + t \leq m$, where the columns are ordered as described above.

Note that indices (a,b) range through $1 \leq a \leq \frac{(m+1)(m+2)}{2}$ and $1 \leq b \leq \frac{(m+1)(m+2)(m+3)}{6}$, but there is no direct formula between a and (i,j,k), nor b and (r,s,t). One must use the above ordering, and example of such can be found after Theorem 95.

The matrix M allows one to write a polynomial $f \in \mathbb{Z}^m[x,y,z]$ in terms of the basis $\left\{\binom{x}{r}\binom{y}{s}\binom{z}{t}\right\}$, where we want d to divide everything in that vector in order to obtain a homogeneous IVP.

Theorem 95. *For a given degree m, let M be the $\frac{(m+1)(m+2)}{2} \times \frac{(m+1)(m+2)(m+3)}{6}$ matrix expressing the monomials $x^iy^jz^k$, for $i+j+k=m$ in terms of the multivariable binomial polynomials. Let $S = UMV$ the Smith normal form of M with diagonal elements $s_i = S[i,i]$. If B the vector of monomials of $\mathbb{Z}^m[x,y,z]$ in decreasing lexicographical order and $\{u_i\}$ is the set obtained from UB, then the set $\left\{\frac{1}{s_i}u_i\right\}$ is a basis of $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$.*

Proof. The Smith normal form of M will be of the form $S = UMV$, where S is diagonal and U, V have determinant 1 and are therefore invertible over $\mathbb{Z}$. We know we can calculate the Smith normal form of M by Theorem 88 and given the divisibility condition that the Smith normal form respects in Definition 81, we can use S, U and V to obtain a basis as described in Theorem 89 and Proposition 90.

All three matrices S, U and V have integer coefficients. We use the notation $S = [s_{i,i}]$ to denote the diagonal elements. We have $U^{-1}S = MV$, where the elements of the i-th column of $U^{-1}S$ are divisible by $s_{i,i}$. We use $U^{-1}S = MV$ to go from one basis to another as illustrated in the following commutative square:

$$\begin{tikzcd}
\mathbb{Z}^m[x,y,z] \arrow[r, "M"] & \mathrm{Int}_m(\mathbb{Z}^3) \arrow[d, "U"] \\
\mathbb{Z}^m[x,y,z] \arrow[u, "V"] \arrow[r, "S"] & \mathrm{Int}_m(\mathbb{Z}^3)
\end{tikzcd}$$

and V^{-1}, U map the given bases for $\mathbb{Z}^m[x,y,z]$, and $\mathrm{Int}_m(\mathbb{Z}^3)$ to bases with respect to which the linear transformation represented by M is diagonal. If the image of the basis for $\mathbb{Z}^m[x, y, z]$ under the linear transformation represented by V^{-1} is $\{f_i\}$, then $\frac{f_i}{s_{i,i}}$ is a homogeneous element of $\text{Int}_m(\mathbb{Z}^3)$ and the polynomials $\left\{\frac{f_i}{s_{i,i}}\right\}$ form a basis for $\text{Int}^m(\mathbb{Z}^3)$, with $1 \leq i \leq \frac{(m+1)(m+2)}{2}$.

By taking B a vector of monomials that form a basis of $\mathbb{Z}^m[x, y, z]$ in lexicographical order, the product UB written as the set $\{u_i\}$, gives that $\left\{\frac{1}{s_i}u_i\right\}$ is a basis for $\text{Int}^m(\mathbb{Z}^3, \mathbb{Z})$. □

Before illustrating this method, we look into data from the two-variable case, in order to compare it to the three variable case. Here is a table returning information about the denominators of the basis elements of homogeneous IVPs in 2-variables:

		k, for Denominators of size 2^k															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Degree m	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	5	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	6	3	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0
	7	3	3	0	2	0	0	0	0	0	0	0	0	0	0	0	0
	8	3	3	0	3	0	0	0	0	0	0	0	0	0	0	0	0
	9	3	3	0	3	1	0	0	0	0	0	0	0	0	0	0	0
	10	3	3	0	3	2	0	0	0	0	0	0	0	0	0	0	0
	11	3	3	0	3	3	0	0	0	0	0	0	0	0	0	0	0
	12	3	3	0	3	3	0	0	1	0	0	0	0	0	0	0	0
	13	3	3	0	3	3	0	0	2	0	0	0	0	0	0	0	0
	14	3	3	0	3	3	0	0	3	0	0	0	0	0	0	0	0
	15	3	3	0	3	3	0	0	3	1	0	0	0	0	0	0	0
	16	3	3	0	3	3	0	0	3	2	0	0	0	0	0	0	0
	17	3	3	0	3	3	0	0	3	3	0	0	0	0	0	0	0
	18	3	3	0	3	3	0	0	3	3	0	1	0	0	0	0	0
	19	3	3	0	3	3	0	0	3	3	0	2	0	0	0	0	0
	20	3	3	0	3	3	0	0	3	3	0	3	0	0	0	0	0
	21	3	3	0	3	3	0	0	3	3	0	3	1	0	0	0	0
	22	3	3	0	3	3	0	0	3	3	0	3	2	0	0	0	0

Table 5.2: Number of Denominators for $\mathrm{Int}^m(\mathbb{Z}^2, \mathbb{Z})$

We illustrate our method with the example $m = 3$. First we display for each entry in M^T, the triples (i, j, k) and (r, s, t) that are being represented.

			Triples (i,j,k) corresponding to a certain a									
			1	2	3	4	5	6	7	8	9	10
Triples (r,s,t) corresponding to a certain b	1	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(000)	(000)	(000)	(000)	(000)	(000)	(000)	(000)	(000)	(000)
	2	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(001)	(001)	(001)	(001)	(001)	(001)	(001)	(001)	(001)	(001)
	3	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(010)	(010)	(010)	(010)	(010)	(010)	(010)	(010)	(010)	(010)
	4	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(100)	(100)	(100)	(100)	(100)	(100)	(100)	(100)	(100)	(100)
	5	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(002)	(002)	(002)	(002)	(002)	(002)	(002)	(002)	(002)	(002)
	6	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(011)	(011)	(011)	(011)	(011)	(011)	(011)	(011)	(011)	(011)
	7	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(101)	(101)	(101)	(101)	(101)	(101)	(101)	(101)	(101)	(101)
	8	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(020)	(020)	(020)	(020)	(020)	(020)	(020)	(020)	(020)	(020)
	9	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(110)	(110)	(110)	(110)	(110)	(110)	(110)	(110)	(110)	(110)
	10	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(200)	(200)	(200)	(200)	(200)	(200)	(200)	(200)	(200)	(200)
	11	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(003)	(003)	(003)	(003)	(003)	(003)	(003)	(003)	(003)	(003)
	12	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(012)	(012)	(012)	(012)	(012)	(012)	(012)	(012)	(012)	(012)
	13	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(102)	(102)	(102)	(102)	(102)	(102)	(102)	(102)	(102)	(102)
	14	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(021)	(021)	(021)	(021)	(021)	(021)	(021)	(021)	(021)	(021)
	15	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(111)	(111)	(111)	(111)	(111)	(111)	(111)	(111)	(111)	(111)
	16	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(201)	(201)	(201)	(201)	(201)	(201)	(201)	(201)	(201)	(201)
	17	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(030)	(030)	(030)	(030)	(030)	(030)	(030)	(030)	(030)	(030)
	18	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(120)	(120)	(120)	(120)	(120)	(120)	(120)	(120)	(120)	(120)
	19	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(210)	(210)	(210)	(210)	(210)	(210)	(210)	(210)	(210)	(210)
	20	(i,j,k)	(003)	(012)	(102)	(021)	(111)	(201)	(030)	(120)	(210)	(300)
		(r,s,t)	(300)	(300)	(300)	(300)	(300)	(300)	(300)	(300)	(300)	(300)

Table 5.3: Decreasing Lexicographical Ordering when $m = 3$

The matrix of Stirling coefficients M, where the indices (i,j,k) and (r,s,t) are as in the transpose of Table 5.3, and the Smith normal form S of M are as follows:

$$M = \begin{bmatrix}
0 & 1 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6
\end{bmatrix}$$

$$S = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

By looking at the diagonal of S we see that the basis for $m = 3$ will have seven elements such that 2 is not present in the denominators and three such that 2^1 is the highest power of 2 in the denominator. Since the degree is low, we can find the basis by taking a linearly independent set that satisfies the above:

$$\left\{xyz, \frac{xy(x-y)}{2}, \frac{xz(x-z)}{2}, \frac{yz(y-z)}{2}, x^2(x-y), x^2(x-z), y^2(y-x), y^2(y-z), z^2(z-x), z^3\right\}.$$

This set was obtained by using 2-subsets of $\{x, y, z\}$ and replacing these in the 2-variable basis of homogeneous IVP, which has been described in Section 2.3.2. This method will not be of much use for bigger m, since we will not be capable of using the case 2-variables only.

Since $m = 3$, we have the following vector of monomials:

$$B = \begin{bmatrix} z^3 & yz^2 & xz^2 & y^2z & xyz & x^2z & y^3 & xy^2 & x^2y & x^3 \end{bmatrix}^T,$$

and the matrix of coefficients is

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & -2 & -1 & 0 & -1 & 1 & 0 \\ 0 & -1 & 3 & 1 & -4 & -3 & 0 & -1 & 1 & 0 \end{bmatrix}.$$

The product $U \cdot B$ will produce polynomials such that $\frac{f_i}{s_{i,i}}$ are a basis for homogeneous IVPs in the case $m = 3$ we get:

$$\left\{ x^3, y^3, z^3, x^2y, x^2z, xyz, \frac{y(yz+z^2)}{2}, \frac{x(x^2+xz+yz+y)}{2}, \frac{x^2y+x^2z+xy^2+xz^2+y^2z+yz^2}{2} \right\}$$

Unfortunately, the polynomials from the bases obtained in this way tend to not factor. In the next chapters we will try to find a solution to this. Nevertheless, the matrix S gives us a way of counting the number of elements with a particular denominator in a basis. We conclude this chapter with computational results obtained this way.

We tabulate these results as follows. In the next part of the MAPLE program, we look at the elements on the diagonal of S, take their p-adic valuation, and store this in a list L. For each m, L is a list of length $\frac{(m+1)(m+2)}{2}$ which contains the p-adic norms of the denominator in the basis. Then a list of lists LL is created using all the L's we obtained at each iteration. Then a second matrix of dimension $n \times n$ is created using LL. The entries from this matrix are obtained by comparing the column index j and the values in $LL[i]$, where i is the row index. We loop through $LL[i]$ and count how many values are equal to j. Thus the (i, j)-th entry of the matrix is the number of basis element for $\mathrm{Int}^i(\mathbb{Z}^3, \mathbb{Z})$ whose denominator has 2-adic valuation j.

Doing this for the cases $1 \leq m \leq 22$, we obtain after removing all columns of zeros the following 22×15 table, where each degree m is represented by the rows, the entry $a_{m,\ell}$ represents the number of elements with denominator of 2-adic valuation ℓ, for $0 \leq \ell$:

		k, for Denominators of Size 2^k														
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Degree m	1	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	7	3	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	7	8	0	0	0	0	0	0	0	0	0	0	0	0	0
	5	7	14	0	0	0	0	0	0	0	0	0	0	0	0	0
	6	7	14	4	3	0	0	0	0	0	0	0	0	0	0	0
	7	7	14	6	9	0	0	0	0	0	0	0	0	0	0	0
	8	7	14	7	14	3	0	0	0	0	0	0	0	0	0	0
	9	7	14	7	14	13	0	0	0	0	0	0	0	0	0	0
	10	7	14	7	14	21	3	0	0	0	0	0	0	0	0	0
	11	7	14	7	14	28	8	0	0	0	0	0	0	0	0	0
	12	7	14	7	14	28	14	4	3	0	0	0	0	0	0	0
	13	7	14	7	14	28	14	6	15	0	0	0	0	0	0	0
	14	7	14	7	14	28	14	7	25	3	1	0	0	0	0	0
	15	7	14	7	14	28	14	7	28	14	3	0	0	0	0	0
	16	7	14	7	14	28	14	7	28	25	6	3	0	0	0	0
	17	7	14	7	14	28	14	7	28	34	9	9	0	0	0	0
	18	7	14	7	14	28	14	7	28	35	14	14	8	0	0	0
	19	7	14	7	14	28	14	7	28	35	14	21	21	0	0	0
	20	7	14	7	14	28	14	7	28	35	14	28	28	7	0	0
	21	7	14	7	14	28	14	7	28	35	14	28	42	6	8	1
	22	7	14	7	14	28	14	7	28	35	14	28	49	14	14	3

Table 5.4: Number of Denominators for $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ at $p = 2$

Note that $7 = 2^2 + 2^1 + 1$ seems to divide the limit of every column. This table will be extended in Table 6.1.

Given a certain column index j and row index i, if $a_{i,j}$ has the same value as the limit of its column we will refer to the corresponding basis elements as being in the stable part of the matrix. If not, the basis elements are considered unstable. We use "diagonal" to refer to the set of first non-zero elements in each column.

Up to degree 7, the 2-variable and the 3-variable case take on the same denominators in the basis elements. The value 3 on the diagonal of table 5.4 can be interpreted as coming from the 2-variable case, and we get three elements since we can pick 2-variables out of three in three different ways. For degree 8, things diverge from the

2-variable case where we previously had that the highest power of two that one can get in the denominator is 2^3 and with 3-variable one can obtain a 2^4. These basis elements with larger denominator need to be created using all 3 variables. Another interesting case to point out from this matrix is degree 14. This is the first instance where we get a 1 on the diagonal, so once again the case of 2-variables will not be helpful.

Using Table 5.2 we can calculate how many basis elements from the 3-variable case are actually obtained from the 2-variable case. This is the previous table with entries multiplied by three, which is the number subsets of 2 variables from 3 variables :

		k, for Denominators of Size 2^k															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Degree m	1	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	9	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	9	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	5	9	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	6	9	9	0	3	0	0	0	0	0	0	0	0	0	0	0	0
	7	9	9	0	6	0	0	0	0	0	0	0	0	0	0	0	0
	8	9	9	0	9	0	0	0	0	0	0	0	0	0	0	0	0
	9	9	9	0	9	3	0	0	0	0	0	0	0	0	0	0	0
	10	9	9	0	9	6	0	0	0	0	0	0	0	0	0	0	0
	11	9	9	0	9	9	0	0	0	0	0	0	0	0	0	0	0
	12	9	9	0	9	9	0	0	3	0	0	0	0	0	0	0	0
	13	9	9	0	9	9	0	0	6	0	0	0	0	0	0	0	0
	14	9	9	0	9	9	0	0	9	0	0	0	0	0	0	0	0
	15	9	9	0	9	9	0	0	9	3	0	0	0	0	0	0	0
	16	9	9	0	9	9	0	0	9	6	0	0	0	0	0	0	0
	17	9	9	0	9	9	0	0	9	9	0	0	0	0	0	0	0
	18	9	9	0	9	9	0	0	9	9	0	3	0	0	0	0	0
	19	9	9	0	9	9	0	0	9	9	0	6	0	0	0	0	0
	20	9	9	0	9	9	0	0	9	9	0	9	0	0	0	0	0
	21	9	9	0	9	9	0	0	9	9	0	9	3	0	0	0	0
	22	9	9	0	9	9	0	0	9	9	0	9	6	0	0	0	0

Table 5.5: Number of Denominators in $\text{Int}_m(\mathbb{Z}^3, \mathbb{Z})$ from $\text{Int}^m(\mathbb{Z}^2, \mathbb{Z})$

The following table lets us know how many basis elements from the 3-variable case are obtained using all three variables :

		k, for Denominators of Size 2^k															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Degree m	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	5	1	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	6	1	5	4	0	0	0	0	0	0	0	0	0	0	0	0	0
	7	1	5	6	3	0	0	0	0	0	0	0	0	0	0	0	0
	8	1	5	7	8	0	0	0	0	0	0	0	0	0	0	0	0
	9	1	5	7	5	10	0	0	0	0	0	0	0	0	0	0	0
	10	1	5	7	5	15	3	0	0	0	0	0	0	0	0	0	0
	11	1	5	7	5	19	8	0	0	0	0	0	0	0	0	0	0
	12	1	5	7	5	19	14	4	0	0	0	0	0	0	0	0	0
	13	1	5	7	5	19	14	6	9	0	0	0	0	0	0	0	0
	14	1	5	7	5	19	14	7	16	3	1	0	0	0	0	0	0
	15	1	5	7	5	19	14	7	19	11	3	0	0	0	0	0	0
	16	1	5	7	5	19	14	7	19	19	6	3	0	0	0	0	0
	17	1	5	7	5	19	14	7	19	25	9	9	0	0	0	0	0
	18	1	5	7	5	19	14	7	19	36	14	11	8	0	0	0	0
	19	1	5	7	5	19	14	7	19	36	14	15	21	0	0	0	0
	20	1	5	7	5	19	14	7	19	36	14	19	28	7	0	0	0
	21	1	5	7	5	19	14	7	19	36	14	19	39	6	8	1	0
	22	1	5	7	5	19	14	7	19	36	14	19	43	14	14	3	0

Table 5.6: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ that Use All 3 Variables

5.2.1 A Basis When $m = 4$

Using Corollary 39 we obtain the following basis elements for $\mathrm{Int}_4(\mathbb{Z}^3, \mathbb{Z})$, that are of degree at least 4 and with denominator at least 2:

$$\left\{\frac{x(x-1)(x-2)(x-3)}{8}, \frac{xy(x-1)(x-2)}{2}, \frac{xz(x-1)(x-2)}{2}, \frac{xy(x-1)(y-1)}{4},\right.$$
$$\frac{xyz(x-1)}{2}, \frac{xz(x-1)(z-1)}{4}, \frac{xy(y-1)(y-2)}{2}, \frac{xyz(y-1)}{2}, \frac{xyz(z-1)}{2},$$
$$\frac{xz(z-1)(z-2)}{2}, \frac{y(y-1)(y-2)(y-3)}{8}, \frac{yz(y-1)(y-2)}{2}, \frac{xz(y-1)(z-1)}{4},$$
$$\left.\frac{yz(z-1)(z-2)}{2}, \frac{z(z-1)(z-2)(z-3)}{8}\right\}.$$

The basis for $\mathbb{Z}^4[x, y, z]$ is:

$$\{x^4,\ x^3y,\ x^3z,\ x^2y^2,\ x^2yz,\ x^2z^2,\ xy^3,\ xy^2z,\ xyz^2,\ xz^3,\ y^4,\ y^3z,\ y^2z^2,\ xz^3,\ z^4\}.$$

By the above Table 5.4, the basis of $\mathrm{Int}^4(\mathbb{Z}^3, \mathbb{Z}_{(2)})$ has seven elements for which no power of two is in the denominator, and eight such that 2^1 is the highest power of two present in the denominator. The following is a linearly independent set respecting the previous, with only homogeneous terms of total degree 4:

$$\left\{x^2yz, \frac{x^2y(x-y)}{2}, \frac{xy^2(x-y)}{2}, \frac{x^2z(x-z)}{2}, \frac{xz^2(x-z)}{2}, \frac{y^2z(y-z)}{2}, \frac{yz^2(y-z)}{2},\right.$$
$$\left. x^3(x-y),\ x^3(x-z),\ y^3(y-x),\ y^3(y-z),\ z^3(z-x), \frac{x^2yz-xy^2z}{2}, \frac{x^2yz-xyz^2}{2}, z^4\right\}.$$

Chapter 6

Intersection of Lattices and the Hermite Normal Form

The results from the previous chapter produced homogeneous IVP bases in a restricted range. We would like to have more efficient computations in order to obtain bases in higher degrees and IVPs with fewer terms, and to better understand them. The calculations in this chapter will achieve part of this. We use our work from Chapter 4 and take the intersection of the three cases, where one of the variables must evaluate at an odd integer. The Hermite normal form of a matrix will be the tool we use to obtain these intersections.

Since the $\mathrm{Int}(S, \mathbb{Z})$, for $S \subseteq \mathbb{Z}$, are $\mathbb{Z}$-modules, we can treat them as lattices and use existing knowledge about these to find more details for the bases of homogeneous IVPs.

Definition 96. [Mic16a, Def. 1] *A lattice is a discrete additive subgroup of* $\mathbb{R}^m$*, i.e., it is a subset* $\Lambda \subseteq \mathbb{R}^n$ *satisfying the following properties:*

(i) Λ *is closed under addition and subtraction,*

(ii) there is an $\epsilon > 0$ *such that any two distinct lattice points* $\mathbf{x} \neq \mathbf{y} \in \Lambda$ *are at distance at least* $||\mathbf{x} - \mathbf{y}|| \geq \epsilon$*.*

Above is the general definition of a lattice Λ, a useful computational definition of lattices is by using the span to linearly independent vectors, where the notation $\mathcal{L}$ will be used.

Definition 97. [GM02, Ch.1, 1] *Let* $\mathbb{R}^m$ *be* m*-dimensional Euclidean space. A lattice in* $\mathbb{R}^m$ *is the set*

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \;\middle|\; x_i \in \mathbb{Z} \right\}$$

of all integral combinations of n $\mathbb{R}$-linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The integers n and m are called the rank and dimension, respectively of the lattice.

We can use the above definition to get a definition using matrices, which will facilitate computations.

Definition 98. [GM02, Ch.1, 1] *The sequence of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in Definition 97 is called a lattice basis, which we represent as a matrix*

$$B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{m \times n}$$

with basis vectors as columns. We will write our lattice as

$$\mathcal{L}(B) = \{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}.$$

Definition 99. [Mic16b, Def. 3] *The dual of a lattice Λ is the set Λ^* of all vectors $\mathbf{x} \in span(\Lambda)$ such that $\langle \mathbf{x}, \mathbf{y} \rangle$ is an integer for all $\mathbf{y} \in \Lambda$,where $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{R}$ is the usual inner product of $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{R}^m$.*

Proposition 100. [Mic16b, Th. 2] *The dual of a lattice with basis B is a lattice with basis $D = BG^{-1}$ where $G = B^T B$ is the Gram matrix of B.*

Proposition 101. [Sch86, 4.4] *If a lattice Λ is generated by the columns of the invertible matrix B, then Λ^* is the lattice generated by the rows of B^{-1}.*

Proof. The lattice generated by the rows of B^{-1} is contained in Λ^* as each row of B^{-1} is contained in Λ^*, since $B^{-1}B = I$. Conversely, if $\mathbf{z} \in \Lambda^*$, then $\mathbf{z}B$ is integral. Hence $\mathbf{z} = (\mathbf{z}B)B^{-1}$ is an integral combination of the rows of B^{-1}. □

The dual of a basis and the Hermite echelon form defined below will be useful in finding the intersection of lattices.

Definition 102. [GM02, Def. 8.2] *A matrix with linearly independent columns $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ is in Hermite normal form (HNF) if and only if*

(i) There exists $1 \leq i_1 \leq \ldots \leq i_h \leq m$ such that if $b_{i,j} \neq 0$, then $j < h$ and $i \geq i_j$.

(ii) For all $k > j$, $0 \leq b_{i_j,k} < b_{i_j,j}$, i.e., all elements at rows i_j are reduced modulo $b_{i_j,j}$.

The HNF of a matrix is an analogue of the reduced normal form of a matrix over $\mathbb{Z}$. We will denote the HNF of a matrix A by $HNF(A)$.

Proposition 103. [GM02, Ch.1, 2.2] *If $\mathcal{L}(B)$ and $\mathcal{L}(B')$ are lattices with bases B and B', then $HNF([B|B'])$ is a basis of $\mathcal{L}(B) \cup \mathcal{L}(B')$.*

Proof. The matrix $[B|B']$ generates the lattice $\mathcal{L}(B) \cup \mathcal{L}(B')$, but there might be linear dependence between the columns of B and of B'. $HNF([B|B'])$ produces a matrix with linearly independent columns with the same span. □

Proposition 104. [GM02, Ch.1, 2.2] *Given lattices $\mathcal{L}(B)$ and $\mathcal{L}(B')$ with respective duals $\mathcal{L}(D)$ and $\mathcal{L}(D')$, the lattice generated by $HNF([D|D'])$ is the dual of $\mathcal{L}(B) \cap \mathcal{L}(B')$.*

Proof. Take $\mathbf{x} \in \text{span}(\mathcal{L}(B) \cap \mathcal{L}(B'))$; we want to show that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{y} \in \text{span}(\mathcal{L}(HNF[D|D']))$.

We know that $HNF([D|D'])$ generates the lattice $\mathcal{L}(D) \cup \mathcal{L}(D')$ by Proposition 103. Hence for all $\mathbf{y} \in \text{span}(\mathcal{L}(HNF[D|D']))$ we have

$$\langle \mathbf{x}_1, \mathbf{y} \rangle \in \mathbb{Z},$$
$$\langle \mathbf{x}_2, \mathbf{y} \rangle \in \mathbb{Z}$$

for all $\mathbf{x}_1 \in \text{span}(\mathcal{L}(D))$ and $\mathbf{x}_2 \in \text{span}(\mathcal{L}(D'))$, since $\mathcal{L}(HNF[D|D'])$ is the lattice generated by the union of $\mathcal{L}(D)$ and $\mathcal{L}(D')$. Thus $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{y} \in \text{span}(\mathcal{L}(B) \cap \mathcal{L}(B'))$. □

By using the above, we get the following procedure for finding the basis of the intersection of two lattices $\mathcal{L}(B)$ and $\mathcal{L}(B')$.

1. Calculate $D = B(B^T B)^{-1}$ and $D' = B'(B'^T B')^{-1}$.

2. Calculate $HNF([D|D'])$.

3. Take the dual of $HNF([D|D'])$, that is,

$$H' = HNF([D|D'])(HNF([D|D'])^T HNF([D|D']))^{-1}.$$

H' is the basis of $\mathcal{L}(B) \cap \mathcal{L}(B')$.

Corollary 105. *Given n bases $B_1, B_2, \ldots, B_n$ for the lattices $\mathcal{L}(B_1), \mathcal{L}(B_2), \ldots, \mathcal{L}(B_n)$ with corresponding dual lattices $\mathcal{L}(D_1), \mathcal{L}(D_2), \ldots, \mathcal{L}(D_n)$, then the dual of $\mathcal{L}(B_1) \cap \mathcal{L}(B_2) \cap \cdots \cap \mathcal{L}(B_n)$ is $\mathcal{L}([D_1|D_2|\cdots|D_n])$.*

Proof. We prove the claim by induction, the base case being Proposition 104. Suppose the basis of the dual of $\mathcal{L}(B_1) \cap \mathcal{L}(B_2) \cap \cdots \cap \mathcal{L}(B_k)$ is $\mathcal{L}([D_1|D_2|\cdots|D_k])$. We want the dual of

$$\mathcal{L}(B_1) \cap \mathcal{L}(B_2) \cap \cdots \cap \mathcal{L}(B_k) \cap \mathcal{L}(B_{k+1}) = (\mathcal{L}(B_1) \cap \mathcal{L}(B_2) \cap \cdots \cap \mathcal{L}(B_k)) \cap \mathcal{L}(B_{k+1})$$

which by Proposition 104 is

$$\mathcal{L}([[D_1|D_2|\cdots|D_k]|D_{k+1}]) = \mathcal{L}([D_1|D_2|\cdots|D_k|D_{k+1}]).$$

□

This means that the above process can be generalized to n lattices.

6.1 The 2-Variable Case

Since we know what to expect in the 2-variable case, we first use this technique for that case, and verify that we obtain the expected results.

Using the material from the previous section with homogeneous IVPs, we have the following lattice of modules:

$$\begin{tikzcd}
 & \mathcal{F} & \\
S_1 \arrow[ur, hook] & & S_2 \arrow[ul, hook'] \\
 & S_1 \cap S_2 \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

$$\begin{aligned}
\mathcal{F} &= \mathrm{Int}_m(\mathbb{Z}^2, \mathbb{Z}) \\
S_1 &= \mathrm{Int}^m(\mathbb{Z} \times (1 + 2\mathbb{Z}), \mathbb{Z}) \cong \mathrm{Int}_m(\mathbb{Z}, \mathbb{Z}) \\
S_2 &= \mathrm{Int}^m((1 + 2\mathbb{Z}) \times \mathbb{Z}, \mathbb{Z}) \cong \mathrm{Int}_m(\mathbb{Z}, \mathbb{Z})
\end{aligned}$$

We are interested in $S_1 \cap S_2 = \mathrm{Int}^m(\mathbb{Z}^2, \mathbb{Z})$. For S_1 we have the isomorphism from Proposition 67:

$$\begin{aligned}
\mathrm{Int}_m(\mathbb{Z}, \mathbb{Z}) &\cong \mathrm{Int}^m(\mathbb{Z} \times (1 + 2\mathbb{Z}), \mathbb{Z}) \\
F\colon f(x) &\mapsto y^m f\left(\frac{x}{y}\right) \\
G\colon g(x, 1) &\leftarrow\!\shortmid g(x, y).
\end{aligned}$$

We have similar maps for S_2. These were explained in Chapter 4.

We know that $\left\{\binom{x}{i}\right\}_{i \leq m}$ and $\left\{\binom{y}{j}\right\}_{j \leq m}$ are bases of $\mathrm{Int}_m(\mathbb{Z}, \mathbb{Z})$, for the variables x and y respectively. We can homogenize these at y and x respectively and obtain that

$$\mathcal{B}_1 = \left\{\binom{\frac{x}{y}}{i} y^m\right\}_{i \leq m} \quad \text{and} \quad \mathcal{B}_2 = \left\{x^m \binom{\frac{y}{x}}{j}\right\}_{j \leq m}$$

are bases for $S_1 = \mathrm{Int}^m(\mathbb{Z} \times (1 + 2\mathbb{Z}), \mathbb{Z})$ and $S_2 = \mathrm{Int}^m((1 + 2\mathbb{Z}) \times \mathbb{Z}, \mathbb{Z})$, respectively.

Let V be an ordered list of basis elements of $\mathbb{Z}^m[x, y]$. We do the following to find a basis for the intersection:

1. Store in A and B the elements of $\mathcal{B}_1$ and $\mathcal{B}_2$ written in terms of V.

2. Dualize A and B in order to obtain A' and B'.

3. Take the HNF (H) of $[A'|B']$ and the Smith normal form (S) of H.

4. Consider H to be the $m \times m$ matrix made from removing the $m \times m$ all zero block from H'.

5. Remove the zero block from H, and call the result H^*, dualize H^* to obtain H'. For a fixed m, $H' \cdot V$ produces a basis.

These polynomials do not admit the same number of elements with certain denominators as the ones obtained by Johnson and Patterson [JP11]. However taking the Smith normal form of H produces a matrix whose diagonal is the denominators of the basis, and when counting these for various m, we obtain the same results as the ones in Table 5.2, which are the values from Johnson and Patterson [JP11]. Thus one needs to use both the HNF and Smith normal form to obtain comparable bases.

6.2 The 3-Variable Case

We do something similar to the previous section for the 3-variable case. Here we are interested in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z}) = S_1 \cap S_2 \cap S_3$ for:

$$\begin{aligned}
S_1 &= \mathrm{Int}^m(\mathbb{Z} \times \mathbb{Z} \times (1+2\mathbb{Z}), \mathbb{Z}) \cong \mathrm{Int}_m(\mathbb{Z}^2, \mathbb{Z}) \\
S_2 &= \mathrm{Int}^m(\mathbb{Z} \times (1+2\mathbb{Z}) \times \mathbb{Z}, \mathbb{Z}) \cong \mathrm{Int}_m(\mathbb{Z}^2, \mathbb{Z}) \\
S_3 &= \mathrm{Int}^m((1+2\mathbb{Z}) \times \mathbb{Z} \times \mathbb{Z}, \mathbb{Z}) \cong \mathrm{Int}_m(\mathbb{Z}^2, \mathbb{Z})
\end{aligned}$$

For S_1, this isomorphism is

$$\begin{aligned}
\mathrm{Int}_m(\mathbb{Z}^2, \mathbb{Z}) &\cong \mathrm{Int}^m(\mathbb{Z} \times \mathbb{Z} \times (1+2\mathbb{Z}), \mathbb{Z}) \\
F\colon f(x) &\mapsto z^m f\left(\frac{x}{z}, \frac{y}{z}\right) \\
G\colon g(x, y, 1) &\hookleftarrow g(x, y, z).
\end{aligned}$$

Similar maps exist for S_2 and S_3.

We work with the following bases for $\mathrm{Int}_m(\mathbb{Z}^2,\mathbb{Z})$:

$$\left\{\binom{x}{i}\binom{y}{j}\right\}_{i+j\leq m}, \quad \left\{\binom{x}{i}\binom{z}{j}\right\}_{i+j\leq m} \quad \text{and} \quad \left\{\binom{y}{i}\binom{z}{j}\right\}_{i+j\leq m},$$

which are bases for the variables (x, y), (x, z) and (y, z) respectively. We homogenize at the variables z, y and x, and obtain

$$\mathcal{B}_1 = \left\{\binom{\frac{x}{z}}{i}\binom{\frac{y}{z}}{j}z^m\right\}_{i+j\leq m} \quad \mathcal{B}_2 = \left\{\binom{\frac{x}{y}}{i}y^m\binom{\frac{z}{y}}{j}\right\}_{i+j\leq m} \quad \text{and } \mathcal{B}_3 = \left\{x^m\binom{\frac{y}{x}}{i}\binom{\frac{z}{x}}{j}\right\}_{i+j\leq m}$$

respectively. Let V be an ordered list of basis elements of $\mathbb{Z}^m[x, y, z]$.

1. Store in A, B, C the elements of $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ written in terms of V.

2. Dualize A, B, C in order to obtain A', B', C'.

3. Take the HNF (H) of $[A'|B'|C']$ and the Smith normal form (S) of H.

4. Remove the zero block from H, and call the result H^*, dualize H^* to obtain H'.

Once again $H' \cdot V$ gives IVPs, but differing from those obtained in Chapter 5. There are usually more elements with bigger denominators than the polynomials from Table 5.4. This does produce the same largest denominators for degree m as Theorem 95. Since this process is faster and requires less memory we can find the next three rows of Table 5.4:

		k, for Denominators of Size 2^k															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Degree m	23	7	14	7	14	28	14	7	28	35	14	28	49	14	14	6	0
	24	7	14	7	14	28	14	7	28	35	14	28	49	14	14	25	6
	25	7	14	7	14	28	14	7	28	35	14	28	49	14	14	34	23

Table 6.1: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3,\mathbb{Z})$ at $p = 2$ Continued from Table 5.4

The faster computations may also be explained by the fact that we are working with $\frac{(m+1)(m+2)}{2} \times \frac{3(m+1)(m+2)}{2}$ matrices for degree m, as opposed to $\frac{(m+1)(m+2)}{2} \times$

$\frac{(m+1)(m+2)(m+3)}{6}$ matrices as needed for the Smith normal form, which will be smaller for degrees 7 and higher.

6.3 Results at Other Primes

We can use the technique from Section 6.2 and localize at other primes. We repeated this process for all primes between 3 and 29 (but only display results up to 13). For $p = 29$, the degrees that were within calculations, produced bases with no denominators. As p gets bigger we get fewer basis elements with denominators, which will allow calculations for higher degrees, since the matrices we work with are simpler. Note that the size of the matrices we work with are independent of the prime, which allows us to get the following tables:

		k, for Denominators of Size 3^k									
		0	1	2	3	4	5	6	7	8	9
Degree m	1	3	0	0	0	0	0	0	0	0	0
	2	6	0	0	0	0	0	0	0	0	0
	3	10	0	0	0	0	0	0	0	0	0
	4	12	3	0	0	0	0	0	0	0	0
	5	13	8	0	0	0	0	0	0	0	0
	6	13	15	0	0	0	0	0	0	0	0
	7	13	23	0	0	0	0	0	0	0	0
	8	13	26	6	0	0	0	0	0	0	0
	9	13	26	16	0	0	0	0	0	0	0
	10	13	26	27	0	0	0	0	0	0	0
	11	13	26	39	0	0	0	0	0	0	0
	12	13	26	39	10	3	0	0	0	0	0
	13	13	26	39	18	9	0	0	0	0	0
	14	13	26	39	23	19	0	0	0	0	0
	15	13	26	39	26	26	6	0	0	0	0
	16	13	26	39	26	33	16	0	0	0	0
	17	13	26	39	26	36	31	0	0	0	0
	18	13	26	39	26	38	41	7	0	0	0
	19	13	26	39	26	39	52	15	0	0	0
	20	13	26	39	26	39	52	36	0	0	0
	21	13	26	39	26	39	52	52	6	0	0
	22	13	26	39	26	39	52	65	16	0	0
	23	13	26	39	26	39	52	78	27	0	0
	24	13	26	39	26	39	52	78	46	6	0
	25	13	26	39	26	39	52	78	49	29	0
	26	13	26	39	26	39	52	78	51	46	8
	27	13	26	39	26	39	52	78	52	62	19

Table 6.2: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ at $p = 3$

		k, for Denominators of Size 5^k				
		0	1	2	3	4
Degree m	1	3	0	0	0	0
	2	6	0	0	0	0
	3	10	0	0	0	0
	4	15	0	0	0	0
	5	21	0	0	0	0
	6	25	3	0	0	0
	7	28	8	0	0	0
	8	30	15	0	0	0
	9	31	24	0	0	0
	10	31	35	0	0	0
	11	31	47	0	0	0
	12	31	54	6	0	0
	13	31	59	15	0	0
	14	31	62	27	0	0
	15	31	62	43	0	0
	16	31	62	60	0	0
	17	31	62	78	0	0
	18	31	62	87	10	0
	19	31	62	93	24	0
	20	31	62	93	45	0
	21	31	62	93	67	0
	22	31	62	93	90	0
	23	31	62	93	114	0
	24	31	62	93	124	15
	25	31	62	93	124	41
	26	31	62	93	124	68
	27	31	62	93	124	96
	28	31	62	93	124	125

Table 6.3: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ at $p = 5$

		k, for Denominators of Size 7^k			
		0	1	2	3
Degree m	1	3	0	0	0
	2	6	0	0	0
	3	10	0	0	0
	4	15	0	0	0
	5	21	0	0	0
	6	28	0	0	0
	7	36	0	0	0
	8	42	3	0	0
	9	47	8	0	0
	10	51	15	0	0
	11	54	24	0	0
	12	56	35	0	0
	13	57	48	0	0
	14	57	63	0	0
	15	57	79	0	0
	16	57	90	6	0
	17	57	99	15	0
	18	57	106	27	0
	19	57	111	42	0
	20	57	114	60	0
	21	57	114	82	0
	22	57	114	105	0
	23	57	114	129	0
	24	57	114	144	10
	25	57	114	156	24
	26	57	114	165	42
	27	57	114	171	64
	28	57	114	171	93

Table 6.4: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ at $p = 7$

		k, for Denominators of Size 11^k		
		0	1	2
Degree m	1	3	0	0
	2	6	0	0
	3	10	0	0
	4	15	0	0
	5	21	0	0
	6	28	0	0
	7	36	0	0
	8	45	0	0
	9	55	0	0
	10	66	0	0
	11	78	0	0
	12	88	3	0
	13	97	8	0
	14	105	15	0
	15	112	24	0
	16	118	35	0
	17	123	48	0
	18	127	63	0
	19	130	80	0
	20	132	99	0
	21	133	120	0
	22	133	143	0
	23	133	167	0
	24	133	186	6
	25	133	203	15
	26	133	218	27
	27	133	231	42
	28	133	242	60

Table 6.5: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ at $p = 11$

		k, for Denominators of Size 13^k	
		0	1
Degree m	1	3	0
	2	6	0
	3	10	0
	4	15	0
	5	21	0
	6	28	0
	7	36	0
	8	45	0
	9	55	0
	10	66	0
	11	78	0
	12	91	0
	13	105	0
	14	117	3
	15	128	8
	16	138	15
	17	147	24
	18	155	35
	19	162	48
	20	168	63
	21	173	80
	22	177	99
	23	180	120
	24	182	143
	25	183	168
	26	183	195
	27	183	223
	28	183	246

Table 6.6: Number of Denominators in $\mathrm{Int}^m(\mathbb{Z}^3, \mathbb{Z})$ at $p = 13$

6.4 Symmetrization

Since symmetric polynomials are of interest in the case of computing the homotopy of BU, we look into finding homogeneous symmetric IVPs.

Definition 106. *A polynomial $p(x_1, \ldots, x_n)$ in n-variables is symmetric if for any* *permutation σ of the subscripts $1, 2, \ldots, n$ one has*

$$p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = p(x_1, \ldots, x_n).$$

Definition 107. *Given a 3-variable polynomial $f(x, y, z)$ one can symmetrize f by taking*

$$f_{sym} = f(x, y, z) + f(y, x, z) + f(z, y, x) + f(x, z, y) + f(y, z, x) + f(z, x, y).$$

An important matter to notice is that when adding six different permutations of an IVP, there is a great chance that we will obtain even numerators for the coefficients which will cancel out with the denominators. Focusing on degree 14 for now, from Table 5.4 we know we can get a homogeneous IVP with 2^9 in its denominator and we wonder if we can obtain the same denominator with a symmetric IVP.

When we let f be the degree 14 homogeneous IVP with a 2^9 in its denominator, we obtained f_{sym} with a 2^8 in its denominator. The main question of interest here is: can we have a symmetric IVP with 2^9 in its denominator? We conjecture that the answer is no.

Amongst other symmetrization attempts we symmetrize polynomials obtained from the HNF and polynomials obtained from the Fano plane, (the construction of these will be explained in Chapter 7).

From these attempts the best we managed to obtain is a homogeneous IVP g with 2^8 in its denominator that factors as a product of linear factors. Even though the denominator is smaller by a power of 2 than the best we can obtain for the non-symmetric case, the factorization is useful to explain how to construct these, and the polynomials can keep their full denominators once they are made symmetric.

Below is a table showing what happened when symmetrizing the polynomials from the HNF up to degree 14. The “sym” column counts how many polynomials were already symmetric, the “null” column counts the number of polynomials that went to zero when symmetrizing, and the other columns count the number of basis elements with each denominator:

		sym	null	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
Degree	1	0	0	3	0	0	0	0	0	0	0	0
	2	0	0	6	0	0	0	0	0	0	0	0
	3	1	3	6	0	0	0	0	0	0	0	0
	4	0	5	7	3	0	0	0	0	0	0	0
	5	0	5	10	6	0	0	0	0	0	0	0
	6	0	8	7	13	0	0	0	0	0	0	0
	7	0	3	12	9	6	6	0	0	0	0	0
	8	0	10	7	12	3	13	0	0	0	0	0
	9	0	4	7	12	3	23	6	0	0	0	0
	10	0	10	7	12	2	19	16	0	0	0	0
	11	0	5	7	14	2	15	31	4	0	0	0
	12	0	6	7	12	2	10	31	20	3	0	0
	13	0	0	7	12	2	13	20	27	21	3	0
	14	0	0	7	12	2	11	20	9	22	32	5

Table 6.7: Denominators Obtained after Symmetrizing

For degrees 1,2,4,5,7,9,11,13 we did not lose all maximal denominators, but we do get fewer elements than in Table 5.4.

Another question one may ask is: can we symmetrize each linear factor first, multiply out and still obtain an IVP with 2^8 in its denominator? The answer is no since each linear factor is of the form $\ell = ax + by + cz$ and calculating:

$$\begin{aligned}\ell_{sym} &= (ax+by+cz)+(bx+ay+cz)+(cx+by+az)\\ &\quad+(ax+cy+bz)+(bx+cy+za)+(cx+ay+bz)\\ &=(2a+2b+2c)(x+y+z)\end{aligned}$$

Hence any linear factor will be divisible by 2 and will cancel out with the denominator.

Chapter 7

Building 3-Variable Homogeneous Integer-valued Polynomials Using Projective Planes

The goal of this chapter is to use projective H-planes, which are a generalization of finite projective planes over rings, to construct a correspondence between lines that cover H-planes and homogeneous IVPs that are a product of linear factors. We will illustrate this correspondence starting with the degree 8 case where we produce a polynomial with largest possible denominator which factors as a product of linear polynomials.

We then show why the degree 14 case, which has a basis element with a 2^9 in its denominator, cannot be written as a product of linear factors. We look into building polynomials of higher degree where we managed to obtain IVPs. We end the chapter by using this correspondence with the 2-variable case and obtain the same results as in Johnson and Patterson [JP11].

7.1 Projective H-Planes

In this section we summarize the literature on Hjelmslev planes, denoted H-planes, in order to use it to build a correspondence later on. What we are interested in is finding a extension of the notion of projective planes over the rings $\mathbb{Z}/(p^k)$. These were first introduced by Wilhelm Klingenberg [Kli54], who was following the work of the Danish mathematician Johannes Hjelmslev, whose main results were in non-Euclidean geometry. Klingenberg altered the axioms of the projective plane to allow two lines to intersect in several distinct points. These points would be called neighbours. This notion of neighbouring was shown by Klingenberg to be an equivalence relation for H-planes. Note that the first paper written in English about projective H-planes is from Erwin Kleinfeld [Kle59].

7.1.1 Projective Planes over Finite Fields

Projective planes arise from wanting a geometry with no parallel lines. This would more closely resemble the situation when we look at two parallel lines in reality. For example, when we look at train tracks, these do seem to meet at a vanishing point.

The study of Projective planes arose in the early 1900's [Veb04], we will present results from [AS68] and [Ayr67], since their book defines finite projective planes in the computational way that will be needed for this chapter.

Definition 108. [AS68, 1.3] *A projective plane consists of a set of lines $\mathcal{L}$, a set of points $\mathcal{P}$, and a relationship between the lines and points called incidence $\mathcal{I}$, having the following properties:*

I Given any two distinct points, there is exactly one line incident to both of them.

II Given any two distinct lines there is exactly one point incident with both of them.

III There exist three non-collinear points.

IV Every line contains at least three points.

We state some general statements about any projective plane and then some more specific ones about projective planes over finite fields.

Lemma 109. [Ayr67, Th. 7.1] *If L_1 and L_2 are distinct lines, then there is a point that is on neither of them.*

Theorem 110. [Ayr67, Th. 7.5] *Every line in the projective plane has the same number of points.*

Over a finite field $\mathbb{F}_q$, where $q = p^k$ for p a prime and $0 < k \in \mathbb{Z}$, we look at the projective n-space.

Definition 111. [AS68, 3.3] *The finite projective n-space over $\mathbb{F}_q$, denoted $\mathbb{F}_q\mathbf{P}^n$, is defined as the set of points $\mathbf{w} \in \mathbb{F}_q^{n+1}\backslash\{\mathbf{0}\}$ with the equivalence relation $\mathbf{w} \sim \lambda\mathbf{w}$ for λ non-zero in $\mathbb{F}_q$.*

For example, consider $\mathbb{F}_q\mathbf{P}^1$, which is called the projective line. $\mathbb{F}_q\mathbf{P}^1$ can be represented as a set of equivalence classes (x, y), such that $(x, y) \sim (\lambda x, \lambda y)$ for all non zero λ. The pairs (x, y) are the points $\mathbf{w}$ in Definition 111. Projective lines will have $q + 1$ points. For example $\mathbb{F}_2\mathbf{P}^1 \simeq \mathbb{F}_2^2 \backslash (0, 0)$, and it has three points.

The finite projective space that we will mainly look at for our work is the finite projective plane $\mathbb{F}_q\mathbf{P}^2$, when $q = p$, where we can do arithmetic $\pmod{p}$.

Definition 112. [AS68, 3.3] *A point in $\mathbb{F}_p\mathbf{P}^2$ is a triple from $\mathbb{F}_p^3 \backslash (0, 0, 0)$, that satisfies the following equivalence relation: $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for all non zero λ in $\mathbb{F}_p$.*

Definition 113. [AS68, 3.3] *A line $L = (a, b, c)$ in $\mathbb{F}_p\mathbf{P}^2$ is determined by a linear polynomial $ax + by + cz$, with at least one of a, b or c not divisible by p, such that the points incident to it are*

$$L_{(a,b,c)} = \{(x, y, z) \mid ax + by + cz \equiv 0 \pmod{p}\}.$$

Note that the above is a symmetric relation, which gives the important result below, referred to as the duality of the projective plane.

Proposition 114. [AS68, 1.7 Th. 3] *Given the incidence relation in Definition 113, the point $P = (x, y, z)$ and the line $L = (a, b, c)$ we also have that $P_1 = (a, b, c)$ is incident to $L_1 = (x, y, z)$. This is referred to as the duality of projective planes.*

$\mathbb{F}_2\mathbf{P}^2$ is referred to as the Fano plane and is the smallest projective plane, pictured below. It has seven points and seven lines.

Any line in $\mathbb{F}_p\mathbf{P}^2$ is isomorphic to $\mathbb{F}_p\mathbf{P}^1$. Any two lines intersect in exactly one point, and any point has exactly three lines going through it. This holds for $p = 2$; in general, $p + 1$ lines go through one point.

Proposition 115. [AS68, 2.3 Th. 1(a)] *When picking all $p+1$ lines that go through a single point P in $\mathbb{F}_p\mathbf{P}^2$, these $p + 1$ lines cover all of $\mathbb{F}_p\mathbf{P}^2$.*

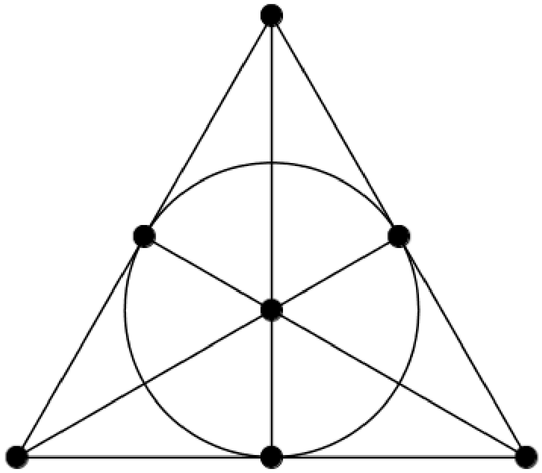


Figure 7.1: $\mathbb{F}_2\mathbf{P}^2$, the Fano Plane

Proof. For any point Q in $\mathbb{F}_p\mathbf{P}^2$ there is a unique line passing through Q and P. □

Proposition 116. [AS68, 2.3 Th. 1(b)] *The projective plane $\mathbb{F}_p\mathbf{P}^2$ has p^2+p+1 distinct points.*

Proof. The set $\mathbb{F}_p$ has p points. The set $(\mathbb{F}_p)^3\backslash(0,0,0)$ has p^3-1 points. Since there are $p-1$ units in $\mathbb{F}_p$ and we get an equivalence class for each of these, we have $\frac{p^3-1}{p-1}=p^2+p+1$ points. □

Corollary 117. [AS68, 2.3 Th. 1(b)] *The projective plane $\mathbb{F}_p\mathbf{P}^2$ has p^2+p+1 distinct lines.*

Proof. This comes from the duality of lines and points in the projective plane. □

7.1.2 Projective H-planes over $\mathbb{Z}/(2^k)$

When trying to keep the same structure as in Section 7.1.1 but replacing $\mathbb{F}_2$ by $\mathbb{Z}/(4)$ or by $\mathbb{Z}/(2^k)$, we will not have a projective plane anymore. Before looking at the planes, we will extend the projective line to $\mathbb{Z}/(p^k)$. The definitions and results from this section were obtained by adapting [Kle59] to get computational results as as in Section 7.1.1.

Definition 118. *The line $\mathbb{Z}/(p^k)\mathbf{P}^1$ will be represented as a set of equivalence classes of pairs $(x, y) \in (\mathbb{Z}/(p^k))^2$, such that at least one of x and y is not divisible by p, with equivalence relation $(x, y) \sim (\lambda x, \lambda y)$ for all units λ in $\mathbb{Z}/(p^k)$.*

Lemma 119. *The line $\mathbb{Z}/(p^k)\mathbf{P}^1$ will contain $\frac{p^{2k}-p^{2(k-1)}}{p^k-p^{k-1}} = p^k + p^{k-1}$ points.*

Proof. We have that $(p^{k-1})^2$ is the number of pairs in $\mathbb{F}_p^2$, where each element is divisible by p and $p^k - p^{k-1}$ is the number of units in $\mathbb{F}_p$. □

For example, $\mathbb{F}_2\mathbf{P}^1$ has $2^1 + 2^0 = 3$ points and $\mathbb{Z}/(4)\mathbf{P}^1$ has $2^2 + 2 = 6$ points.

Now to extend the projective plane, we take all the triples (a, b, c) in $\mathbb{Z}/(4)^3$ such that there is at least one odd value in the triple, and we use the same equivalence relationship on these. This will give us $\frac{4^3-8}{2} = 28$ points since there are eight even triples in $\mathbb{Z}/(4)^3$ and two units in $\mathbb{Z}/(4)$. There will also be 28 lines by duality which will be revisited in Proposition 123. More generally, we have the definition below.

Definition 120. *The projective H-plane over $\mathbb{Z}/(p^k)$: $\mathbb{Z}/(p^k)\mathbf{P}^2$ is the set of triples from $\mathbb{Z}/(p^k)^3$, such that p does not divide all values in the triple, with the equivalence relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for all units λ in $\mathbb{Z}/(p^k)$.*

The properties of incidence of lines and points in projective H-planes have been studied, especially by those interested in coding theory, through arcs in projective H-planes. These will not be of any help for this work. However, the coding theorist Michael Kiermaier [Kie] did produce a very useful visual representation of $\mathbb{Z}/(4)\mathbf{P}^2$.

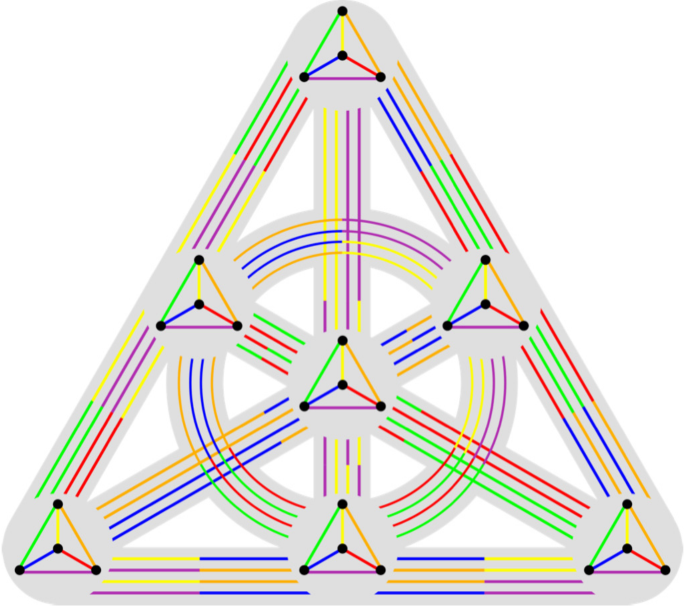


Figure 7.2: $\mathbb{Z}/(4)\mathbf{P}^2$ [Kie]

Given this picture every point of $\mathbb{F}_2\mathbf{P}^2$ is lifted to a tetrahedron that has four points, which are the points over $\mathbb{Z}/(4)\mathbf{P}^2$. Every line from $\mathbb{F}_2\mathbf{P}^2$ is lifted to four lines, that are represented by four coloured segments which are the lines over $\mathbb{Z}/(4)\mathbf{P}^2$. Each line in $\mathbb{Z}/(4)\mathbf{P}^2$ on the picture can be found by taking one of the four lines corresponding to a line over $\mathbb{F}_2\mathbf{P}^2$ which is represented by four coloured segments. Then taking the points that are adjacent to these coloured segments on the tetrahedrons.

Lemma 121. *The projective plane $\mathbb{Z}/(p^k)\mathbf{P}^2$ has $\dfrac{p^{3k}-(p^{k-1})^3}{p^k-p^{k-1}} = p^{2(k-1)}(p^2+p+1)$ points.*

Proof. We have that $(p^{k-1})^3$ is the number of triples in $\mathbb{F}_p^3$, where each element is divisible by p and $p^k - p^{k-1}$ is the number of units in $\mathbb{Z}/(p^k)$. □

Incidence of lines and planes is defined in a similar way:

Definition 122. *A line $L = (a, b, c)$ in $\mathbb{Z}/(p^k)\mathbf{P}^2$ is determined by a homogeneous linear polynomial $ax + by + cz$, with at least one of a, b or c not divisible by p. The points incident to L are those such that*

$$L_{(a,b,c)} = \{(x, y, z) \mid ax + by + cz \equiv 0 \pmod{p^k}\}.$$

Proposition 123. *Given the incidence relation in Definition 122, the point $P = (x, y, z)$ and the line $L = (a, b, c)$ we also have that $P_1 = (a, b, c)$ is incident to $L_1 = (x, y, z)$. This is referred to as the duality of projective H-planes.*

We can build an incidence matrix of size $|\mathbb{Z}/(p^k)\mathbf{P}^2| \times |\mathbb{Z}/(p^k)\mathbf{P}^2|$. Since both point and lines can be represented by triples, we label the triple of the line with coordinates L_i be the same as the triple of the point with coordinates P_i. A zero entry in the matrix means that the point is incident to the line.

For $\mathbb{F}_2\mathbf{P}^2$ we get the following incidence matrix:

$$\begin{array}{r c}
 & \begin{array}{ccccccc} L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 \end{array} \\
\begin{array}{r} P_1 = (0,0,1) \\ P_2 = (0,1,0) \\ P_3 = (0,1,1) \\ P_4 = (1,0,0) \\ P_5 = (1,0,1) \\ P_6 = (1,1,0) \\ P_7 = (1,1,1) \end{array} &
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}
\end{array}$$

One can build a similar 28×28 matrix for $\mathbb{Z}/(p^k)\mathbf{P}^2$. The duality between points and lines is equivalent to the incidence matrices being symmetric.

Proposition 124. *Each line in $\mathbb{Z}/(2^k)\mathbf{P}^2$ is incident to $2^{k+1} - 2^{k-1}$ points.*

Proof. For a line $L = (a, b, c)$ at least one of $a,\ b,\ c$ is odd. Without loss of generality, assume c is odd. Thus for any (x, y) in $\mathbb{Z}/(2^k)\mathbf{P}^1$ there is a z such that $(x, y, z) \in L$, namely $z = c^{-1}(-ax - by)$. This gives us a one-to-one correspondence between L and $\mathbb{Z}/(2^k)\mathbf{P}^1$, which has $2^{k+1} - 2^{k-1}$ elements by Lemma 119. □

Corollary 125. *Each point in $\mathbb{Z}/(2^k)\mathbf{P}^2$ is incident to $2^{k+1} - 2^{k-1}$ lines.*

Proof. This follows since the incidence relation is symmetric. □

Proposition 126. *Suppose $L_1 = (a_1, b_1, c_1)$ and $L_2 = (a_2, b_2, c_2)$ are lines in $\mathbb{Z}/(2^k)\mathbf{P}^2$ for some $k > 1$. If $(a_1, b_1, c_1) \equiv (a_2, b_2, c_2) \pmod{2^h}$ for some $h < k$ and $(a_1, b_1, c_1) \not\equiv (a_2, b_2, c_2) \pmod{2^{h+1}}$, then $|L_{(a_1,b_1,c_1)} \cap L_{(a_2,b_2,c_2)}| = 2^{k-h}$.*

Proof. Suppose $L = (a_1, b_1, c_1)$ and $L = (a_2, b_2, c_2)$ are lines over $\mathbb{Z}/(2^k)\mathbf{P}^2$ for some $k > 1$. We want to find the number of solutions to the following matrix equation:

$$AX = 0$$

$$\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{2^k}.$$

Replacing A by its Smith normal form gives

$$USV \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{2^k},$$

where U is a 2×2 matrix and V is a 3×3 matrix, and both are unimodular. Since U is invertible, we multiply both sides by its inverse, and since V represents a change of variables on $x,\ y,\ z$, we can write our equation as

$$S \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{2^k}.$$

First we look at when $L_1 \equiv L_2 \pmod{2^h}$, for $0 < h < k$. Here h is the maximal exponent such that the lines are congruent. Therefore we have:

$$\begin{aligned} a_2 &\equiv a_1 \pmod{2^h} \\ b_2 &\equiv b_1 \pmod{2^h} \\ c_2 &\equiv c_1 \pmod{2^h}. \end{aligned}$$

Without loss of generality we may assume that a_1 is odd, and a_2 is also odd since the lines are congruent $\pmod{2^h}$, so $a_1 \equiv a_2 \pmod 2$. Now reduce A in order to obtain the Smith normal form over $\mathbb{Z}_{(2)}$, which exists by Theorem 88:

$$\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} \sim \begin{bmatrix} 1 & \frac{b_1}{a_1} & \frac{c_1}{a_1} \\ 1 & \frac{b_2}{a_2} & \frac{c_2}{a_2} \end{bmatrix}.$$

Since invertible column and row operations will not change the congruences, we have that

$$\begin{aligned} \frac{b_1}{a_1} &\equiv \frac{b_2}{a_2} \pmod{2^h}, \\ \frac{c_1}{a_1} &\equiv \frac{c_2}{a_2} \pmod{2^h}, \end{aligned}$$

which gives in $\mathbb{Z}_{(2)}$

$$\begin{aligned} \frac{b_2}{a_2} &= \frac{b_1}{a_1} + m2^h, \\ \frac{c_2}{a_2} &= \frac{c_1}{a_1} + n2^h. \end{aligned}$$

Note that either m or n is odd since the two equations below have the same set of solutions

$$\begin{aligned} a_2x + b_2y + c_2z &\equiv 0 \pmod{2^k} \\ a_1x + \frac{a_1}{a_2}b_2y + \frac{a_1}{a_2}c_2z &\equiv 0 \pmod{2^k} \end{aligned}$$

since the second equation is obtained by multiplying the first by a unit. From there we get a_1 as the coefficient of x in both equations hence h is maximal such that

$$\begin{aligned} \frac{a_1}{a_2}b_2 &\equiv b_1 \pmod{2^h} \\ \frac{a_1}{a_2}c_2 &\equiv c_1 \pmod{2^h}, \end{aligned}$$

and

$$\begin{aligned} b_2 &\equiv b_1 \pmod{2^h} \\ c_2 &\equiv c_1 \pmod{2^h}. \end{aligned}$$

Returning to our matrix reduction, we get

$$\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} \sim \begin{bmatrix} 1 & \frac{b_1}{a_1} & \frac{c_1}{a_1} \\ 1 & \frac{b_1}{a_1} + m2^h & \frac{c_1}{a_1} + n2^h \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & m2^h & n2^h \end{bmatrix}$$

Without loss of generality suppose m is odd

$$\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^h & \frac{n}{m}2^h \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^h & 0 \end{bmatrix}$$

We then have the following matrix equation:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^h & 0 \end{bmatrix} \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{2^k}$$

We need to solve $x' \equiv 0 \pmod{2^k}$ and $2^h y' \equiv 0 \pmod{2^k}$. The first equation does not affect the number of solutions, and there are 2^{h-k} values for $y' \pmod{2^k}$ such that $2^h y' \equiv 0 \pmod{2^k}$.

□

Corollary 127. *Two lines over $\mathbb{Z}/(4)\mathbf{P}^2$ will intersect either in 2 points, when the projections of the lines over $\mathbb{F}_2\mathbf{P}^2$ are equal, or in 1 point when they are not.*

Example 128. *Proposition 126 has been programmed for the 28 lines over $\mathbb{Z}/(4)\mathbf{P}^2$ in MAPLE, where all the distinct pairs of lines when put in a matrix and their Smith normal form was calculated over $\mathbb{Z}$ using MAPLE. The following four matrices were obtained:*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{bmatrix}, \textit{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

The first three correspond to the cases when the lines only intersect once, and the last one occurs where the lines intersect in two points. Writing the element $S_{2,2}$ of the Smith normal form, S, as $2^i u$, the lines intersect in 2^i points.

Lemma 129. *Given a point P in $\mathbb{Z}/(4)\mathbf{P}^2$, the 6 lines that are incident to P, reduce pairwise to three lines in $\mathbb{F}_2\mathbf{P}^2$.*

Proof. Given the point $P = (x, y, z)$, we know that six lines are incident to it, given the duality of $\mathbb{Z}/(4)\mathbf{P}^2$. Without loss of generality $P = (1, 0, 0)$. Over $\mathbb{Z}/(4)\mathbf{P}^2$, P is on the lines with the following linear representations: z, $2y + z$, y, $y + 2z$, $y + z$ and $y + 3z$. Thus the lines reduce to $z \equiv 2y + z \pmod 2$, $y \equiv y + 2z \pmod 2$ and $y + z \equiv y + 3z \pmod 2$. □

Proposition 130. *Given a point P in $\mathbb{Z}/(4)\mathbf{P}^2$ the six lines that are incident to P cover all of $\mathbb{Z}/(4)\mathbf{P}^2$.*

Proof. By Proposition 126 we have that any two lines intersect in one point, and by the duality any two points are joined by a line. Thus when taking all the lines that go through P, we cover all the points. □

Proposition 131. *Given a point P in $\mathbb{Z}/(2^k)\mathbf{P}^2$, the $3 \cdot 2^{k-1}$ lines that are incident to P cover all of $\mathbb{Z}/(2^k)\mathbf{P}^2$.*

Proof. The proof of Proposition 130 does not depend on the number of lines that cover the plane, so the statement can be generalized. □

7.2 Using the Projective Plane to Build a Correspondence

This section will explain how we can use the correspondence between sets of lines in projective H-planes and homogeneous IVPs that factor completely. Understanding this correspondence will allow us to better understand both topics and solve problems on each side using knowledge of the other.

On the projective H-plane side we are interested in the geometry of those planes, especially in how we can cover all points in the plane using a minimal number of lines. On the homogeneous IVP side we are interested in our classical problem: how can we construct a homogeneous IVP of a certain degree with the highest power of the prime in which we are are interested in its denominator?

Starting with the Fano plane we have that if we take any three lines that intersect in one point, we manage to cover all seven points in the plane. If we multiply three linear factors corresponding to the equations of the lines that all meet in one point, say $f_1(x, y, z),\ f_2(x, y, z),\ f_3(x, y, z)$, we get that $\frac{f_1 \cdot f_2 \cdot f_3}{2}$ is an IVP.

Given how the Fano plane was constructed when taking seven linear factors that correspond to all seven lines of the Fano plane, namely

$$f_1(x, y, z),\ f_2(x, y, z),\ f_3(x, y, z),\ f_4(x, y, z),\ f_5(x, y, z),\ f_6(x, y, z),\ f_7(x, y, z),$$

then $\frac{f_1 \cdot f_2 \cdot f_3 \cdot f_4 \cdot f_5 \cdot f_6 \cdot f_7}{2^3}$ is an IVP, since each point will be on three lines, hence those linear factors will each evaluate to an even value over $\mathbb{Z}$.

We want to expand the previous to $\mathbb{Z}/(p^k)\mathbf{P}^2$, and see if for higher k, we can obtain bigger denominators when we cover the full plane. We start with the case of trying to cover $\mathbb{Z}/(4)\mathbf{P}^2$ with seven lines that would reduce to the lines of the Fano plane.

In general the number of points covered by a set of lines can be counted using the inclusion-exclusion principle stated below:

Theorem 132. [vLW01] *Given a finite number of finite sets, $A_1, A_2, \ldots, A_n$ we have*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \\ \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Using this to count for seven distinct lines $L_1, \ldots, L_7$ in $\mathbb{Z}/(4)\mathbf{P}^2$, we get that

$$\begin{aligned}|L_1 \cup \cdots \cup L_7| = 7 \cdot 6 - \sum_{i<j} |L_i \cap L_j| + \sum_{i<j<k} |L_i \cap L_j \cap L_k| \\ - \sum_{i<j<k<\ell} |L_i \cap L_j \cap L_k \cap L_\ell| + \sum_{i<j<k<\ell<m} |L_i \cap L_j \cap L_k \cap L_\ell \cap L_m| \\ - \sum_{i<j<k<\ell<m<n} |L_i \cap L_j \cap L_k \cap L_\ell \cap L_m \cap L_n|.\end{aligned}$$

Note that since each point is on at most six lines, there is no point where all seven lines intersect. The above can simplify to :

$$|L_1 \cup \cdots \cup L_7| = 7 \cdot 6 - i_2 + i_3 - i_4 + i_5 - i_6,$$

where i_j represents that number of points where j lines intersect. If we restrict this to seven lines over $\mathbb{Z}/(4)\mathbf{P}^2$ that reduce to the full set of lines of the Fano plane, we get at most three lines going through a point:

$$|L_1 \cup \cdots \cup L_7| = 7 \cdot 6 - i_2 + i_3.$$

Each pair of lines intersect in exactly one point since the lines are not congruent modulo 2. This gives us $\binom{7}{2} = 21 = i_2$ points of intersection. Thus we have

$$|L_1 \cup \cdots \cup L_7| = 7 \cdot 6 - 21 + i_3 = 21 + i_3.$$

Thus, the number of points we cover depends on i_3, the number of points that are on the intersection of three lines. We can establish that $0 \leq i_3 \leq 7$, since the Fano plane only has seven lines. When using MAPLE to calculate all options, we get that $i_3 \in \{0, 2, 4, 6\}$. What is of main interest here is that $i_3 \neq 7$, which means that we cannot fully cover $\mathbb{Z}/(4)\mathbf{P}^2$ with seven lines that reduce to the Fano plane.

Proposition 133. *Given i_3 defined as above, we have $i_3 \neq 7$.*

Proof. Proposition 126 and an exhaustive combinatorial argument can be used to prove this. However, we can get the same claim from our results in Chapter 5 where from Table 5.4, we know that for degree 7 the best denominator we can have is 2^3. If we did obtain a full covering of the H-plane, from seven lines, then we would know that for each triple of integers (a, b, c), three linear factors would evaluate to an even value and one of them would be a multiple of 4 which would guarantee a 2^4 in the denominator of this polynomial. □

This can be used to prove the geometric result below that states that there is no copy of the Fano plane in $\mathbb{Z}/(4)\mathbf{P}^2$. By this we mean that we cannot find seven lines that reduce to the Fano plane when there are seven points that are the intersection of three lines.

Corollary 134. *There is no embedded copy of the Fano plane in $\mathbb{Z}/(4)\mathbf{P}^2$.*

Proof. Suppose we did have seven lines over $\mathbb{Z}/(4)\mathbf{P}^2$ such that there are seven points over $\mathbb{Z}/(4)\mathbf{P}^2$ that reduce to $\mathbb{F}_2\mathbf{P}^2$ and three lines intersect at these seven points.

The reduction map

$$\pi\colon \mathbb{Z}/(4)\mathbf{P}^2 \to \mathbb{F}_2\mathbf{P}^2$$

which reduces all three coordinates of a point $\pmod 2$ is a surjective homomorphism. Let

$$\varphi\colon \mathbb{F}_2\mathbf{P}^2 \to \mathbb{Z}/(4)\mathbf{P}^2$$

be the map that sends $\mathbb{F}_2\mathbf{P}^2$ to the seven corresponding points of $\mathbb{Z}/(4)\mathbf{P}^2$ where the three lines intersect. Then

$$\pi \circ \varphi = 1_{\mathbb{F}_2\mathbf{P}^2},$$

which is not a possible composition, since the identity should only map $\mathbb{F}_2\mathbf{P}^2$ to the points of $\mathbb{Z}/(4)\mathbf{P}^2$ with the same coordinates, but these do not form an embedded Fano plane. □

The Theorem explain how covering projective planes can help us build homogeneous IVPs.

Theorem 135. *When building a polynomial f of degree $m > k$, such that $\frac{f(x,y,z)}{2^k}$*

is an homogeneous IVP, it is sufficient to verify that $\frac{f(x,y,z)}{2^k}$ *is integer valued at the points of* $\mathbb{Z}/(2^k)\mathbf{P}^2$.

Proof. We have that $f(2x', 2y', 2z') = 2^m f(x', y', z')$ since f is homogeneous. Therefore, one only needs to focus on the triples (x', y', z'), where at least one of x', y' or z' is odd. For $\lambda \in \mathbb{Z}/(2^k)^*$, if $(x', y', z') = (\lambda x, \lambda y, \lambda z)$, then $f(x', y', z') = \lambda^m f(x, y, z)$. Hence if $2^\ell | f(x, y, z)$, then $2^\ell | f(x', y', z')$. It is sufficient that f only covers one representative per equivalence class. □

Note that Theorem 135 builds a homogenous IVP with 2^k for denominator, the next result, as well the following sections will demonstrate, that larger denominators can be obtained.

The result below is a corollary of Proposition 130.

Corollary 136. *When picking six lines that intersect in the same point over* $\mathbb{Z}/(4)\mathbf{P}^2$, *one can build the homogeneous IVP* $\frac{f(x,y,z)}{2^3}$, *where* 2^3 *is the greatest possible denominator.*

Proof. Given P, the 6 lines going through it will cover all 28 points of $\mathbb{Z}/(4)P^2$ by Proposition 130. Using Theorem 135 $f(x, y, z)$ the product of these linear factors, is such that $\frac{f(x,y,z)}{2^2}$ is an IVP.

Since the lines will cover twice the Fano plane for each point in $\mathbb{Z}/(4)\mathbf{P}^2$, there are two linear factors f_i such that $f_i(x, y, z) \equiv 0 \pmod 2$ at all points of $\mathbb{Z}/(2)\mathbf{P}^2$, which gives an extra power of two in the denominator, and $\frac{f(x,y,z)}{2^3}$ is an IVP.

From Chapters 5 and 6 we know that we cannot get the IVP $\frac{f(x,y,z)}{2^4}$, thus 2^3 is the biggest possible denominator. □

7.2.1 The Degree 8 Case

As mentioned previously, the case $m = 8$ is of interest, since three basis elements of $\mathrm{Int}^8(\mathbb{Z}^3, \mathbb{Z}_{(2)})$ will have a 2^4 in their denominator ,which does not happen in the 2-variable degree 8 case, i.e., there is no homogeneous degree 8 polynomial in two variables with denominator 2^4. Using $\mathbb{Z}/(4)\mathbf{P}^2$, it is possible to construct degree 8 homogeneous polynomials that have a 2^4 in the denominator. First we start with the product of seven linear factors, such that they reduce to the seven distinct lines in $\mathbb{F}_2\mathbf{P}^2$. No matter which triple from $\mathbb{Z}^3$ we take, we always have that at least 3 of these will evaluate to an even number. The main thing we are interested in here is how we can pick an extra 8-th factor in a way that we will add an extra factor of 2 when evaluating to a point.

For example, each line $L = (a, b, c)$ can be written as a linear factor $ax + by + cz$. The 28 lines in $\mathbb{Z}/(4)\mathbf{P}^2$ are: x, $x + 2z$, $x + 2y$, $x + 2y + 2z$, y, $y + 2z$, $2x + y$, $2x + y + 2z$, z, $2y + z$, $2x + z$, $2x + 2y + z$, $x + y$, $x + y + 2x$, $x + 3y$, $x + 3y + 2z$, $x + z$, $x + 3z$, $x + 2y + z$, $x + 2y + 3z$, $y + z$, $y + 3z$, $2x + y + z$, $2x + y + 3z$, $x + y + z$, $x + y + 3z$, $x + 3y + z$ and $x + 3y + 3z$.

Let f be the degree 7 homogeneous polynomial made of a product of the lines in $\mathbb{Z}/(4)\mathbf{P}^2$, which cover all the lines in $\mathbb{F}_2\mathbf{P}^2$, namely

$$f(x, y, z) = x \cdot y \cdot z \cdot (y + z) \cdot (x + z) \cdot (x + y) \cdot (x + y + z).$$

Since f modulo 2 consists of all the lines in $\mathbb{F}_2\mathbf{P}^2$, at any integer triple (a, b, c) three linear factors will be even. Thus $\frac{f}{2^3}$ is an IVP. The points on each line corresponding to a linear factor are the following:

L	Points in $\mathbb{Z}/(4)\mathbf{P}^2$ on L
x	(0,0,1), (0,2,1), (0,1,0), (0,1,2), (0,1,1), (0,1,3)
y	(0,0,1), (2,0,1), (1,0,0), (1,0,2), (1,0,1), (1,0,3)
z	(0,1,0), (2,1,0), (1,0,0), (1,2,0), (1,1,0), (3,1,0)
$y + z$	(0,1,3), (2,1,3), (1,0,0), (1,2,2), (1,1,3), (1,3,1)
$x + z$	(0,1,0), (2,1,2), (1,0,3), (1,2,3), (1,1,3), (1,3,3)
$x + y$	(0,0,1), (2,2,1), (3,1,0), (3,1,2), (1,3,1), (1,3,3)
$x + y + z$	(0,1,3), (2,1,1), (1,0,3), (1,2,1), (1,1,2), (3,1,0)

Table 7.1: Points on Seven Lines of $\mathbb{Z}/(4)\mathbf{P}^2$

Theorem 137. *The lines listed in Table 7.1 can be used to build a polynomial of* *degree 8, $h(x, y, z) \in \mathbb{Z}[x, y, z]$, such that $\frac{h}{2^4}$ is an IVP.*

Proof. By processing Table 7.1 , we get that $(1, 1, 1)$ is the only point that is not on any of the lines of those seven linear factors. Thus, to complete f to an IVP with denominator 2^4, we need only multiply by a linear factor which is even when evaluated at $(1, 1, 1)$. If we multiply f by g, a linear polynomial such that $g(1, 1, 1)$ is even, then the result will be an IVP when divided by 2^4. In that case $h = \frac{f \cdot g}{2^4}$ will be a homogeneous IVP. Out of the 28 possible linear factors coming from $\mathbb{Z}/(4)\mathbf{P}^2$, the following twelve will be even at $(1, 1, 1)$: $2x + y + 3z$, $y + z$, $y + 3z$, $2x + y + z$, $x + 2y + 3z$, $x + z$, $x + 3z$, $x + y + 2z$, $x + y$, $x + 3z$, $x + 3y + 2z$ and $x + 2y + z$. □

7.2.2 Building Higher Degree Homogeneous IVPs that Can Be Written as a Product of Linear Factors

The degree 14 case is of interest since from Chapter 5, we know we can obtain a polynomial with a 2^9 in its denominator. Since the degree 14 case corresponds to covering twice the Fano plane, we would like to construct an IVP with a 2^9 in its denominator from a set of lines in $\mathbb{Z}/(4)\mathbf{P}^2$ that covers the Fano plane twice. Various calculations were implemented in MAPLE, including grouping all 28 lines from $\mathbb{Z}/(4)\mathbf{P}^2$ into sets of congruent lines over $\mathbb{F}_2\mathbf{P}^2$ and picking two lines from each of the seven sets. Unfortunately, even when looking at all 6^7possible combinations of lines, the best we could get is a 2^8 in the denominator.

Since we cannot find a degree 14 polynomial with a 2^9 in its denominator, we turn our attention to the question: what is the biggest power of 2 we can have in a homogeneous IVP of a certain larger degree? We start with the case degree 28 and use the lifting from $\mathbb{Z}/(4)\mathbf{P}^2$ to $\mathbb{Z}/(8)\mathbf{P}^2$ to construct a degree 28 polynomial that is a product of homogeneous factors and is divisible by 2^{19}.

$\mathbb{Z}/(8)\mathbf{P}^2$ has 112 points and lines. We got MAPLE to randomly pick 28 lines from $\mathbb{Z}/(8)\mathbf{P}^2$ such that each line reduces to a different one over $\mathbb{Z}/(4)\mathbf{P}^2$. When these 28 lines cover the 112 points of $\mathbb{Z}/(8)\mathbf{P}^2$, we get a polynomial that is divisible by 2^{19}. An example of such a set of 28 lines is:

$(0,0,1)$, $(4,1,0)$, $(0,1,5)$, $(1,0,1)$, $(1,1,4)$, $(1,0,4)$, $(1,1,1)$, $(0,2,1)$, $(0,1,2)$, $(0,1,3)$, $(1,4,3)$, $(1,1,2)$, $(1,0,6)$, $(1,1,3)$, $(2,0,3)$, $(2,1,0)$, $(2,3,3)$, $(1,6,0)$, $(1,6,1)$, $(1,3,0)$, $(1,3,5)$, $(2,6,1)$, $(2,1,2)$, $(2,1,7)$, $(1,2,6)$, $(1,2,3)$, $(1,3,2)$, $(1,7,7)$

If we randomly pick a subset of 14 triples from the 28 above and find the corresponding degree 14 homogeneous polynomial. Some of these polynomials are actually divisible by 2^8 and still produce an IVP. Since 2^9 is not attainable through a product of linear factors, this is the biggest possible denominator we can get. An example of this set is:

$(0,1,5)$, $(1,1,4)$, $(1,1,1)$, $(0,1,3)$, $(1,4,3)$, $(1,0,6)$, $(1,1,3)$, $(2,0,3)$, $(2,1,0)$, $(1,6,0)$, $(2,6,1)$, $(2,1,2)$, $(1,2,3)$, $(1,3,2)$.

These lines cover twice the Fano plane.

Proposition 138. *When taking 28 lines from $\mathbb{Z}/(8)\mathbf{P}^2$ that cover all 112 points of $\mathbb{Z}/(8)\mathbf{P}^2$, one can build homogeneous IVPs with a 2^{19} in their denominators.*

Proof. Write each line as a linear factor f_i. We can then take $f = \prod f_i$ which gives a degree 28 homogeneous polynomial.

We consider $(a,b,c) \in \mathbb{Z}^3$ such that at least one of a,b,c is odd. Otherwise $2^{28}|f(a,b,c)$. Up to multiplication by a unit in $\mathbb{Z}/(8)$, $(a,b,c) \in \mathbb{Z}/(8)\mathbf{P}^2$, since we could pick 28 lines that covered all of $\mathbb{Z}/(8)\mathbf{P}^2$. Thus $f(a,b,c) \equiv 0 \pmod 8$, and we get from this a 2^3 in the denominator that is guaranteed.

(a,b,c) is a point on six lines over $\mathbb{Z}/(4)\mathbf{P}^2$, since the 28 lines we picked reduce to $\mathbb{Z}/(4)\mathbf{P}^2$. Thus $f_i(a,b,c) \equiv 0 \pmod 4$ for 6 f_is. Since one of these was counted above, our denominator is now $2^3 \cdot (2^2)^5$.

(a, b, c) is a point on three lines over $\mathbb{F}_2\mathbf{P}^2$, and we have four lines that cover all of these over $\mathbb{F}_2\mathbf{P}^2$. Six of these were already counted, so our denominator is now

$$2^3 \cdot 2^{10} \cdot 2^6 = 2^{19}.$$

□

The very useful thing that happened over $\mathbb{Z}/(8)\mathbf{P}^2$ was that we could find 28 lines that reduced to all of $\mathbb{Z}/(4)\mathbf{P}^2$ and covered all 112 points of $\mathbb{Z}/(8)\mathbf{P}^2$. That was not possible when picking seven lines over $\mathbb{Z}/(4)\mathbf{P}^2$ that cover the Fano plane. Therefore this will affect our denominator when we generalize by a factor of 2. We will assume that we do not have that property for the remainder of the section.

Suppose we make up a degree 112 polynomial where the factors are made from lines over $\mathbb{Z}/(16)\mathbf{P}^2$ that reduce to all lines over $\mathbb{Z}/(8)\mathbf{P}^2$. Each point (a, b, c) is on 12 lines, so $f_i(a, b, c) \equiv 0 \pmod 8$ for 12 values i, which gives us a $(2^3)^{12}$ in the denominator.

Over $\mathbb{Z}/(4)\mathbf{P}^2$ each point is on six lines and is covered four times. Half of these were already counted, so multiply by $(2^2)^{12}$ in the denominator. Over $\mathbb{F}_2\mathbf{P}^2$ each point is on three lines and is covered eight times. Removing those that are counted already, we can multiply the denominator by 2^{12}. Therefore

$$\frac{\prod_{i=1}^{112} f_i}{2^{36}2^{24}2^{12}}$$

is a degree 112 homogeneous IVP.

Corollary 139. *When taking $7 \cdot 2^{2k-2}$ lines over $\mathbb{Z}/(2^{k+1})\mathbf{P}^2$ that reduce to all the lines of $\mathbb{Z}/(2^k)\mathbf{P}^2$, one can build homogeneous IVPs with*

$$(2^k)^{3 \cdot 2^{k-1}} \cdot (2^{k-1})^{3 \cdot 2^{k-1}} \cdots (2)^{3 \cdot 2^{k-1}}$$

in their denominators.

Proof. This is obtained by generalizing Proposition 138 as described for the degree 112 case. □

So we have that

$$\nu_2(f(a,b,c)) \geq \left(\sum_{i=0}^{k+1} 3i\right) \cdot 2^k = 3 \cdot 2^k \cdot \frac{(k+1)(k+2)}{2}.$$

As k approaches infinity, this expression divided by the degree of the polynomial, is $\frac{3(k+1)(k+2)}{7 \cdot 2^{k-3}}$, which approaches 0. (Even if we get an extra power of two from covering all points in the plane, the limit is still 0.) Thus this approach is not optimal.

7.3 Statement of the Correspondence

We can use finite projective H-planes to produce IVPs, but they are dependent on coverings of those planes, which means we cannot obtain full bases using this technique. The polynomials we produce do have the nice property of factoring as a product of linear factors.

Theorem 140. *There is a one-to-one correspondence between products of m lines in $\mathbb{Z}/(2^k)\mathbf{P}^2$ and homogeneous IVPs of degree m that completely factor with denominator 2^h, where h depends on the number of coverings of $\mathbb{Z}/(2^k)\mathbf{P}^2$ that the lines achieve.*

Proof. We want to show the duality between

$$f = \prod_{i=1}^{m}(a_i x + b_i y + c_i z),$$

where $(a_i, b_i, c_i) \in \mathbb{Z}/(2^k)\mathbf{P}^2$, and

$$g = \frac{1}{2^h}\prod_{j=1}^{m}(a_j x + b_j y + c_j z),$$

where $(a_i, b_i, c_i) \in \mathbb{Z}/(2^h)^3$. Note that (a_j, b_j, c_j) are not all even; otherwise we would cancel a 2 in the denominator.

First, suppose that f comes from a set of lines that fully covers $\mathbb{Z}/(2^k)\mathbf{P}^2$ once, that is, one that reduces exactly to all lines in $\mathbb{Z}/(2^{k-1})\mathbf{P}^2$.

Then by Corollary 139 we have

$$2^h = (2^k)^{3\cdot 2^{k-1}} \cdot (2^{k-1})^{3\cdot 2^{k-1}} \cdots (2)^{3\cdot 2^{k-1}}.$$

Now if f comes from a set of lines that fully covers $\mathbb{Z}/(2^k)\mathbf{P}^2$ in such a way that it reduces to ℓ coverings of $\mathbb{Z}/(2^{k-1})\mathbf{P}^2$, then

$$2^h = ((2^k)^{3\cdot 2^{k-1}} \cdot (2^{k-1})^{3\cdot 2^{k-1}} \cdots (2)^{3\cdot 2^{k-1}})^{\ell}.$$

In the case of f not being a full covering of $\mathbb{Z}/(2^k)\mathbf{P}^2$, proceed in the following recursive way. Find the largest k_1 such that ℓ_1 coverings of $\mathbb{Z}/(2^{k_1-1})\mathbf{P}^2$ can be obtained. Let the polynomial corresponding to this set be f_1. Then

$$2^{h_1} = ((2^{k_1})^{3\cdot 2^{k_1-1}} \cdot (2^{k_1-1})^{3\cdot 2^{k_1-1}} \cdots (2)^{3\cdot 2^{k_1-1}})^{\ell_1}.$$

Repeat this process with $\frac{f}{f_1}$ until no coverings of the Fano plane are possible. Then $h = \sum_{n=1} h_n \cdot \ell_n$, that is the resulting h will be the sum of the $h_n \cdot \ell_n$ obtained at each iteration. □

Corollary 141. *Consider f as in Theorem 140, such that k is the largest integer for which the linear factors of f fully cover $\mathbb{Z}/(2^k)\mathbf{P}^2$ ℓ times. Then h from Theorem 140 is bounded by*

$$\ell(2^{k+1} - 2) \leq h < m.$$

Proof. For ℓ coverings of $\mathbb{Z}/(2^k)\mathbf{P}^2$ we know that at any triple in $\mathbb{Z}/(2^k)\mathbf{P}^2$ one of the linear factors will be congruent to 0 (mod 2^k), and that will be the case for $i < k$.

Thus

$$\ell \sum_{i=1}^{k} 2^i \leq h < m,$$
$$\ell(2^{k+1} - 2) \leq h < m.$$

□

7.4 Using the Projective Plane for the 2-Variable Case

Starting over $\mathbb{Z}_{(2)}$, we can list the pairs that respect the same rules as the triples of the projective plane, namely $(0,1),\ (1,1),\ (1,0)$. These are all the linear 2-variable polynomials we can make and the different points at which we can evaluate them. When taking the dot product of these, we get what happens when evaluating our linear factors at a given point. The table below displays a 1 if the dot product is even, and a 0 if it is odd:

	(0,1)	(1,1)	(1,0)
(0,1)	0	0	1
(1,1)	0	1	0
(1,0)	1	0	0

Table 7.2: Parity of Dot Products of $\mathbb{F}_2\mathbf{P}^1$

In order to introduce a 2 in the denominator of a homogeneous polynomial, we need to pick a subset of three columns such that we have a 1 in each row. In this case that is the three columns, which gives a polynomial of degree 3.

When repeating this process over $\mathbb{Z}/(4)$, we obtain the table below where a 0 entry indicates that the dot product of the pairs is odd, 1 that it is congruent to 2 (mod 4) and 2 that it is congruent to 0 (mod 4):

	(0,1)	(1,1)	(1,0)	(2,1)	(3,1)	(1,2)
(0,1)	0	0	2	0	0	1
(1,1)	0	1	0	0	2	0
(1,0)	2	0	0	1	0	0
(2,1)	0	0	1	0	0	2
(3,1)	0	2	0	0	1	0
(1,2)	1	0	0	2	0	0

Table 7.3: 2-Valuation of Dot Products of $\mathbb{Z}/(4)\mathbf{P}^1$

If we try picking a subset of columns such that we always get a 2 in each row, we will always get an extra 1. Hence with a degree 6 polynomial we always get a 2^3 in the denominator.

When repeating this process over $\mathbb{Z}/(8)$, we obtain the table below where a 0 entry indicates that the dot product of the pairs is odd, 1 that it is congruent to 2 (mod 8), 2 that it is congruent to $4 \pmod 8$ and 3 that it is congruent to $0 \pmod 8$:

	(0,1)	(1,1)	(1,0)	(2,1)	(3,1)	(1,2)	(4,1)	(5,1)	(1,4)	(6,1)	(7,1)	(1,6)
(0,1)	0	0	3	0	0	1	0	0	2	0	0	1
(1,1)	0	1	0	0	2	0	0	1	0	0	3	0
(1,0)	3	0	0	1	0	0	2	0	0	1	0	0
(2,1)	0	0	1	0	0	2	0	0	1	0	0	3
(3,1)	0	2	0	0	1	0	0	3	0	0	1	0
(1,2)	1	0	0	2	0	0	1	0	0	3	0	0
(4,1)	0	0	2	0	0	1	0	0	3	0	0	1
(5,1)	0	1	0	0	3	0	0	1	0	0	2	0
(1,4)	2	0	0	1	0	0	3	0	0	1	0	0
(6,1)	0	0	1	0	0	3	0	0	1	0	0	2
(7,1)	0	3	0	0	1	0	0	2	0	0	1	0
(1,6)	1	0	0	3	0	0	1	0	0	2	0	0

Table 7.4: 2-Valuation of Dot Products of $\mathbb{Z}/(8)\mathbf{P}^1$

When wanting to get a 2^4 in the denominator, we do not need all 12 linear factors here. We see that a subset of nine columns is sufficient. By picking subsets of 10 or 11 columns, we still get that we can only put a 2^4 in the denominator. The next power we get is 2^7, which corresponds to degree 12, since all the rows (and columns) add to 7.

Note that all the above matrices are doubly stochastic.

Chapter 8

Conclusion

In this thesis we explored ways of finding bases for the 3-variable homogeneous integer-valued polynomials using two different approaches. First we developed computational tools that used linear algebra to generate bases for the polynomials in Chapters 5 and 6, and second, we studied the correspondence with a covering of lines in finite H-plane for a constructive approach demonstrated in Chapter 7.

Given the corresponding problem in algebraic topology, described in Chapter 3, it is not surprising that finding bases for the 3-variable case is a more difficult problem than the 2-variable case. In this thesis we did find methods that produce 3-variable homogeneous IVPs, but finding more efficient algorithms would be necessary to obtain bases for degrees greater than 25. These would help when trying to generalize to more variables, since the matrices we would work with would be much bigger. A promising approach for this would be to implement local version of the Hermite normal form and Smith normal form. These would produce the same output we are looking for here, but, by focusing on a single prime of interest, the calculations would be faster.

A broader goal is to get the basis elements obtained in Chapter 5 and 6 written with as few terms as possible and written as almost a product of linear factors to better understand how these polynomials arise. Ideally, we would have a recursive construction for constructing homogeneous IVPs of any degree and even any number of variables.

In Chapters 4, 5, 6 and 7 of this thesis we worked locally, that we were interested in the highest power of 2 that could be in the denominators of the basis elements. The results from Chapter 6, were generalized to odd primes. It would be of interest to use all the local results to get bases for homogeneous IVPs integrally.

The broader goal of this work is to develop efficient tools for calculating bases of IVPs on various subsets of $\mathbb{Z}^n$ in the general and homogeneous cases. There are various ways of studying these; one of which is through the valuative capacity, which is an invariant of the set of IVPs. An example of this can be found in [B.L17], where the valuative capacity of the set of sums of d^{th} powers is calculated.

This thesis displays many results about homogeneous IVPs, yet there is much more to be found. Hopefully these results can be used as a starting point for the case homogeneous 3-variables and for more variables.

Bibliography

[Ada58] J. F. Adams, *On the structure and applications of the Steenrod algebra*, Comment. Math. Helv. **32** (1958), 180–214.

[AHS71] J. F. Adams, A. Harris, and R. Switzer, *Hopf algebras of cooperations for real and complex K-theory*, Proc. London Math. Soc. **23** (1971), 385–408.

[AGP02] M. Aguilar, S. Gitler, and C. Prieto, *Algebraic Topology from a Homotopical Viewpoint*, Springer-Verlag New York, 2002.

[AS68] A. Albert and R. Sandler, *An Introduction to Finite Projective Planes*, Holt, Rinehart and Winston, New York-Toronto, Ont.-London, 1968.

[Ayr67] F. Ayres, *Theory and Problems of Projective Geometry*, Schaum Publishing Co., New York, 1967.

[B.L17] M. B.Langlois, *The valuative capacity of the set of sums of d^{th} powers*, J. Number Theory **171** (2017), 155–168.

[BCRS89] A. Baker, F. Clarke, N. Ray, and L. Schwartz, *On the Kummer congruences and the stable homotopy of BU*, Trans. Amer. Math. Soc. **316** (1989), 385–432.

[BR10] M. Baker and R. Rumely, *Potential Theory and Dynamics on the Berkovich Projective Line*, Vol. 159, Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2010.

[Bha97] M. Bhargava, *p-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew. Math. **490** (1997), 101–127.

[Bha00] ______, *The factorial function and generalizations.*, Amer. Math. Monthly **107** (2000), 783–799.

[Bro93] W. Brown, *Matrices over Commutative Rings*, Marcel Dekker, Inc., New York, 1993.

[CC97] P.-J. Cahen and J.-L. Chabert, *Integer-valued Polynomials*, Vol. 48, American Mathematical Society, Providence, Providence, RI, 1997.

[Cha14] J. Chabert, *Integer-Valued Polynomials: Looking for Regular Bases (a Survey)*, Commutative algebra (2014), 83–111.

[Cla81] F. Clarke, *Self maps of BU*, Math. Proc. Cambridge Philos. Soc. **89** (1981), 491–500.

[DF04] D. Dummit and R. Foote, *Abstract Algebra.*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[Evr12] S. Evrard, *Bhargava's factorials in several variables*, J. Algebra **372** (2012), 134–148.

[GM02] S. Goldwasser and D. Micciancio, *Complexity of Lattice Problems, A Cryptographic Perspective*, Vol. 671, Kluwer Academic Publishers, Boston, MA, 2002.

[GKP98] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, Reading, MA, 1998.

[Hub97] J. Hubbuck, *Numerical Forms*, J. London Math. Soc. **55** (1997), 65–75.

[JP11] K. Johnson and D. Patterson, *Projective p-orderings and homogeneous integer-valued polynomials*, Integers, 11 (2011), 597–604.

[Joh14] K. Johnson, *Stable Homotopy Theory, Formal Group Laws, and Integer-Valued Polynomials*, Commutative algebra (2014), 213–223.

[Kle59] E. Kleinfeld, *Finite Hjelmslev Planes*, Illinois J. Math **3** (1959), 403–407.

[Kli54] W. Klingenberg, *Projektive und affine Ebenen mit Nachbarelementen*, Math. Z. **60** (1954), 384–406.

[Kie] M. Kiermair, *Dr. Michael Kiermaier*, `http://www.mathe2.uni-bayreuth.de/michaelk/`. Accessed April 20, 2018.

[Leg30] A. M. Legendre, *Théorie des Nombres.*, Paris: Firmin Didot Frères (1830).

[Mic16a] D. Micciancio, *Lecture notes for CSE 206A: Lattice Algorithms and Applications: Introduction* (2016), `https://cseweb.ucsd.edu/classes/wi10/cse206a/lec1.pdf`.

[Mic16b] ———, *Lecture notes for CSE 206A: Lattice Algorithms and Applications: Basic Algorithms* (2016), `https://cseweb.ucsd.edu/classes/wi10/cse206a/lec2.pdf`.

[Mol12] V. Moll, *Numbers and Functions*, American Mathematical Society, Providence, Providence, RI, 2012.

[Nor12] C. Norman, *Finitely Generated Abelian Groups and Similarity of Matrices over a Field*, Springer Undergraduate Mathematics Series, 2012.

[Nov67] S. Novikov, *Methods of algebraic topology from the point of view of cobordism theory*, Izv. Akad. Nauk SSSR Ser. Mat. (in Russian) **31** (1967), 855–951.

[OEIS] *On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`. Accessed April 19, 2018.

[Rav86] D. Ravenel, *Complex Cobordism and Stable Homotopy Groups of Spheres*, Vol. 121, Academic Press, Orlando, FL, 1986.

[Sch86] A. Schrijver, *Theory of Linear and Integer Programming*, John Wiley & Sons, Ltd, 1986.

[vLW01] J. van Lint and .R. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge University Press, New York, 2001.

[Veb04] O. Veblen, *A system of axioms for geometry*, Trans. Amer. Math. Soc. **5** (1904), 343–384.

Appendix A

Examples of Bases Calculations

Below is a table that displays bases for degrees 1 to 7 using the technique described in Chapter 6.

For degrees 8 to 14 we only display one of the polynomials with largest denominator, since the full basis would be too large.

m	Basis
1	x, y, z
2	x^2, xy, xz, y^2, yz, z^2
3	x^3, x^2y, zx^2, $\frac{-1}{2}x^2y+\frac{1}{2}xy^2$, zxy, $\frac{-1}{2}zx^2+\frac{1}{2}z^2x$, y^3, zy^2, $\frac{-1}{2}zy^2+\frac{1}{2}z^2y$, z^3
4	x^4, x^3y, zx^3, $\frac{-1}{2}x^3y+\frac{1}{2}x^2y^2$, zx^2y, $\frac{-1}{2}zx^3+\frac{1}{2}z^2x^2$, $\frac{-1}{2}x^3y+\frac{1}{2}xy^3$, $\frac{-1}{2}zx^2y+\frac{1}{2}zxy^2$, $\frac{-1}{2}zx^2y+\frac{1}{2}z^2xy$, $\frac{-1}{2}zx^3+\frac{1}{2}z^3x$, y^4, zy^3, $\frac{-1}{2}zy^3+\frac{1}{2}z^2y^2$, $\frac{-1}{2}zy^3+\frac{1}{2}z^3y$, z^4
5	x^5, x^4y, zx^4, $\frac{-1}{2}x^4y+\frac{1}{2}x^3y^2$, zx^3y, $\frac{-1}{2}zx^4+\frac{1}{2}z^2x^3$, $\frac{-1}{2}x^4y+\frac{1}{2}x^2y^3$, $\frac{-1}{2}zx^3y+\frac{1}{2}zx^2y^2$, $\frac{-1}{2}zx^3y+\frac{1}{2}z^2x^2y$, $\frac{-1}{2}zx^4+\frac{1}{2}z^3x^2$, $\frac{-1}{2}x^4y+\frac{1}{2}xy^4$, $\frac{-1}{2}zx^3y+\frac{1}{2}zxy^3$, $\frac{-1}{2}zx^3y+\frac{1}{2}z^2xy^2$, $\frac{-1}{2}zx^3y+\frac{1}{2}z^3xy$, $\frac{-1}{2}zx^4+\frac{1}{2}z^4x$, y^5, zy^4, $\frac{-1}{2}zy^4+\frac{1}{2}z^2y^3$, $\frac{-1}{2}zy^4+\frac{1}{2}z^3y^2$, $\frac{-1}{2}zy^4+\frac{1}{2}z^4y$, z^5
6	x^6, x^5y, zx^5, $\frac{-1}{2}x^5y+\frac{1}{2}x^4y^2$, zx^4y, $\frac{-1}{2}zx^5+\frac{1}{2}z^2x^4$, $\frac{-1}{2}x^5y+\frac{1}{2}x^3y^3$, $\frac{-1}{2}zx^4y+\frac{1}{2}zx^3y^2$, $\frac{-1}{2}zx^4y+\frac{1}{2}z^2x^3y$, $\frac{-1}{2}zx^5+\frac{1}{2}z^3x^3$, $\frac{-1}{4}x^4y^2+\frac{1}{4}x^2y^4$, $\frac{-1}{2}zx^4y+\frac{1}{2}zx^2y^3$, $\frac{1}{4}zx^4y-\frac{1}{4}zx^3y^2-\frac{1}{4}z^2x^3y+\frac{1}{4}z^2x^2y^2$, $\frac{-1}{2}zx^4y+\frac{1}{2}z^3x^2y$, $\frac{-1}{4}z^2x^4+\frac{1}{4}z^4x^2$, $\frac{-1}{4}x^5y+\frac{1}{8}x^4y^2-\frac{1}{8}x^2y^4+\frac{1}{4}xy^5$, $\frac{-1}{2}zx^4y+\frac{1}{2}zxy^4$, $\frac{3}{4}zx^4y-\frac{1}{4}zx^3y^2-\frac{1}{4}z^2x^3y-\frac{1}{4}zx^2y^3-\frac{1}{4}zxy^4+\frac{1}{4}z^2xy^3$, $\frac{1}{4}zx^4y-\frac{1}{4}z^3x^2y-\frac{1}{4}zxy^4+\frac{1}{4}z^3xy^2$, $\frac{1}{2}zx^4y-\frac{1}{4}zx^3y^2-\frac{1}{4}z^2x^3y-\frac{1}{4}zxy^4+\frac{1}{4}z^4xy$, $\frac{-1}{4}zx^5+\frac{1}{8}z^2x^4-\frac{1}{8}z^4x^2+\frac{1}{4}z^5x$, y^6, zy^5, $\frac{-1}{2}zy^5+\frac{1}{2}z^2y^4$, $\frac{-1}{2}zy^5+\frac{1}{2}z^3y^3$, $\frac{-1}{4}z^2y^4+\frac{1}{4}z^4y^2$, $\frac{-1}{4}zy^5+\frac{1}{8}z^2y^4-\frac{1}{8}z^4y^2+\frac{1}{4}z^5y$, z^6
7	x^7, x^6y, zx^6, $\frac{-1}{2}x^6y+\frac{1}{2}x^5y^2$, zx^5y, $\frac{-1}{2}zx^6+\frac{1}{2}z^2x^5$, $\frac{-1}{2}x^6y+\frac{1}{2}x^4y^3$, $\frac{-1}{2}zx^5y+\frac{1}{2}zx^4y^2$, $\frac{-1}{2}zx^5y+\frac{1}{2}z^2x^4y$, $\frac{-1}{2}zx^6+\frac{1}{2}z^3x^4$, $\frac{-1}{2}zx^5y+\frac{1}{2}zx^3y^3$, $\frac{1}{4}x^6y-\frac{1}{8}x^5y^2-\frac{1}{4}x^4y^3+\frac{1}{8}x^3y^4$, $\frac{1}{4}zx^5y-\frac{1}{4}zx^4y^2-\frac{1}{4}z^2x^4y+\frac{1}{4}z^2x^3y^2$, $\frac{-1}{2}zx^5y+\frac{1}{2}z^3x^3y$, $\frac{1}{4}zx^6-\frac{1}{8}z^2x^5-\frac{1}{4}z^3x^4+\frac{1}{8}z^4x^3$, $\frac{-1}{4}x^4y^3+\frac{1}{4}x^2y^5$, $\frac{-1}{4}zx^4y^2+\frac{1}{4}zx^2y^4$, $\frac{1}{4}zx^5y-\frac{1}{4}z^2x^4y-\frac{1}{4}zx^3y^3+\frac{1}{4}z^2x^2y^3$, $\frac{-1}{4}z^3x^4+\frac{1}{4}z^5x^2$, $\frac{1}{2}zx^5y+\frac{1}{8}zx^4y^2-\frac{1}{8}z^2x^4y-\frac{1}{4}zx^3y^3-\frac{1}{4}z^3x^3y-\frac{1}{8}zx^2y^4+\frac{1}{8}z^4x^2y$, $\frac{-1}{4}x^5y^2+\frac{1}{8}x^4y^3-\frac{1}{8}x^2y^5+\frac{1}{4}xy^6$, $\frac{1}{4}zx^5y-\frac{1}{4}zx^4y^2-\frac{1}{4}z^3x^3y+\frac{1}{4}z^3x^2y^2$, $\frac{1}{2}zx^5y-\frac{1}{8}zx^4y^2-\frac{1}{4}z^2x^4y-\frac{1}{4}zx^3y^3-\frac{1}{8}zx^2y^4+\frac{1}{4}z^2xy^4$, $\frac{-1}{4}zx^5y+\frac{1}{8}zx^4y^2-\frac{1}{8}zx^2y^4+\frac{1}{4}zxy^5$, $\frac{1}{8}zx^4y^2-\frac{1}{4}z^3x^3y-\frac{1}{8}zx^2y^4+\frac{1}{4}z^3xy^3$, $\frac{1}{2}zx^5y-\frac{1}{4}zx^3y^3-\frac{1}{4}z^3x^3y-\frac{1}{8}z^2xy^4+\frac{1}{8}z^4xy^2$, y^7, zy^6, $\frac{-1}{2}zy^6+\frac{1}{2}z^3y^4$, $\frac{1}{4}zx^5y+\frac{1}{8}zx^4y^2-\frac{1}{4}zx^3y^3-\frac{1}{4}z^3x^3y-\frac{1}{8}zx^2y^4+\frac{1}{4}z^5xy$, $\frac{-1}{4}z^2x^5+\frac{1}{8}z^3x^4-\frac{1}{8}z^5x^2+\frac{1}{4}z^6x$, $\frac{1}{4}zy^6-\frac{1}{8}z^2y^5-\frac{1}{4}z^3y^4+\frac{1}{8}z^4y^3$, $\frac{-1}{4}z^3y^4+\frac{1}{4}z^5y^2$, $\frac{-1}{4}z^2y^5+\frac{1}{8}z^3y^4-\frac{1}{8}z^5y^2+\frac{1}{4}z^6y$, z^7

m	Polynomial with Biggest Denominator
8	$\frac{-1}{2}zx^6y+\frac{3}{16}zx^5y^2+\frac{3}{16}z^2x^5y+\frac{3}{8}zx^4y^3+\frac{1}{8}z^3x^4y-\frac{1}{16}zx^3y^4-\frac{1}{8}z^2x^3y^3-\frac{1}{8}z^3x^3y^2-\frac{1}{16}z^4x^3y-\frac{1}{16}z^2x^2y^4+\frac{1}{16}z^4x^2y^2$
9	$\frac{-1}{8}zx^7y+\frac{1}{16}zx^6y^2+\frac{3}{8}zx^5y^3+\frac{1}{16}z^2x^5y^2-\frac{1}{4}z^3x^5y-\frac{1}{16}zx^4y^4-\frac{1}{8}z^2x^4y^3-\frac{1}{16}z^2x^3y^4+\frac{1}{8}z^6x^2y$
10	$\frac{1}{8}zx^8y-\frac{3}{16}zx^7y^2-\frac{3}{32}zx^6y^3+\frac{3}{32}z^2x^6y^2+\frac{1}{8}z^3x^6y+\frac{3}{32}zx^5y^4+\frac{3}{32}z^2x^5y^3-\frac{1}{32}zx^4y^5-\frac{1}{16}z^3x^4y^3-\frac{1}{32}z^4x^4y^2+\frac{1}{32}zx^3y^6-\frac{1}{32}z^2x^3y^5-\frac{3}{32}z^2x^2y^6-\frac{1}{16}z^3x^2y^5+\frac{1}{32}z^4x^2y^4$
11	$\frac{1}{8}z^2x^8y-\frac{3}{32}zx^7y^3+\frac{1}{32}z^2x^7y^2+\frac{1}{8}z^3x^7y+\frac{1}{32}zx^6y^4-\frac{3}{32}z^2x^6y^3+\frac{3}{32}zx^5y^5-\frac{1}{8}z^3x^5y^3-\frac{1}{32}z^4x^5y^2-\frac{1}{32}zx^4y^6-\frac{1}{32}z^2x^4y^5-\frac{1}{32}z^2x^3y^6+\frac{1}{32}z^4x^3y^4$
12	$\frac{-3}{8}x^{11}y+\frac{3}{32}x^{10}y^2+\frac{9}{32}x^9y^3-\frac{7}{128}x^8y^4+\frac{1}{32}x^7y^5-\frac{1}{64}x^6y^6-\frac{1}{32}x^5y^7+\frac{1}{128}x^4y^8-\frac{1}{32}x^3y^9-\frac{1}{32}x^2y^{10}+\frac{1}{8}xy^{11}$
13	$\frac{-1}{8}zx^{12}+\frac{1}{32}z^2x^{11}+\frac{5}{32}z^3x^{10}-\frac{1}{128}z^4x^9-\frac{3}{64}z^6x^7-\frac{1}{32}z^7x^6-\frac{1}{128}z^8x^5+\frac{1}{32}z^{10}x^3$
14	$\frac{11}{256}x^3y^5z^6-\frac{1}{256}x^2y^6z^6+\frac{23}{128}xy^8z^5-\frac{3}{64}xy^5z^8+\frac{3}{512}x^2y^8z^4+\frac{1}{8}x^2y^{11}z-\frac{1}{256}x^3y^6z^5-\frac{21}{64}x^3y^2z^9-\frac{121}{512}x^2y^4z^8+\frac{1}{128}xy^4z^9-\frac{1}{32}xy^{11}z^2+\frac{1}{256}x^3y^3z^8-\frac{7}{64}x^2y^9z^3+\frac{1}{64}xy^7z^6-\frac{15}{256}x^3y^8z^3-\frac{121}{128}x^4yz^9-\frac{1}{512}x^4y^2z^8-\frac{1}{256}x^4y^5z^5-\frac{1}{512}x^4y^8z^2+\frac{1}{128}x^4y^9z-\frac{1}{128}x^5yz^8-\frac{1}{256}x^5y^3z^6+\frac{1}{256}x^5y^4z^5+\frac{9}{256}x^5y^5z^4+\frac{3}{256}x^5y^6z^3-\frac{19}{32}x^5y^7z^2-\frac{11}{128}x^5y^8z-\frac{1}{256}x^6y^2z^6-\frac{35}{256}x^6y^3z^5+\frac{11}{64}x^6y^4z^4+\frac{1}{256}x^6y^5z^3+\frac{579}{256}x^6y^6z^2+\frac{1}{128}x^8yz^5+\frac{27}{512}x^8y^2z^4-\frac{1}{256}x^8y^3z^3+\frac{3}{512}x^8y^4z^2-\frac{25}{128}x^8y^5z-\frac{23}{128}x^9yz^4+\frac{1}{64}x^9y^3z^2+\frac{3}{128}x^9y^4z$

Appendix B

MAPLE Code

Useful computations for this work and how they were implemented are appended in the follwoing pages. The following code is present:

1. The code for Chapter 5, calculations using Smith normal form.

2. The code for Chapter 6, calculations using Hermite normal form.

3. Code that generates $\mathbb{Z}/_{(2^k)}\mathbf{P}^2$, and groups the points given what they are congruent to over $\mathbb{F}_2\mathbf{P}^2$, for calculations in Chapter 7.

4. Code for Chapter 7 that shows that the degree 14 polynomial with a 2^9 in its denominator does not factor as a product of linear factor.

```
> #Code that shows that taking the SNF of the matrix of Stirling coefficients, creates IVPs.
> #Upload the necessary packages for the computations and allow the display of big matrices.
> with(combinat) : with(linalg) : with(LinearAlgebra) : with(padic) : interface(rtablesize = 110) :
        with(ListTools) :
>
>  #Given as input a list L and a value a this procedure counts the number of entries in L equal to a
  num ≔ proc(a, L) local i, c; c ≔ 0;for i from 1 to nops(L) do if L[i] = a then c ≔ c + 1 else
        fi; od ; c;end:
>
> # Establish p, the prime we are working at, q the maximum degree we want the calculation to go
        for, and create an empty list LL.
  p ≔ 2 :
   LL ≔ [ ]:
   q ≔ 14 :

   # repeat the process for degress 1 to q
   for n from 1 to q do

   M ≔ Matrix((n + 1) * (n + 2) / 2, (n + 1) * (n + 2) * (n + 3) / 6) :
  # Builds the matrix M, which will have the coefficients of our monomials, written as a product of
        factorials and Stirling numbers of the second kind,  since we are storing values of triples (i,j,k)
         <=(r,s,t), in  matrix we need more loops.

   cr ≔ 0 : for rs from 0 to n do
   for r from 0 to rs do
   s ≔ rs − r; t ≔ n − rs;
   cr ≔ cr + 1 : cc ≔ 0 :
   for ijk from 0 to n do
   for ij from 0 to ijk do
   for i from 0 to ij do
   j ≔ ij − i; k ≔ ijk − ij;
   cc ≔ cc + 1;
   M[cr, cc] ≔ (i!)·(j!)·(k!)·stirling2(r, i) * stirling2(s, j) * stirling2(t, k) :
   M;
   od;od;od;
   od;od;

   # Returns S,U,V, the Smith Normal form of M.
  S ≔ ismith(M, U, V);
  L ≔ [ ]:


   # Stores the p-adic norms of the diagonal of S in the list L.
  for i from 1 to (n + 1)·(n + 2)/2 do
   L ≔ [op(L), ordp(S[i, i], p)] :od:

   # appends L to LL, which will contain the p-adic norms of the basis elements for degrees 1 to q.
```

```
LL := [op(LL), L];
od:

#At this point we are done looping from degrees 1 to q.


    # Create a matrix N which is table 5.2 in the thesis, where for degree i, N[i,j], is how many
    basis elements have denominators with 2-adic norm j.
N := Matrix(q, q) :
#Note that the second q in the dimension could be smaller since we get columns of zeros.
for i from 1 to q do for j from 0 to (q - 1) do
N[i, j + 1] := num(j, LL[i]);od;od;
N;
```

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 6 & 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 21 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 28 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 28 & 14 & 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 28 & 14 & 6 & 15 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 7 & 14 & 28 & 14 & 7 & 25 & 3 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \textbf{(1)}$$

```
> #The next section shows how to extract polynomials, from the Smith normal form by using the
    matrix U above. We will illustrate this for degree 14, and by looking at the last row of N above
    we know we have a basis element with a 2^9 in its denominator.
```

```
> #V is a vector of coefficients of the polynomials of degree 14 with a 2^9 in its denominator.
V := Row(eval(U), 120);
```

$$V := \begin{bmatrix} \text{1 .. 120 } \mathit{Vector}_{row} \\ \text{Data Type: anything} \\ \text{Storage: rectangular} \\ \text{Order: Fortran\_order} \end{bmatrix} \qquad \textbf{(2)}$$

```
> #We reduce these coefficient mod 2^9, to make the polynomial easier to display.
Vmod := [ ]:
for i in V do: Vmod := [op(Vmod),mod(i, 2^9)]:
```

```
od:
Vmod;
```

$$[0, 256, 0, 64, 384, 128, 192, 72, 40, 256, 304, 72, 488, 272, 32, 416, 262, 476, 444, 382, 352, 272, 354, 31, 14, 337, 252, 160, 320, 468, 264, 316, 192, 204, 340, 64, 272, 396, 370, 46, 296, 462, 174, 136, 224, 32, 38, 456, 390, 178, 430, 258, 248, 430, 352, 304, 210, 247, 120, 148, 146, 404, 388, 257, 380, 96, 64, 216, 300, 330, 40, 262, 122, 232, 306, 248, 440, 0, 320, 88, 120, 420, 177, 496, 450, 36, 93, 400, 504, 48, 384, 256, 64, 168, 256, 86, 188, 476, 304, 126, 260, 8, 400, 32, 0, 0, 0, 128, 256, 480, 64, 0, 0, 96, 64, 64, 128, 256, 0, 0] \tag{3}$$

> *#Divide the coefficients by* 2^9, *since we want an IVP with* 2^9 **in** *its denominator.*

```
V := [ ];
for i in Vmod do: V := [op(V), i·1/2^9]:
od:
V;
```

$$V := [\ ]$$

$$\left[0, \frac{1}{2}, 0, \frac{1}{8}, \frac{3}{4}, \frac{1}{4}, \frac{3}{8}, \frac{9}{64}, \frac{5}{64}, \frac{1}{2}, \frac{19}{32}, \frac{9}{64}, \frac{61}{64}, \frac{17}{32}, \frac{1}{16}, \frac{13}{16}, \frac{131}{256}, \frac{119}{128}, \frac{111}{128}, \frac{191}{256}, \frac{11}{16}, \frac{17}{32}, \frac{177}{256}, \frac{31}{512}, \frac{7}{256}, \frac{337}{512}, \frac{63}{128}, \frac{5}{16}, \frac{5}{8}, \frac{117}{128}, \frac{33}{64}, \frac{79}{128}, \frac{3}{8}, \frac{51}{128}, \frac{85}{128}, \frac{1}{8}, \frac{17}{32}, \frac{99}{128}, \frac{185}{256}, \frac{23}{256}, \frac{37}{64}, \frac{231}{256}, \frac{87}{256}, \frac{17}{64}, \frac{7}{16}, \frac{1}{16}, \frac{19}{256}, \frac{57}{64}, \frac{195}{256}, \frac{89}{256}, \frac{215}{256}, \frac{129}{256}, \frac{31}{64}, \frac{215}{256}, \frac{11}{16}, \frac{19}{32}, \frac{105}{256}, \frac{247}{512}, \frac{15}{64}, \frac{37}{128}, \frac{73}{256}, \frac{101}{128}, \frac{97}{128}, \frac{257}{512}, \frac{95}{128}, \frac{3}{16}, \frac{1}{8}, \frac{27}{64}, \frac{75}{128}, \frac{165}{256}, \frac{5}{64}, \frac{131}{256}, \frac{61}{256}, \frac{29}{64}, \frac{153}{256}, \frac{31}{64}, \frac{55}{64}, 0, \frac{5}{8}, \frac{11}{64}, \frac{15}{64}, \frac{105}{128}, \frac{177}{512}, \frac{31}{32}, \frac{225}{256}, \frac{9}{128}, \frac{93}{512}, \frac{25}{32}, \frac{63}{64}, \frac{3}{32}, \frac{3}{4}, \frac{1}{2}, \frac{1}{8}, \frac{21}{64}, \frac{1}{2}, \frac{43}{256}, \frac{47}{128}, \frac{119}{128}, \frac{19}{32}, \frac{63}{256}, \frac{65}{128}, \frac{1}{64}, \frac{25}{32}, \frac{1}{16}, 0, 0, 0, \frac{1}{4}, \frac{1}{2}, \frac{15}{16}, \frac{1}{8}, 0, 0, \frac{3}{16}, \frac{1}{8}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 0, 0\right] \tag{4}$$

> *#Produce in lexicographical order, all monomials of degree 14.*

```
m := 14;
B := [ ];
for i  from 0 to m do:
for j from 0 to m do:
for k from 0 to m do:


if (i + j + k = m) then: B := [op(B), x^i·y^j·z^k];  end if;

od;od;od;
```

```
#Reversing the list produces the ordering we want.
 B := Reverse(B);
```

$$m := 14$$

$$B := [\ ]$$

$$B := [x^{14}, x^{13}y, x^{13}z, x^{12}y^2, x^{12}yz, x^{12}z^2, x^{11}y^3, x^{11}y^2z, x^{11}yz^2, x^{11}z^3, x^{10}y^4, x^{10}y^3z, x^{10}y^2z^2, x^{10}yz^3, x^{10}z^4, x^9y^5, x^9y^4z, x^9y^3z^2, x^9y^2z^3, x^9yz^4, x^9z^5, x^8y^6, x^8y^5z, x^8y^4z^2, x^8y^3z^3, x^8y^2z^4, x^8yz^5, x^8z^6, x^7y^7, x^7y^6z, x^7y^5z^2, x^7y^4z^3, x^7y^3z^4, x^7y^2z^5, x^7yz^6, x^7z^7, x^6y^8, x^6y^7z, x^6y^6z^2, x^6y^5z^3, x^6y^4z^4, x^6y^3z^5, x^6y^2z^6, x^6yz^7, x^6z^8, x^5y^9, x^5y^8z, x^5y^7z^2, x^5y^6z^3, x^5y^5z^4, x^5y^4z^5, x^5y^3z^6, x^5y^2z^7, x^5yz^8, x^5z^9, x^4y^{10}, x^4y^9z, x^4y^8z^2, x^4y^7z^3, x^4y^6z^4, x^4y^5z^5, x^4y^4z^6, x^4y^3z^7, x^4y^2z^8, x^4yz^9, x^4z^{10}, x^3y^{11}, x^3y^{10}z, x^3y^9z^2, x^3y^8z^3, x^3y^7z^4, x^3y^6z^5, x^3y^5z^6, x^3y^4z^7, x^3y^3z^8, x^3y^2z^9, x^3yz^{10}, x^3z^{11}, x^2y^{12}, x^2y^{11}z, x^2y^{10}z^2, x^2y^9z^3, x^2y^8z^4, x^2y^7z^5, x^2y^6z^6, x^2y^5z^7, x^2y^4z^8, x^2y^3z^9, x^2y^2z^{10}, x^2yz^{11}, x^2z^{12}, xy^{13}, xy^{12}z, xy^{11}z^2, xy^{10}z^3, xy^9z^4, xy^8z^5, xy^7z^6, xy^6z^7, xy^5z^8, xy^4z^9, xy^3z^{10}, xy^2z^{11}, xyz^{12}, xz^{13}, y^{14}, y^{13}z, y^{12}z^2, y^{11}z^3, y^{10}z^4, y^9z^5, y^8z^6, y^7z^7, y^6z^8, y^5z^9, y^4z^{10}, y^3z^{11}, y^2z^{12}, yz^{13}, z^{14}] \quad \mathbf{(5)}$$

```
> #Change V to a list instead of a vector, to be capable of using the dot product procedure.
  Vlist := [ ]:
  for i in V do: Vlist := [op(Vlist), i] : od:
  Vlist :
```

```
> #Taking the dot product of B the monomials and Vlist the coefficients produces the IVP f.
  f := DotProduct(B, Vlist);
```

$$f := \frac{1}{2}y^2z^{12} + \frac{1}{64}xy^3z^{10} + \frac{1}{8}y^5z^9 + \frac{65}{128}xy^4z^9 + \frac{63}{256}xy^5z^8 + \frac{19}{32}xy^6z^7 + \frac{119}{128}xy^7z^6 + \frac{47}{128}xy^8z^5 + \frac{43}{256}xy^9z^4 + \frac{1}{2}xy^{10}z^3 + \frac{21}{64}xy^{11}z^2 + \frac{1}{8}xy^{12}z + \frac{1}{2}xy^{13} + \frac{3}{4}x^2z^{12} + \frac{3}{32}x^2yz^{11} + \frac{63}{64}x^2y^2z^{10} + \frac{25}{32}x^2y^3z^9 + \frac{93}{512}x^2y^4z^8 + \frac{9}{128}x^2y^5z^7 + \frac{225}{256}x^2y^6z^6 + \frac{31}{32}x^2y^7z^5 + \frac{177}{512}x^2y^8z^4 + \frac{105}{128}x^2y^9z^3 + \frac{15}{64}x^2y^{10}z^2 + \frac{11}{64}x^2y^{11}z + \frac{5}{8}x^2y^{12} + \frac{55}{64}x^3yz^{10} + \frac{31}{64}x^3y^2z^9 + \frac{153}{256}x^3y^3z^8 + \frac{29}{64}x^3y^4z^7 + \frac{61}{256}x^3y^5z^6 + \frac{131}{256}x^3y^6z^5 + \frac{5}{64}x^3y^7z^4 + \frac{165}{256}x^3y^8z^3 + \frac{75}{128}x^3y^9z^2 + \frac{27}{64}x^3y^{10}z + \frac{1}{8}x^3y^{11} + \frac{3}{16}x^4z^{10} + \frac{95}{128}x^4yz^9 + \frac{257}{512}x^4y^2z^8 + \frac{97}{128}x^4y^3z^7 + \frac{101}{128}x^4y^4z^6 + \frac{73}{256}x^4y^5z^5 + \frac{37}{128}x^4y^6z^4 \quad \mathbf{(6)}$$

$$+\frac{15}{64}x^4y^7z^3+\frac{247}{512}x^4y^8z^2+\frac{105}{256}x^4y^9z+\frac{19}{32}x^4y^{10}+\frac{11}{16}x^5z^9+\frac{215}{256}x^5yz^8$$
$$+\frac{31}{64}x^5y^2z^7+\frac{129}{256}x^5y^3z^6+\frac{215}{256}x^5y^4z^5+\frac{89}{256}x^5y^5z^4+\frac{195}{256}x^5y^6z^3$$
$$+\frac{57}{64}x^5y^7z^2+\frac{19}{256}x^5y^8z+\frac{1}{16}x^5y^9+\frac{7}{16}x^6z^8+\frac{17}{64}x^6yz^7+\frac{87}{256}x^6y^2z^6$$
$$+\frac{231}{256}x^6y^3z^5+\frac{37}{64}x^6y^4z^4+\frac{23}{256}x^6y^5z^3+\frac{185}{256}x^6y^6z^2+\frac{99}{128}x^6y^7z$$
$$+\frac{17}{32}x^6y^8+\frac{1}{8}x^7z^7+\frac{85}{128}x^7yz^6+\frac{51}{128}x^7y^2z^5+\frac{3}{8}x^7y^3z^4+\frac{79}{128}x^7y^4z^3$$
$$+\frac{33}{64}x^7y^5z^2+\frac{117}{128}x^7y^6z+\frac{5}{8}x^7y^7+\frac{5}{16}x^8z^6+\frac{63}{128}x^8yz^5+\frac{337}{512}x^8y^2z^4$$
$$+\frac{7}{256}x^8y^3z^3+\frac{31}{512}x^8y^4z^2+\frac{177}{256}x^8y^5z+\frac{17}{32}x^8y^6+\frac{11}{16}x^9z^5+\frac{191}{256}x^9yz^4$$
$$+\frac{111}{128}x^9y^2z^3+\frac{119}{128}x^9y^3z^2+\frac{131}{256}x^9y^4z+\frac{13}{16}x^9y^5+\frac{1}{16}x^{10}z^4+\frac{17}{32}x^{10}yz^3$$
$$+\frac{61}{64}x^{10}y^2z^2+\frac{9}{64}x^{10}y^3z+\frac{19}{32}x^{10}y^4+\frac{1}{2}x^{11}z^3+\frac{5}{64}x^{11}yz^2+\frac{9}{64}x^{11}y^2z$$
$$+\frac{3}{8}x^{11}y^3+\frac{1}{4}x^{12}z^2+\frac{3}{4}x^{12}yz+\frac{1}{8}x^{12}y^2+\frac{1}{2}x^{13}y+\frac{1}{8}y^4z^{10}+\frac{3}{16}y^6z^8$$
$$+\frac{1}{2}y^{11}z^3+\frac{15}{16}y^{10}z^4+\frac{1}{4}y^3z^{11}+\frac{25}{32}xy^2z^{11}+\frac{1}{16}xyz^{12}+\frac{1}{4}y^{12}z^2$$
$$+\frac{1}{8}y^9z^5$$

```
> #Unapplying f will allow us to evaluate at given triples (i,j,k).
> f := unapply(f, x, y, z) :
>
> #Show that f is an IVP, by evaluating it at all triples (i,j,k) of positive integers less than 2^9.
  for i from 0 to 511 do:
  for j from 0 to 511 do:
  for k from 0 to 511 do:

   a := f(i, j, k);
   if type(a, integer) = false then: print("error"); end if:
   od:od:od:
>
```

```
> #  Code that shows that taking the dual of the HNF of the dual of the bases of IVPs where one
      variable is restricted to evaluate at odd values only produces a basis for homogeneous IVPs
      Taking the SNF of the HNF will produce a basis equivalent to the one in the previous code.
> #Upload necessary procedures.
  with(ListTools) : with(linalg) : with(LinearAlgebra) : with(padic) : with(PolynomialTools) :
      with(combinat) : interface(rtablesize = 110) :
> #create binomial polynomial of degree n.
> binompoly := proc(x, n)
  local f, i, v;
  v := ordp((n!), 2);
  f := 1/2^v;
  for i from 0 to n − 1 do:
  f := f·(x − i);
  od:
  return f;
  end:
>
> #find basis of 2-variable IVPs of degree less than n, for all subsets of two variables from (x,y,z).
> binomxy := proc(n)
  local i, j, Lxy;
  Lxy := [ ]:
  for i from 0 to n do:
  for j from 0 to n do:
  if i + j ≤ n then Lxy := [op(Lxy), binompoly(x, i)·binompoly(y, j)] : fi:
  od:od:
  return Lxy;
 end:
> binomxz := proc(n)
  local i, j, Lxz;
  Lxz := [ ]:
  for i from 0 to n do:
  for j from 0 to n do:
  if i + j ≤ n then Lxz := [op(Lxz), binompoly(x, i)·binompoly(z, j)] : fi:
  od:od:
  return Lxz;
 end:
> binomyz := proc(n)
  local i, j, Lyz;
  Lyz := [ ]:
  for i from 0 to n do:
  for j from 0 to n do:
  if i + j ≤ n then Lyz := [op(Lyz), binompoly(y, i)·binompoly(z, j)] : fi:
  od:od:
  return Lyz;
 end:
>
```

```
> #Homogenize these at the third variable.
> homogz :=proc(LB, n)
   local f, LH, g;
   LH := [ ]:
   for f in LB do:
  f := unapply(f, x, y) :
   g := z^n·f(x/z, y/z) :
   LH := [op(LH), expand(g)] :
   od:
   return  LH;
   end:
> homogy :=proc(LB, n)
   local f, LH, g;
   LH := [ ]:
   for f in LB do:
  f := unapply(f, x, z) :
   g := y^n·f(x/y, z/y) :
   LH := [op(LH), expand(g)] :
   od:
   return  LH;
   end:
> homogx :=proc(LB, n)
   local f, LH, g;
   LH := [ ]:
   for f in LB do:
  f := unapply(f, y, z) :
   g := x^n·f(y/x, z/x) :
   LH := [op(LH), expand(g)] :
   od:
   return  LH;
   end:
>
> #Create a list in lexicographical order of all monomials of degree n.
> monomials :=proc(n)
   local LM, i, j, k;
   LM := [ ]:
  for i from 0 to n do:
  for j from 0 to n do:
  for k from 0 to n do:
   if (i + j + k = n) then LM := [op(LM), x^i·y^j·z^k] :fi:
   od:od:od:
   return  Reverse(LM);
   end:
>
```

```
> #Given a polynomial f and a variable return the coefficent of the variable in f.
> co := proc(f, x)
    local c, i, k;
    c := [coeffs(f, indets(x), k)];
    if member(x, [k], i) then c[i] else 0 fi
  end:
> #Given a homogeneous polynomial f of degree n return a list of coefficients of f, given the
      lexicographical ordering.
  listofcoeffs := proc(f, n)
  local fn, i, v, u, gn, L, k, w, LM;
  gn := expand(f) :
  L := [ ]:
  LM := monomials(n) :
  for i  in LM do:
   v := co(gn, i) :
  L := [op(L), v]:
  od:
  return L;
  end:
>
> # Finding bases using intersection of lattices, create three empty lists Lpolys for the polynomials
      from the HNF, Lotherpolys for the polynomials from SNF and LLL to count denominators.
> Lpolys := [ ]:
  Lotherpolys := [ ]:
  LLL := [ ]:

  #Repeat the process for degrees 1 to 14.
  for m from 1 to 14 do:

      #Create a list of two binomial variable polynomials of degree m, the variable in the name of
      the list is the one not present in the polynomials.
  LBz := binomxy(m) :
  LBy := binomxz(m) :
  LBx := binomyz(m) :


      #Homogenize the list at the third variable, which is the one restricted to be odd only. The
      varaible in the name of the list is the one the polynomials were homogenized at.
  LHz := homogz(LBz, m) :
  LHy := homogy(LBy, m) :
  LHx := homogx(LBx, m) :


      #For each of these store in a list of list the coefficients of the homogeneous monomials from the
      two variable binomial polynomials that were homogenized.
   LL0 := [ ]:
  for i in LHz do:
  LL0 := [op(LL0), listofcoeffs(i, m)]:
```

```
od:
LL := [ ]:
for i in LHy do:
LL := [op(LL), listofcoeffs(i, m)]:
od:
LL1 := [ ]:
for i in LHx do:
LL1 := [op(LL1), listofcoeffs(i, m)]:
od:


    #Create matrices from the list of list and take their dual, DA, DB, DC are the dual basis for
    each homogeneous basis where one varaible evalautes at only odd values.
C := Matrix(LL0) :
C := Transpose(C) :
A := Matrix(LL) :
A := Transpose(A) :
B := Matrix(LL1) :
B := Transpose(B) :
DC := C.MatrixInverse((Transpose(C).C)) :
DB := B.MatrixInverse((Transpose(B).B)) :
DA := A.MatrixInverse((Transpose(A).A)) :

#Join these matrices and take the HNF of the result
DC := Matrix([[DC, DA, DB]]) :
HDC := HermiteForm(Transpose(DC)) :

#Remove all rows of zeros from the HNF and dualize
n := Dimension(HDC)[2]:
HDC := HDC(1 ..n, 1 ..n) :
H := HDC.MatrixInverse((Transpose(HDC).HDC)) :

#The the SNF of the HNF to obtain bases similar as the ones on the previous code.
S := SmithForm(HDC) :


    #Using the dual of the HNF creat a list of homogeneous integer valued polynomial by taking
    the dot product of the coefficients from the rows of H and the lexicographical ordering.
LP := [ ]:
for i from 1 to Dimension(H)[1] do:
f := Vector(Row(H, i)).Vector(monomials(m)) :
LP := [op(LP), f]:
od:

#Lpolys a list of IVPs of degree m for each m up to degree 14.
Lpolys := [op(Lpolys), LP]:

#count the 2-adic norm of the diagonal of the SNF, and store it in LLL the list of list.
```

```
L := [ ] :
for i from 1 to n do
L := [op(L), ordp(S[i, i], 2) ] :od:
LLL := [op(LLL), L];

od:
```

```
>
> #Look at the polynomials from the Hermite normal form and find the denomianator with greatest 2
     -adic norm.
  L2 := [ ] :
   for i in Lpolys do:
  L0 := [ ] :
   for j in i do:
   L1 := [coeffs(j)] :
   c := 0 :
   for k in L1 do:
   d := ordp(k, 2) :
   if d < c then c := d :fi:
   od:
   L0 := [op(L0),-c] :
   od:
   L2 := [op(L2), L0] :
  od:
>
> #necessary procedure used to count how many of the polynomials have a certain 2-adic norm
   num :=proc(a, L) local i, c; c := 0;for i from 1 to nops(L) do if L[i] = a then c := c + 1 else
     fi; od ; c;end:
   N := Matrix(nops(L2), nops(L2) - 1) :


     # builds the table with ij-entry the number of basis elementsin degree i whose denominator is
     of 2-norm j, from the polynomials obtained by the HNF.
   for i from 1 to (nops(L2)) do for j from 0 to ((nops(L2) - 2)) do
   N[i, j + 1] := num(j, L2[i]);od;od;
> N;
```

(1)

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 14 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 11 & 7 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 7 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 8 & 17 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 4 & 14 & 20 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 4 & 14 & 28 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 4 & 14 & 35 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 4 & 10 & 22 & 23 & 12 & 3 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 4 & 10 & 18 & 6 & 27 & 23 & 0 & 0 & 0 & 0 & 0 \\ 7 & 10 & 4 & 10 & 18 & 7 & 18 & 34 & 7 & 5 & 0 & 0 & 0 \end{bmatrix} \quad \textbf{(1)}$$

```
> #Note that this matrix is different from the one of the SNF technique.
> #We count the 2-adic norm of the diagonal elements of the Smith normal form of the Hermite
      normal form
> N1 := Matrix(nops(L2), nops(L2) − 1) :


      # builds the table with ij-entry the number of basis elements of degree i whose denominator is
      of 2-norm j
  for i from 1 to (nops(L2)) do for j from 0 to ((nops(L2) − 2)) do
  N1[i, j + 1] := num(j, LLL[i]);od;od;
> N1;
```

(2)

$$\left[\begin{array}{ccccccccccccc}
3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 6 & 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 21 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 28 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 28 & 14 & 4 & 3 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 28 & 14 & 6 & 15 & 0 & 0 & 0 & 0 & 0 \\
7 & 14 & 7 & 14 & 28 & 14 & 7 & 25 & 3 & 1 & 0 & 0 & 0
\end{array}\right] \qquad \textbf{(2)}$$

> *#this produced the same matrix as the SNF code*

> *#L2 contains the 2-adic norm of the denomianators of the IVPs obtained by the hermite normal form, find the indices of the degree 14 polynomials with a* 2^9 **in** *their denomiantor*

for i **from** 1 **to** 120 **do**: **if** $L2[14][i] = 9$ **then** $print(i)$;**fi**:**od**:

$$100$$

$$101$$

$$102$$

$$103$$

$$104 \qquad \textbf{(3)}$$

> *#Take f obtained from the dual of the Hermite normal form, which is an IVP of degree 14 with* 2^9 **in** *its denomiantor*

$f0 := Lpolys[14][100];$

$$\begin{aligned}
f0 := {} & \frac{9}{128} z^4 x^7 y^3 + \frac{1}{32} z^3 x^7 y^4 - \frac{1}{64} z x^3 y^{10} - \frac{1}{256} z^6 x^3 y^5 + \frac{1}{256} z^5 x^3 y^6 \qquad \textbf{(4)} \\
& + \frac{9}{256} z^2 x^6 y^6 - \frac{1}{128} z x^6 y^7 - \frac{1}{128} z^2 x^5 y^7 + \frac{3}{512} z^2 x^4 y^8 + \frac{3}{128} z^3 x^4 y^7 \\
& + \frac{3}{128} z^4 x^3 y^7 - \frac{1}{256} z^3 x^3 y^8 - \frac{11}{128} z^4 x^9 y - \frac{9}{64} z^3 x^9 y^2 - \frac{1}{128} z^5 x^2 y^7 \\
& + \frac{3}{512} z^4 x^2 y^8 + \frac{1}{64} z x^5 y^8 + \frac{3}{256} z^5 x^5 y^4 - \frac{1}{256} z^4 x^5 y^5 + \frac{1}{64} z^9 x^3 y^2 \\
& - \frac{1}{256} z^8 x^3 y^3 - \frac{15}{256} z x^4 y^9 - \frac{1}{128} z^4 x^6 y^4 - \frac{1}{256} z^5 x^4 y^5 - \frac{1}{128} z^4 x^4 y^6 \\
& + \frac{1}{256} z^8 x y^5 - \frac{1}{128} z^6 x y^7 - \frac{1}{64} z^5 x y^8 - \frac{3}{256} z^4 x y^9 + \frac{1}{64} z^3 x y^{10}
\end{aligned}$$

$$+\frac{1}{64} z^{2} x y^{11}+\frac{1}{256} z^{3} x^{5} y^{6}-\frac{23}{256} z^{3} x^{8} y^{3}-\frac{1}{128} z^{9} x^{2} y^{3}-\frac{1}{512} z^{8} x^{2} y^{4}$$
$$-\frac{1}{256} z^{6} x^{2} y^{6}-\frac{1}{128} z^{8} x^{5} y-\frac{1}{256} z^{6} x^{5} y^{3}+\frac{9}{256} z^{3} x^{6} y^{5}-\frac{1}{64} z x^{7} y^{6}$$
$$+\frac{1}{64} z^{2} x^{3} y^{9}+\frac{1}{256} z^{6} x^{6} y^{2}+\frac{13}{256} z^{5} x^{6} y^{3}+\frac{1}{64} z x^{2} y^{11}+\frac{1}{128} z^{9} x^{4} y$$
$$+\frac{1}{512} z^{8} x^{4} y^{2}+\frac{11}{512} z^{2} x^{8} y^{4}+\frac{25}{256} z x^{8} y^{5}-\frac{5}{128} z^{5} x^{8} y+\frac{5}{512} z^{4} x^{8} y^{2}$$
$$+\frac{1}{32} z^{3} x^{10} y-\frac{1}{16} z^{2} x^{10} y^{2}-\frac{3}{64} z^{5} x^{7} y^{2}-\frac{7}{128} z^{2} x^{7} y^{5}-\frac{3}{32} z^{2} x^{9} y^{3}$$
$$-\frac{11}{64} z x^{9} y^{4}+\frac{5}{16} z x^{12} y+\frac{5}{32} z^{2} x^{11} y+\frac{5}{16} z x^{11} y^{2}-\frac{23}{64} z x^{10} y^{3}$$

> $f1 := Lpolys[14][101];$

$$f1 := \frac{5}{128} z^{4} x^{7} y^{3}+\frac{1}{16} z^{3} x^{7} y^{4}-\frac{1}{128} z^{3} x^{2} y^{9}-\frac{1}{256} z^{6} x^{3} y^{5}+\frac{1}{256} z^{5} x^{3} y^{6} \tag{5}$$
$$+\frac{9}{256} z^{2} x^{6} y^{6}-\frac{1}{32} z^{2} x^{5} y^{7}+\frac{13}{512} z^{2} x^{4} y^{8}+\frac{3}{128} z^{3} x^{4} y^{7}+\frac{1}{64} z^{4} x^{3} y^{7}$$
$$-\frac{3}{256} z^{3} x^{3} y^{8}-\frac{19}{256} z^{4} x^{9} y+\frac{17}{128} z^{3} x^{9} y^{2}-\frac{1}{128} z^{5} x^{2} y^{7}-\frac{1}{512} z^{4} x^{2} y^{8}$$
$$+\frac{1}{256} z x^{5} y^{8}+\frac{1}{256} z^{5} x^{5} y^{4}+\frac{1}{256} z^{4} x^{5} y^{5}+\frac{1}{128} z^{9} x^{3} y^{2}-\frac{1}{256} z^{8} x^{3} y^{3}$$
$$-\frac{1}{64} z^{2} x^{2} y^{10}-\frac{1}{32} z x^{4} y^{9}-\frac{1}{128} z^{4} x^{6} y^{4}-\frac{1}{256} z^{5} x^{4} y^{5}-\frac{1}{128} z^{4} x^{4} y^{6}$$
$$+\frac{1}{128} z^{9} x y^{4}-\frac{3}{128} z^{5} x y^{8}-\frac{3}{64} z^{3} x y^{10}-\frac{1}{16} z^{2} x y^{11}+\frac{5}{256} z^{3} x^{5} y^{6}$$
$$-\frac{71}{256} z^{3} x^{8} y^{3}-\frac{1}{512} z^{8} x^{2} y^{4}+\frac{1}{256} z^{6} x^{2} y^{6}-\frac{3}{256} z^{8} x^{5} y-\frac{1}{256} z^{6} x^{5} y^{3}$$
$$-\frac{5}{256} z^{3} x^{6} y^{5}-\frac{9}{128} z x^{7} y^{6}+\frac{3}{128} z^{2} x^{3} y^{9}-\frac{1}{256} z^{6} x^{6} y^{2}+\frac{11}{256} z^{5} x^{6} y^{3}$$
$$+\frac{1}{16} z x^{2} y^{11}+\frac{1}{64} z^{9} x^{4} y+\frac{1}{512} z^{8} x^{4} y^{2}+\frac{1}{512} z^{2} x^{8} y^{4}+\frac{7}{64} z x^{8} y^{5}$$
$$-\frac{5}{64} z^{5} x^{8} y+\frac{9}{512} z^{4} x^{8} y^{2}-\frac{1}{16} z^{3} x^{10} y-\frac{3}{64} z^{2} x^{10} y^{2}-\frac{3}{128} z^{6} x^{7} y$$
$$-\frac{1}{32} z^{5} x^{7} y^{2}+\frac{3}{128} z^{2} x^{7} y^{5}-\frac{1}{8} z^{2} x^{9} y^{3}-\frac{35}{256} z x^{9} y^{4}+\frac{3}{8} z x^{12} y+\frac{15}{64} z^{2} x^{11} y$$
$$+\frac{5}{64} z x^{11} y^{2}-\frac{9}{64} z x^{10} y^{3}$$

> $f2 := Lpolys[14][102];$

$$f2 := \frac{9}{128} z^{4} x^{7} y^{3}+\frac{3}{32} z^{3} x^{7} y^{4}+\frac{1}{128} z^{3} x^{2} y^{9}-\frac{1}{256} z^{6} x^{3} y^{5}+\frac{3}{256} z^{5} x^{3} y^{6} \tag{6}$$

$$
\begin{aligned}
&+\frac{5}{256} z^{2} x^{6} y^{6}-\frac{1}{32} z x^{6} y^{7}-\frac{3}{64} z^{2} x^{5} y^{7}+\frac{1}{512} z^{2} x^{4} y^{8}+\frac{7}{128} z^{3} x^{4} y^{7} \\
&+\frac{1}{32} z^{4} x^{3} y^{7}+\frac{1}{256} z^{3} x^{3} y^{8}-\frac{21}{256} z^{4} x^{9} y-\frac{9}{64} z^{3} x^{9} y^{2}-\frac{1}{128} z^{5} x^{2} y^{7} \\
&+\frac{3}{512} z^{4} x^{2} y^{8}+\frac{1}{256} z x^{5} y^{8}+\frac{1}{256} z^{5} x^{5} y^{4}-\frac{3}{256} z^{4} x^{5} y^{5}-\frac{1}{64} z^{10} x^{3} y \\
&+\frac{1}{64} z^{9} x^{3} y^{2}-\frac{1}{256} z^{8} x^{3} y^{3}-\frac{1}{64} z^{2} x^{2} y^{10}-\frac{3}{64} z x^{4} y^{9}-\frac{1}{64} z^{4} x^{6} y^{4} \\
&-\frac{1}{256} z^{5} x^{4} y^{5}-\frac{1}{64} z^{4} x^{4} y^{6}+\frac{1}{64} z^{10} x y^{3}-\frac{1}{64} z^{5} x y^{8}-\frac{1}{64} z^{4} x y^{9}-\frac{3}{64} z^{3} x y^{10} \\
&-\frac{1}{16} z^{2} x y^{11}-\frac{1}{256} z^{3} x^{5} y^{6}-\frac{93}{256} z^{3} x^{8} y^{3}-\frac{1}{128} z^{9} x^{2} y^{3}-\frac{1}{512} z^{8} x^{2} y^{4} \\
&-\frac{1}{128} z^{7} x^{2} y^{5}-\frac{1}{256} z^{6} x^{2} y^{6}-\frac{1}{256} z^{8} x^{5} y-\frac{1}{256} z^{6} x^{5} y^{3}+\frac{17}{256} z^{3} x^{6} y^{5} \\
&-\frac{1}{128} z x^{7} y^{6}-\frac{1}{128} z^{2} x^{3} y^{9}+\frac{1}{64} z^{7} x^{6} y+\frac{1}{256} z^{6} x^{6} y^{2}+\frac{5}{256} z^{5} x^{6} y^{3} \\
&+\frac{1}{16} z x^{2} y^{11}+\frac{1}{128} z^{9} x^{4} y+\frac{1}{512} z^{8} x^{4} y^{2}-\frac{1}{128} z^{7} x^{4} y^{3}-\frac{3}{512} z^{2} x^{8} y^{4} \\
&+\frac{3}{32} z x^{8} y^{5}-\frac{1}{128} z^{5} x^{8} y+\frac{13}{512} z^{4} x^{8} y^{2}+\frac{15}{64} z^{3} x^{10} y-\frac{1}{128} z^{6} x^{7} y \\
&-\frac{3}{64} z^{5} x^{7} y^{2}-\frac{1}{128} z^{2} x^{7} y^{5}+\frac{19}{64} z^{2} x^{9} y^{3}-\frac{3}{256} z x^{9} y^{4}+\frac{3}{4} z x^{12} y-\frac{9}{64} z^{2} x^{11} y \\
&+\frac{9}{64} z x^{11} y^{2}-\frac{53}{64} z x^{10} y^{3}
\end{aligned}
$$

```
> f3 := Lpolys[14][103];
```

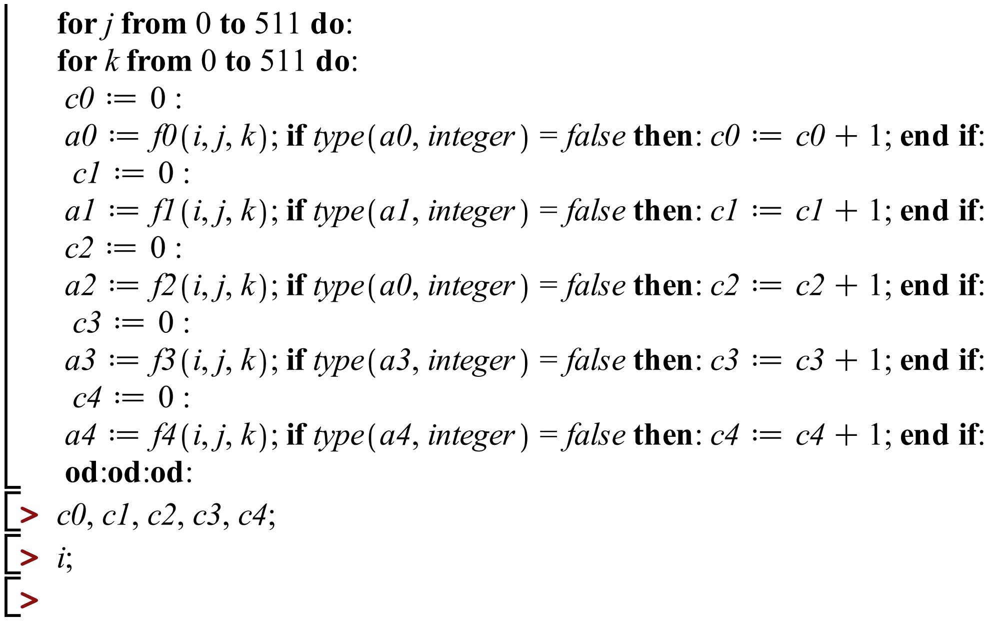
$$
\begin{aligned}
f3 := {}&\frac{3}{64} z^{4} x^{7} y^{3}+\frac{1}{128} z^{3} x^{7} y^{4}-\frac{1}{128} z^{3} x^{2} y^{9}-\frac{1}{256} z^{6} x^{3} y^{5}+\frac{3}{256} z^{5} x^{3} y^{6} \\
&+\frac{1}{256} z^{2} x^{6} y^{6}-\frac{1}{64} z x^{6} y^{7}-\frac{1}{64} z^{2} x^{5} y^{7}-\frac{5}{512} z^{2} x^{4} y^{8}+\frac{1}{32} z^{3} x^{4} y^{7} \\
&+\frac{1}{64} z^{4} x^{3} y^{7}-\frac{3}{256} z^{3} x^{3} y^{8}-\frac{19}{256} z^{4} x^{9} y-\frac{21}{128} z^{3} x^{9} y^{2}-\frac{1}{512} z^{4} x^{2} y^{8} \\
&-\frac{3}{256} z x^{5} y^{8}+\frac{3}{256} z^{5} x^{5} y^{4}-\frac{1}{256} z^{4} x^{5} y^{5}+\frac{1}{64} z^{9} x^{3} y^{2}-\frac{1}{256} z^{8} x^{3} y^{3} \\
&-\frac{7}{128} z x^{4} y^{9}-\frac{1}{256} z^{5} x^{4} y^{5}+\frac{1}{64} z^{11} x y^{2}-\frac{1}{256} z^{9} x y^{4}-\frac{1}{128} z^{7} x y^{6} \\
&-\frac{1}{256} z^{5} x y^{8}-\frac{1}{64} z^{11} x^{2} y-\frac{1}{256} z^{3} x^{5} y^{6}-\frac{37}{256} z^{3} x^{8} y^{3}-\frac{1}{128} z^{9} x^{2} y^{3} \\
&-\frac{1}{512} z^{8} x^{2} y^{4}+\frac{1}{256} z^{6} x^{2} y^{6}-\frac{3}{256} z^{8} x^{5} y-\frac{1}{64} z^{7} x^{5} y^{2}-\frac{1}{256} z^{6} x^{5} y^{3}
\end{aligned}
\tag{7}
$$

$$- \frac{9}{256} z^{3} x^{6} y^{5} - \frac{3}{128} z x^{7} y^{6} + \frac{1}{128} z^{2} x^{3} y^{9} + \frac{5}{128} z^{7} x^{6} y + \frac{3}{256} z^{6} x^{6} y^{2}$$
$$- \frac{1}{256} z^{5} x^{6} y^{3} + \frac{1}{32} z x^{2} y^{11} + \frac{3}{256} z^{9} x^{4} y + \frac{5}{512} z^{8} x^{4} y^{2} - \frac{1}{64} z^{7} x^{4} y^{3}$$
$$+ \frac{11}{512} z^{2} x^{8} y^{4} + \frac{21}{128} z x^{8} y^{5} + \frac{11}{256} z^{5} x^{8} y + \frac{5}{512} z^{4} x^{8} y^{2} + \frac{15}{64} z^{3} x^{10} y$$
$$- \frac{3}{64} z^{2} x^{10} y^{2} - \frac{3}{128} z^{6} x^{7} y - \frac{13}{128} z^{5} x^{7} y^{2} + \frac{1}{64} z^{2} x^{7} y^{5} + \frac{17}{128} z^{2} x^{9} y^{3}$$
$$- \frac{35}{256} z x^{9} y^{4} + \frac{1}{4} z x^{12} y - \frac{5}{64} z^{2} x^{11} y + \frac{27}{64} z x^{11} y^{2} - \frac{1}{2} z x^{10} y^{3}$$

```
> f4 := Lpolys[14][104];
```

$$f4 := \frac{5}{128} z^{4} x^{7} y^{3} + \frac{11}{128} z^{3} x^{7} y^{4} - \frac{1}{256} z^{6} x^{3} y^{5} + \frac{1}{256} z^{5} x^{3} y^{6} + \frac{1}{256} z^{2} x^{6} y^{6} \tag{8}$$
$$- \frac{1}{32} z^{2} x^{5} y^{7} - \frac{3}{512} z^{2} x^{4} y^{8} + \frac{1}{128} z^{3} x^{4} y^{7} + \frac{1}{64} z^{4} x^{3} y^{7} - \frac{5}{256} z^{3} x^{3} y^{8}$$
$$- \frac{27}{256} z^{4} x^{9} y - \frac{21}{128} z^{3} x^{9} y^{2} - \frac{1}{128} z^{5} x^{2} y^{7} - \frac{1}{512} z^{4} x^{2} y^{8} + \frac{5}{256} z x^{5} y^{8}$$
$$+ \frac{1}{256} z^{5} x^{5} y^{4} + \frac{1}{256} z^{4} x^{5} y^{5} - \frac{1}{64} z^{10} x^{3} y + \frac{1}{64} z^{9} x^{3} y^{2} - \frac{1}{256} z^{8} x^{3} y^{3}$$
$$- \frac{1}{64} z^{2} x^{2} y^{10} - \frac{3}{64} z x^{4} y^{9} - \frac{1}{128} z^{4} x^{6} y^{4} - \frac{1}{256} z^{5} x^{4} y^{5} - \frac{1}{128} z^{4} x^{4} y^{6}$$
$$- \frac{1}{16} z x y^{12} + \frac{1}{16} z^{12} x y + \frac{1}{256} z^{3} x^{5} y^{6} - \frac{41}{256} z^{3} x^{8} y^{3} - \frac{1}{512} z^{8} x^{2} y^{4}$$
$$- \frac{1}{128} z^{7} x^{2} y^{5} + \frac{1}{256} z^{6} x^{2} y^{6} - \frac{3}{256} z^{8} x^{5} y - \frac{1}{256} z^{6} x^{5} y^{3} - \frac{1}{256} z^{3} x^{6} y^{5}$$
$$+ \frac{3}{128} z x^{7} y^{6} + \frac{1}{128} z^{2} x^{3} y^{9} - \frac{1}{256} z^{6} x^{6} y^{2} + \frac{11}{256} z^{5} x^{6} y^{3} + \frac{1}{32} z x^{2} y^{11}$$
$$+ \frac{1}{64} z^{9} x^{4} y + \frac{1}{512} z^{8} x^{4} y^{2} + \frac{1}{128} z^{7} x^{4} y^{3} + \frac{1}{512} z^{2} x^{8} y^{4} + \frac{1}{16} z x^{8} y^{5}$$
$$- \frac{1}{64} z^{5} x^{8} y + \frac{9}{512} z^{4} x^{8} y^{2} + \frac{1}{64} z^{2} x^{10} y^{2} - \frac{5}{128} z^{6} x^{7} y - \frac{7}{128} z^{5} x^{7} y^{2}$$
$$+ \frac{5}{128} z^{2} x^{7} y^{5} + \frac{3}{16} z^{2} x^{9} y^{3} - \frac{15}{256} z x^{9} y^{4} + \frac{3}{8} z x^{12} y - \frac{9}{64} z^{2} x^{11} y + \frac{13}{64} z x^{11} y^{2}$$
$$- \frac{19}{64} z x^{10} y^{3}$$

```
>
> #Show that these are IVPs, by evaluating these at all triples (i,j,k) where the indices range through
      all values less than 512.
  f0 := unapply(f0, x, y, z) : f1 := unapply(f1, x, y, z) : f2 := unapply(f2, x, y, z) : f3 :=
      unapply(f3, x, y, z) : f4 := unapply(f4, x, y, z) :
  for i from 0 to 511 do:
```



```
for j from 0 to 511 do:
for k from 0 to 511 do:
 c0 := 0 :
 a0 := f0(i, j, k); if type(a0, integer) = false then: c0 := c0 + 1; end if:
  c1 := 0 :
 a1 := f1(i, j, k); if type(a1, integer) = false then: c1 := c1 + 1; end if:
 c2 := 0 :
 a2 := f2(i, j, k); if type(a0, integer) = false then: c2 := c2 + 1; end if:
  c3 := 0 :
 a3 := f3(i, j, k); if type(a3, integer) = false then: c3 := c3 + 1; end if:
  c4 := 0 :
 a4 := f4(i, j, k); if type(a4, integer) = false then: c4 := c4 + 1; end if:
 od:od:od:
> c0, c1, c2, c3, c4;
> i;
>
```

```
> #Code that for a given m that is a power of 2, will generate all points (and lines) in ZmP^2.
> #Upload necessary procedures.
> with(padic) :
> #For a given m, find all triples over Zm, where at least one entry is odd, store these in L.
  m := 4 :
  L := [ ] :
  for i from 0 to m − 1 do:
  for j from 0 to m − 1 do:
  for k from 0 to m − 1 do:

  if (((type(i/2, integer))and (type(j/2, integer)) and (type(k/2, integer)))then c := 0 :
       else L := [op(L), [i, j, k]] :fi:

  od:od:od:
>
> #Find all units in Zm, store these in U.
  U := [ ] :
  for i from 1 to m − 1 do:
  if gcd(i, m) = 1 then U := [op(U), i] :fi:
  od:
>
> #Given all triples in L, find those who are equivalent when multiplied by a unit and only keep one
       representative per equivalence class.
  P := { } :

  for a in L do:
  a1 := a[1] :
  a2 := a[2] :
  a3 := a[3] :

  Q := {[ a1, a2, a3]} :
  for u in U do:
  for b in L do:

   b1 :=mod((u·b[1]), m) :
  b2 :=mod((u·b[2]), m) :
  b3 :=mod((u·b[3]), m) :
  if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then Q := Q ∪ {[b[1], b[2], b[3]]} : fi:
  od:od:
  P := P∪ {Q} :
  od:

>
> #Convert the set into a list, which will be the list of points and lines in ZmP2.
  Q := [ ] :
    for i in P do:
    Q := [op(Q), i[1]] :
    od:
```

```
> #Display Q, which in this case represents all points in Z4P^2
  Q;
[[0, 0, 1], [0, 1, 0], [0, 1, 1], [0, 1, 2], [0, 1, 3], [0, 2, 1], [1, 0, 0], [1, 0, 1], [1, 0, 2], [1, 0,      (1)
    3], [1, 1, 0], [1, 1, 1], [1, 1, 2], [1, 1, 3], [1, 2, 0], [1, 2, 1], [1, 2, 2], [1, 2, 3], [1, 3, 0],
    [1, 3, 1], [1, 3, 2], [1, 3, 3], [2, 0, 1], [2, 1, 0], [2, 1, 1], [2, 1, 2], [2, 1, 3], [2, 2, 1]]
```

```
> #Group the points according to what they are congruent over Z2P^2
  S := { } :
    for a in Q do:
   a1 := mod(a[1], 2) :
   a2 := mod(a[2], 2) :
   a3 := mod(a[3], 2) :

   T := {[ a[1], a[2], a[3]]} :

   for b in Q do:
   b1 := mod((b[1]), 2) :
   b2 := mod((b[2]), 2) :
   b3 := mod((b[3]), 2) :

   if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then  T := T ⋃ {[b[1], b[2], b[3]]} : fi:

  od:
   S := S ⋃ {T} :

   od:
>
> for i in S do: print(i) : od:
                                 {[0, 0, 1], [0, 2, 1], [2, 0, 1], [2, 2, 1]}
                                 {[0, 1, 0], [0, 1, 2], [2, 1, 0], [2, 1, 2]}
                                 {[0, 1, 1], [0, 1, 3], [2, 1, 1], [2, 1, 3]}
                                 {[1, 0, 0], [1, 0, 2], [1, 2, 0], [1, 2, 2]}
                                 {[1, 0, 1], [1, 0, 3], [1, 2, 1], [1, 2, 3]}
                                 {[1, 1, 0], [1, 1, 2], [1, 3, 0], [1, 3, 2]}
                                 {[1, 1, 1], [1, 1, 3], [1, 3, 1], [1, 3, 3]}                          (2)
> #Each set is 4 lines over Z4P^2 that are congruent over Z2P^2
>
```

> *kernelopts* (*printbytes* = *false*) :

> *#this file shows that the polynomial we are interested in is not made of a product of 14 linear factors that correspont to a product of seven pair of lines that are congruent in the fano plane.*

>

> *#the polynomial obtained from the Smith normal form and the matrix of Sterling coefficients*

> $$\begin{aligned}f := {} & \frac{7}{16} x^6 z^8 + \frac{17}{64} x^6 y z^7 + \frac{87}{256} x^6 y^2 z^6 + \frac{231}{256} x^6 y^3 z^5 + \frac{37}{64} x^6 y^4 z^4 + \frac{23}{256} x^6 y^5 z^3 \\ & + \frac{185}{256} x^6 y^6 z^2 + \frac{99}{128} x^6 y^7 z + \frac{17}{32} x^6 y^8 + \frac{1}{8} x^7 z^7 + \frac{85}{128} x^7 y z^6 + \frac{51}{128} x^7 y^2 z^5 \\ & + \frac{3}{8} x^7 y^3 z^4 + \frac{79}{128} x^7 y^4 z^3 + \frac{33}{64} x^7 y^5 z^2 + \frac{117}{128} x^7 y^6 z + \frac{5}{8} x^7 y^7 + \frac{5}{16} x^8 z^6 \\ & + \frac{63}{128} x^8 y z^5 + \frac{337}{512} x^8 y^2 z^4 + \frac{7}{256} x^8 y^3 z^3 + \frac{31}{512} x^8 y^4 z^2 + \frac{177}{256} x^8 y^5 z \\ & + \frac{17}{32} x^8 y^6 + \frac{11}{16} x^9 z^5 + \frac{191}{256} x^9 y z^4 + \frac{111}{128} x^9 y^2 z^3 + \frac{119}{128} x^9 y^3 z^2 + \frac{131}{256} x^9 y^4 z \\ & + \frac{13}{16} x^9 y^5 + \frac{1}{16} x^{10} z^4 + \frac{17}{32} x^{10} y z^3 + \frac{61}{64} x^{10} y^2 z^2 + \frac{9}{64} x^{10} y^3 z + \frac{19}{32} x^{10} y^4 \\ & + \frac{1}{2} x^{11} z^3 + \frac{5}{64} x^{11} y z^2 + \frac{9}{64} x^{11} y^2 z + \frac{3}{8} x^{11} y^3 + \frac{1}{4} x^{12} z^2 + \frac{3}{4} x^{12} y z \\ & + \frac{1}{8} x^{12} y^2 + \frac{1}{2} x^{13} y + \frac{1}{2} y^2 z^{12} + \frac{1}{4} y^{12} z^2 + \frac{1}{64} x y^3 z^{10} + \frac{65}{128} x y^4 z^9 \\ & + \frac{63}{256} x y^5 z^8 + \frac{19}{32} x y^6 z^7 + \frac{119}{128} x y^7 z^6 + \frac{47}{128} x y^8 z^5 + \frac{43}{256} x y^9 z^4 + \frac{1}{2} x y^{10} z^3 \\ & + \frac{21}{64} x y^{11} z^2 + \frac{1}{8} x y^{12} z + \frac{1}{2} x y^{13} + \frac{3}{4} x^2 z^{12} + \frac{3}{32} x^2 y z^{11} + \frac{63}{64} x^2 y^2 z^{10} \\ & + \frac{25}{32} x^2 y^3 z^9 + \frac{93}{512} x^2 y^4 z^8 + \frac{9}{128} x^2 y^5 z^7 + \frac{225}{256} x^2 y^6 z^6 + \frac{31}{32} x^2 y^7 z^5 \\ & + \frac{177}{512} x^2 y^8 z^4 + \frac{105}{128} x^2 y^9 z^3 + \frac{15}{64} x^2 y^{10} z^2 + \frac{11}{64} x^2 y^{11} z + \frac{5}{8} x^2 y^{12} \\ & + \frac{55}{64} x^3 y z^{10} + \frac{31}{64} x^3 y^2 z^9 + \frac{153}{256} x^3 y^3 z^8 + \frac{29}{64} x^3 y^4 z^7 + \frac{61}{256} x^3 y^5 z^6 \\ & + \frac{131}{256} x^3 y^6 z^5 + \frac{5}{64} x^3 y^7 z^4 + \frac{165}{256} x^3 y^8 z^3 + \frac{75}{128} x^3 y^9 z^2 + \frac{27}{64} x^3 y^{10} z \\ & + \frac{1}{8} x^3 y^{11} + \frac{3}{16} x^4 z^{10} + \frac{95}{128} x^4 y z^9 + \frac{257}{512} x^4 y^2 z^8 + \frac{97}{128} x^4 y^3 z^7 + \frac{101}{128} x^4 y^4 z^6 \\ & + \frac{73}{256} x^4 y^5 z^5 + \frac{37}{128} x^4 y^6 z^4 + \frac{15}{64} x^4 y^7 z^3 + \frac{247}{512} x^4 y^8 z^2 + \frac{105}{256} x^4 y^9 z \\ & + \frac{19}{32} x^4 y^{10} + \frac{11}{16} x^5 z^9 + \frac{215}{256} x^5 y z^8 + \frac{31}{64} x^5 y^2 z^7 + \frac{129}{256} x^5 y^3 z^6 + \frac{215}{256} x^5 y^4 z^5 \\ & + \frac{89}{256} x^5 y^5 z^4 + \frac{195}{256} x^5 y^6 z^3 + \frac{57}{64} x^5 y^7 z^2 + \frac{19}{256} x^5 y^8 z + \frac{1}{16} x^5 y^9 + \frac{25}{32} x y^2 z^{11} \\ & + \frac{1}{4} y^3 z^{11} + \frac{3}{16} y^6 z^8 + \frac{1}{2} y^{11} z^3 + \frac{1}{8} y^4 z^{10} + \frac{1}{8} y^5 z^9 + \frac{1}{16} x y z^{12} + \frac{15}{16} y^{10} z^4 \\ & + \frac{1}{8} y^9 z^5 :\end{aligned}$$

```
> #clear out denominators
> f := 512·f;
```

$$
\begin{aligned}
f := {} & 256 x^{13} y + 64 x^{12} y^{2} + 384 x^{12} y z + 128 x^{12} z^{2} + 192 x^{11} y^{3} + 72 x^{11} y^{2} z + 40 x^{11} y z^{2} \\
& + 256 x^{11} z^{3} + 304 x^{10} y^{4} + 72 x^{10} y^{3} z + 488 x^{10} y^{2} z^{2} + 272 x^{10} y z^{3} + 32 x^{10} z^{4} \\
& + 416 x^{9} y^{5} + 262 x^{9} y^{4} z + 476 x^{9} y^{3} z^{2} + 444 x^{9} y^{2} z^{3} + 382 x^{9} y z^{4} + 352 x^{9} z^{5} \\
& + 272 x^{8} y^{6} + 354 x^{8} y^{5} z + 31 x^{8} y^{4} z^{2} + 14 x^{8} y^{3} z^{3} + 337 x^{8} y^{2} z^{4} + 252 x^{8} y z^{5} \\
& + 160 x^{8} z^{6} + 320 x^{7} y^{7} + 468 x^{7} y^{6} z + 264 x^{7} y^{5} z^{2} + 316 x^{7} y^{4} z^{3} + 192 x^{7} y^{3} z^{4} \\
& + 204 x^{7} y^{2} z^{5} + 340 x^{7} y z^{6} + 64 x^{7} z^{7} + 272 x^{6} y^{8} + 396 x^{6} y^{7} z + 370 x^{6} y^{6} z^{2} \\
& + 46 x^{6} y^{5} z^{3} + 296 x^{6} y^{4} z^{4} + 462 x^{6} y^{3} z^{5} + 174 x^{6} y^{2} z^{6} + 136 x^{6} y z^{7} + 224 x^{6} z^{8} \\
& + 32 x^{5} y^{9} + 38 x^{5} y^{8} z + 456 x^{5} y^{7} z^{2} + 390 x^{5} y^{6} z^{3} + 178 x^{5} y^{5} z^{4} + 430 x^{5} y^{4} z^{5} \\
& + 258 x^{5} y^{3} z^{6} + 248 x^{5} y^{2} z^{7} + 430 x^{5} y z^{8} + 352 x^{5} z^{9} + 304 x^{4} y^{10} + 210 x^{4} y^{9} z \\
& + 247 x^{4} y^{8} z^{2} + 120 x^{4} y^{7} z^{3} + 148 x^{4} y^{6} z^{4} + 146 x^{4} y^{5} z^{5} + 404 x^{4} y^{4} z^{6} + 388 x^{4} y^{3} z^{7} \\
& + 257 x^{4} y^{2} z^{8} + 380 x^{4} y z^{9} + 96 x^{4} z^{10} + 64 x^{3} y^{11} + 216 x^{3} y^{10} z + 300 x^{3} y^{9} z^{2} \\
& + 330 x^{3} y^{8} z^{3} + 40 x^{3} y^{7} z^{4} + 262 x^{3} y^{6} z^{5} + 122 x^{3} y^{5} z^{6} + 232 x^{3} y^{4} z^{7} + 306 x^{3} y^{3} z^{8} \\
& + 248 x^{3} y^{2} z^{9} + 440 x^{3} y z^{10} + 320 x^{2} y^{12} + 88 x^{2} y^{11} z + 120 x^{2} y^{10} z^{2} + 420 x^{2} y^{9} z^{3} \\
& + 177 x^{2} y^{8} z^{4} + 496 x^{2} y^{7} z^{5} + 450 x^{2} y^{6} z^{6} + 36 x^{2} y^{5} z^{7} + 93 x^{2} y^{4} z^{8} + 400 x^{2} y^{3} z^{9} \\
& + 504 x^{2} y^{2} z^{10} + 48 x^{2} y z^{11} + 384 x^{2} z^{12} + 256 x y^{13} + 64 x y^{12} z + 168 x y^{11} z^{2} \\
& + 256 x y^{10} z^{3} + 86 x y^{9} z^{4} + 188 x y^{8} z^{5} + 476 x y^{7} z^{6} + 304 x y^{6} z^{7} + 126 x y^{5} z^{8} \\
& + 260 x y^{4} z^{9} + 8 x y^{3} z^{10} + 400 x y^{2} z^{11} + 32 x y z^{12} + 128 y^{12} z^{2} + 256 y^{11} z^{3} \\
& + 480 y^{10} z^{4} + 64 y^{9} z^{5} + 96 y^{6} z^{8} + 64 y^{5} z^{9} + 64 y^{4} z^{10} + 128 y^{3} z^{11} + 256 y^{2} z^{12}
\end{aligned}
\tag{1}
$$

```
> #reduce this polynomial mod 8
> f := mod(f, 8);
```

$$
\begin{aligned}
f := {} & 6 x^{9} y^{4} z + 4 x^{9} y^{3} z^{2} + 4 x^{9} y^{2} z^{3} + 6 x^{9} y z^{4} + 2 x^{8} y^{5} z + 7 x^{8} y^{4} z^{2} + 6 x^{8} y^{3} z^{3} \\
& + x^{8} y^{2} z^{4} + 4 x^{8} y z^{5} + 4 x^{7} y^{6} z + 4 x^{7} y^{4} z^{3} + 4 x^{7} y^{2} z^{5} + 4 x^{7} y z^{6} + 4 x^{6} y^{7} z \\
& + 2 x^{6} y^{6} z^{2} + 6 x^{6} y^{5} z^{3} + 6 x^{6} y^{3} z^{5} + 6 x^{6} y^{2} z^{6} + 6 x^{5} y^{8} z + 6 x^{5} y^{6} z^{3} + 2 x^{5} y^{5} z^{4} \\
& + 6 x^{5} y^{4} z^{5} + 2 x^{5} y^{3} z^{6} + 6 x^{5} y z^{8} + 2 x^{4} y^{9} z + 7 x^{4} y^{8} z^{2} + 4 x^{4} y^{6} z^{4} + 2 x^{4} y^{5} z^{5} \\
& + 4 x^{4} y^{4} z^{6} + 4 x^{4} y^{3} z^{7} + x^{4} y^{2} z^{8} + 4 x^{4} y z^{9} + 4 x^{3} y^{9} z^{2} + 2 x^{3} y^{8} z^{3} + 6 x^{3} y^{6} z^{5} \\
& + 2 x^{3} y^{5} z^{6} + 2 x^{3} y^{3} z^{8} + 4 x^{2} y^{9} z^{3} + x^{2} y^{8} z^{4} + 2 x^{2} y^{6} z^{6} + 4 x^{2} y^{5} z^{7} + 5 x^{2} y^{4} z^{8} \\
& + 6 x y^{9} z^{4} + 4 x y^{8} z^{5} + 4 x y^{7} z^{6} + 6 x y^{5} z^{8} + 4 x y^{4} z^{9}
\end{aligned}
\tag{2}
$$

```
> #multiply f by all the other units mod 8
> f1 := mod(3·f, 8) :
> f2 := mod(5·f, 8) :
> f3 := mod(7·f, 8) :
>
> #find all 4 linear factors mod 8 that are congruent to a factor coming from a line over Z4P2
> #lines congruent in Z2P2 have been grouped
> #store the coefficients of each line
>
> L := [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 := [ ] : M2 := [ ] : M3 := [ ] : M4 := [ ] :

  h1 := x :
  h2 := x + 2·y :
  h3 := x + 2·z :
  h4 := x + 2·y + 2·z :

  for i in L do:
  for j in L do:
  for k in L do:
  g := i·x + j·y + k·z :
  g1 := mod(g, 4) :
  if g1 = h1 then M1 := [op(M1), [i, j, k]] : fi:
   if g1 = h2 then M2 := [op(M2), [i, j, k]] : fi:
   if g1 = h3 then M3 := [op(M3), [i, j, k]] : fi:
   if g1 = h4 then M4 := [op(M4), [i, j, k]] : fi:
  od:od:od:

  PP := [ ] :
 U := [1, 3, 5, 7] :
  m := 8 :

  M := [M1, M2, M3, M4] :

  for Mi in M do:
  P := { } :
  for a in Mi do:

  a1 := a[1] : a2 := a[2] : a3 := a[3] :

  Q := {[a1, a2, a3]} :
  for u in U do:
   for b in Mi do:
  b1 := mod((u·b[1]), m) : b2 := mod((u·b[2]), m) : b3 := mod((u·b[3]), m) :
  if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then Q := Q ⋃ {[b[1], b[2], b[3]]} : fi:
  od:od:
  P := P ∪ {Q} :
  od:
  PP := [op(PP), P] :
  od:

  Q0 := [ ] : for i in PP[1] do: Q0 := [op(Q0), i[1]] : od: Q0;
  Q1 := [ ] :for i in PP[2] do: Q1 := [op(Q1), i[1]] :od: Q1;
```

```
Q2 := [ ] :for i in PP[3] do: Q2 := [op(Q2), i[1]] :od: Q2;
Q3 := [ ] : for i in PP[4] do: Q3 := [op(Q3), i[1]] :od: Q3;
QQ1 := [op(Q0), op(Q1), op(Q2), op(Q3)] :

                    [[1, 0, 0], [1, 0, 4], [1, 4, 0], [1, 4, 4]]
                    [[1, 2, 0], [1, 2, 4], [1, 6, 0], [1, 6, 4]]
                    [[1, 0, 2], [1, 0, 6], [1, 4, 2], [1, 4, 6]]
                    [[1, 2, 2], [1, 2, 6], [1, 6, 2], [1, 6, 6]]                    (3)
```

```
> #then with the 16 factors all congruent mod 2, find all the possible quadratics that are a product of
     two of these, store these in Ri
```

```
> R1 := { } :

  for i in QQ1 do:
  for j in QQ1 do:

  i1 := (i[1])·x + (i[2])·y + (i[3])·z :
  j1 := (j[1])·x + (j[2])·y + (j[3])·z :
  g := mod(expand(i1·j1), 8) :
  R1 := R1 ⋃ {g} :

  od:od:
```

```
>
```

```
> R1;
{x^2, x^2 + 4 y^2, x^2 + 2 x y, x^2 + 4 x y, x^2 + 6 x y, x^2 + 4 z^2, x^2 + 2 x z, x^2 + 4 x z, x^2 + 6 x z, x^2    (4)
   + 4 x y + 4 y^2, x^2 + 4 x z + 4 z^2, x^2 + 4 y^2 + 4 z^2, x^2 + 4 x z + 4 y^2, x^2 + 4 x y + 4 z^2, x^2
   + 2 x y + 2 x z, x^2 + 2 x y + 4 x z, x^2 + 2 x y + 6 x z, x^2 + 4 x y + 2 x z, x^2 + 4 x y
   + 4 x z, x^2 + 4 x y + 6 x z, x^2 + 6 x y + 2 x z, x^2 + 6 x y + 4 x z, x^2 + 6 x y + 6 x z, x^2
   + 4 x z + 4 y^2 + 4 z^2, x^2 + 2 x z + 4 y^2 + 4 y z, x^2 + 6 x z + 4 y^2 + 4 y z, x^2 + 2 x y
   + 4 y z + 4 z^2, x^2 + 6 x y + 4 y z + 4 z^2, x^2 + 4 x y + 4 y^2 + 4 z^2, x^2 + 4 x y + 4 x z
   + 4 z^2, x^2 + 2 x y + 2 x z + 4 y z, x^2 + 2 x y + 6 x z + 4 y z, x^2 + 6 x y + 2 x z + 4 y z, x^2
   + 6 x y + 6 x z + 4 y z, x^2 + 4 x y + 4 x z + 4 y^2, x^2 + 2 x y + 4 x z + 4 y z + 4 z^2, x^2
   + 6 x y + 4 x z + 4 y z + 4 z^2, x^2 + 4 x y + 4 x z + 4 y^2 + 4 z^2, x^2 + 4 x y + 2 x z + 4 y^2
   + 4 y z, x^2 + 4 x y + 6 x z + 4 y^2 + 4 y z}
```

```
> L := [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 := [ ] : M2 := [ ] : M3 := [ ] : M4 := [ ] :

  h1 := y :
  h2 := 2· x + y :
  h3 := y + 2·z :
  h4 := 2· x + y + 2·z :
```

```
for i in L do:
for j in L do:
for k in L do:
g := i·x + j·y + k·z :
g1 := mod(g, 4) :
if g1 = h1 then M1 := [op(M1), [i, j, k]] : fi:
 if g1 = h2 then M2 := [op(M2), [i, j, k]] : fi:
 if g1 = h3 then M3 := [op(M3), [i, j, k]] : fi:
 if g1 = h4 then M4 := [op(M4), [i, j, k]] : fi:
od:od:od:

PP := [ ] :
U := [1, 3, 5, 7] :
m := 8 :

M := [M1, M2, M3, M4] :

for Mi in M do:
P := { } :
for a in Mi do:

a1 := a[1] : a2 := a[2] : a3 := a[3] :

Q := {[a1, a2, a3]} :
for u in U do:
 for b in Mi do:
b1 := mod((u·b[1]), m) : b2 := mod((u·b[2]), m) : b3 := mod((u·b[3]), m) :
if ((a1 = b1) and (a2 = b2) and (a3 = b3)) then Q := Q ∪ {[b[1], b[2], b[3]]} : fi:
od:od:
P := P∪ {Q} :
od:
PP := [op(PP), P] :
od:

Q4 := [ ] :for i in PP[1] do: Q4 := [op(Q4), i[1]] :od: Q4;
Q5 := [ ] :for i in PP[2] do: Q5 := [op(Q5), i[1]] :od: Q5;
Q6 := [ ] :for i in PP[3] do: Q6 := [op(Q6), i[1]] :od: Q6;
Q7 := [ ] :for i in PP[4] do: Q7 := [op(Q7), i[1]] :od: Q7;
QQ2 := [op(Q4), op(Q5), op(Q6), op(Q7)] :
```

```
                    [[0, 1, 0], [0, 1, 4], [4, 1, 0], [4, 1, 4]]
                    [[2, 1, 0], [2, 1, 4], [6, 1, 0], [6, 1, 4]]
                    [[0, 1, 2], [0, 1, 6], [4, 1, 2], [4, 1, 6]]
                    [[2, 1, 2], [2, 1, 6], [6, 1, 2], [6, 1, 6]]          (5)
```

```
> R2 := { } :
```

```
for i in QQ2 do:
for j in QQ2 do:

i1 := (i[1])·x + (i[2])·y + (i[3])·z :
 j1 := (j[1])·x + (j[2])·y + (j[3])·z :
 g := mod(expand(i1·j1), 8) :
R2 := R2 ⋃ {g} :

od:od:
```

```
> R2;
```

$$\begin{gathered}\{y^2, 2\,x\,y+y^2, 4\,x\,y+y^2, 6\,x\,y+y^2, 4\,x^2+y^2, y^2+4\,z^2, y^2+2\,y\,z, y^2+4\,y\,z, y^2+6\,y\,z, \\ 4\,x^2+4\,x\,y+y^2, y^2+4\,y\,z+4\,z^2, 4\,x\,y+y^2+4\,z^2, 2\,x\,y+y^2+2\,y\,z, 2\,x\,y+y^2 \\ +4\,y\,z, 2\,x\,y+y^2+6\,y\,z, 4\,x\,y+y^2+2\,y\,z, 4\,x\,y+y^2+4\,y\,z, 4\,x\,y+y^2+6\,y\,z, 6\,x\,y \\ +y^2+2\,y\,z, 6\,x\,y+y^2+4\,y\,z, 6\,x\,y+y^2+6\,y\,z, 4\,x^2+y^2+4\,z^2, 4\,x^2+y^2+4\,y\,z, \\ 4\,x\,y+y^2+4\,y\,z+4\,z^2, 2\,x\,y+4\,x\,z+y^2+4\,z^2, 6\,x\,y+4\,x\,z+y^2+4\,z^2, 2\,x\,y+4\,x\,z \\ +y^2+2\,y\,z, 2\,x\,y+4\,x\,z+y^2+6\,y\,z, 6\,x\,y+4\,x\,z+y^2+2\,y\,z, 6\,x\,y+4\,x\,z+y^2 \\ +6\,y\,z, 4\,x^2+y^2+4\,y\,z+4\,z^2, 4\,x^2+4\,x\,z+y^2+2\,y\,z, 4\,x^2+4\,x\,z+y^2+6\,y\,z, 4\,x^2 \\ +4\,x\,y+y^2+4\,z^2, 4\,x^2+4\,x\,y+y^2+4\,y\,z, 2\,x\,y+4\,x\,z+y^2+4\,y\,z+4\,z^2, 6\,x\,y \\ +4\,x\,z+y^2+4\,y\,z+4\,z^2, 4\,x^2+4\,x\,y+y^2+4\,y\,z+4\,z^2, 4\,x^2+4\,x\,y+4\,x\,z+y^2 \\ +2\,y\,z, 4\,x^2+4\,x\,y+4\,x\,z+y^2+6\,y\,z\}\end{gathered} \qquad \textbf{(6)}$$

```
>
```

```
> nops(R2);
```

$$40 \qquad \textbf{(7)}$$

```
> L := [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 := [ ] : M2 := [ ] : M3 := [ ] : M4 := [ ] :

  h1 := z :
  h2 := 2· x + 2· y + z :
  h3 := 2·x + z :
  h4 := 2· y + z :

  for i in L do:
  for j in L do:
  for k in L do:
  g := i·x + j·y + k·z :
  g1 := mod(g, 4) :
  if g1 = h1 then M1 := [op(M1), [i, j, k]] : fi:
   if g1 = h2 then M2 := [op(M2), [i, j, k]] : fi:
   if g1 = h3 then M3 := [op(M3), [i, j, k]] : fi:
   if g1 = h4 then M4 := [op(M4), [i, j, k]] : fi:
  od:od:od:
```

```
PP := [ ] :
U := [1, 3, 5, 7] :
m := 8 :

M := [M1, M2, M3, M4] :

for Mi in M do:
P := { } :
for a in Mi do:

a1 := a[1] : a2 := a[2] : a3 := a[3] :

Q := {[a1, a2, a3]} :
for u in U do:
 for b in Mi do:
b1 := mod((u·b[1]), m) : b2 := mod((u·b[2]), m) : b3 := mod((u·b[3]), m) :
if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then Q := Q ⋃ {[b[1], b[2], b[3]]} : fi:
od:od:
P := P∪ {Q} :
od:
PP := [op(PP), P] :
od:

Q8 := [ ] :for i in PP[1] do: Q8 := [op(Q8), i[1]] :od: Q8;
Q9 := [ ] :for i in PP[2] do: Q9 := [op(Q9), i[1]] :od: Q9;
Q10 := [ ] :for i in PP[3] do: Q10 := [op(Q10), i[1]] :od: Q10;
Q11 := [ ] :for i in PP[4] do: Q11 := [op(Q11), i[1]] :od: Q11;
QQ3 := [op(Q8), op(Q9), op(Q10), op(Q11)] :
```

```
                    [[0, 0, 1], [0, 4, 1], [4, 0, 1], [4, 4, 1]]
                    [[2, 2, 1], [2, 6, 1], [6, 2, 1], [6, 6, 1]]
                    [[2, 0, 1], [2, 4, 1], [6, 0, 1], [6, 4, 1]]
                    [[0, 2, 1], [0, 6, 1], [4, 2, 1], [4, 6, 1]]          (8)
```

```
> R3 := { } :

for i in QQ3 do:
for j in QQ3 do:

i1 := (i[1])·x + (i[2])·y + (i[3])·z :
 j1 := (j[1])·x + (j[2])·y + (j[3])·z :
 g := mod(expand(i1·j1), 8) :
R3 := R3 ⋃ {g} :

od:od:
> R3;
```

$\{z^2, 2\,x\,z + z^2, 4\,x\,z + z^2, 6\,x\,z + z^2, 4\,x^2 + z^2, 2\,y\,z + z^2, 4\,y\,z + z^2, 6\,y\,z + z^2, 4\,y^2 + z^2,$ **(9)**

```
  4 x^2 + 4 x z + z^2, 4 y^2 + 4 y z + z^2, 2 x z + 2 y z + z^2, 2 x z + 4 y z + z^2, 2 x z + 6 y z
   + z^2, 4 x z + 2 y z + z^2, 4 x z + 4 y z + z^2, 4 x z + 6 y z + z^2, 6 x z + 2 y z + z^2, 6 x z      135
   + 4 y z + z^2, 6 x z + 6 y z + z^2, 4 x z + 4 y^2 + z^2, 4 x^2 + 4 y z + z^2, 4 x^2 + 4 y^2 + z^2,
  4 x z + 4 y^2 + 4 y z + z^2, 4 x y + 2 x z + 2 y z + z^2, 4 x y + 2 x z + 6 y z + z^2, 4 x y
   + 6 x z + 2 y z + z^2, 4 x y + 6 x z + 6 y z + z^2, 4 x y + 2 x z + 4 y^2 + z^2, 4 x y + 6 x z
   + 4 y^2 + z^2, 4 x^2 + 4 y^2 + 4 y z + z^2, 4 x^2 + 4 x z + 4 y z + z^2, 4 x^2 + 4 x z + 4 y^2 + z^2,
  4 x^2 + 4 x y + 2 y z + z^2, 4 x^2 + 4 x y + 6 y z + z^2, 4 x y + 2 x z + 4 y^2 + 4 y z + z^2, 4 x y
   + 6 x z + 4 y^2 + 4 y z + z^2, 4 x^2 + 4 x z + 4 y^2 + 4 y z + z^2, 4 x^2 + 4 x y + 4 x z + 2 y z
   + z^2, 4 x^2 + 4 x y + 4 x z + 6 y z + z^2}
```

```
> nops(R3);
                                    40                                         (10)
```

```
> L := [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 := [ ] : M2 := [ ] : M3 := [ ] : M4 := [ ] :

  h1 := x + z :
  h2 := x + 2· y + 3· z :
  h3 := x + 2·y + z :
  h4 := x + 3· z :

  for i in L do:
  for j in L do:
  for k in L do:
  g := i·x + j·y + k·z :
  g1 := mod(g, 4) :
  if g1 = h1 then M1 := [op(M1), [i, j, k]] : fi:
   if g1 = h2 then M2 := [op(M2), [i, j, k]] : fi:
   if g1 = h3 then M3 := [op(M3), [i, j, k]] : fi:
   if g1 = h4 then M4 := [op(M4), [i, j, k]] : fi:
  od:od:od:

  PP := [ ] :
 U := [1, 3, 5, 7] :
  m := 8 :

  M := [M1, M2, M3, M4] :

  for Mi in M do:
  P := { } :
  for a in Mi do:

  a1 := a[1] : a2 := a[2] : a3 := a[3] :

  Q := {[a1, a2, a3]} :
  for u in U do:
```

```
 for b in Mi do:
b1 := mod((u·b[1]), m) : b2 := mod((u·b[2]), m) : b3 := mod((u·b[3]), m) :
if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then  Q := Q ⋃  {[b[1], b[2], b[3]]} :  fi:

od:od:
P := P∪ {Q} :
od:
PP := [op(PP), P] :
od:

Q12 := [ ] :for i in PP[1] do: Q12 := [op(Q12), i[1]] :od: Q12;
Q13 := [ ] :for i in PP[2] do: Q13 := [op(Q13), i[1]] :od: Q13;
Q14 := [ ] :for i in PP[3] do: Q14 := [op(Q14), i[1]] :od: Q14;
Q15 := [ ] :for i in PP[4] do: Q15 := [op(Q15), i[1]] :od: Q15;
QQ4 := [op(Q12), op(Q13), op(Q14), op(Q15)] :
```

```
                    [[1, 0, 1], [1, 0, 5], [1, 4, 1], [1, 4, 5]]
                    [[1, 2, 3], [1, 2, 7], [1, 6, 3], [1, 6, 7]]
                    [[1, 2, 1], [1, 2, 5], [1, 6, 1], [1, 6, 5]]
                    [[1, 0, 3], [1, 0, 7], [1, 4, 3], [1, 4, 7]]                    (11)
```

```
> R4 := { } :

for i in QQ4 do:
for j in QQ4 do:

i1 := (i[1])·x + (i[2])·y + (i[3])·z :
 j1 := (j[1])·x + (j[2])·y + (j[3])·z :
 g := mod(expand(i1·j1), 8) :
R4 := R4 ⋃  {g} :
od:od:
```

```
> R4;
{x^2 + 7 z^2, x^2 + 2 x z + z^2, x^2 + 2 x z + 5 z^2, x^2 + 4 x z + 3 z^2, x^2 + 6 x z + z^2, x^2 + 6 x z      (12)
    + 5 z^2, x^2 + 4 y^2 + 4 y z + 7 z^2, x^2 + 2 x z + 4 y^2 + z^2, x^2 + 2 x z + 4 y^2 + 5 z^2, x^2
    + 6 x z + 4 y^2 + z^2, x^2 + 6 x z + 4 y^2 + 5 z^2, x^2 + 2 x y + 2 y z + 7 z^2, x^2 + 2 x y + 6 y z
    + 7 z^2, x^2 + 4 x y + 4 y z + 7 z^2, x^2 + 6 x y + 2 y z + 7 z^2, x^2 + 6 x y + 6 y z + 7 z^2, x^2
    + 4 x y + 4 y^2 + 7 z^2, x^2 + 4 x z + 4 y^2 + 4 y z + 3 z^2, x^2 + 2 x y + 2 x z + 2 y z + z^2, x^2
    + 2 x y + 2 x z + 6 y z + 5 z^2, x^2 + 2 x y + 4 x z + 2 y z + 3 z^2, x^2 + 2 x y + 4 x z + 6 y z
    + 3 z^2, x^2 + 2 x y + 6 x z + 2 y z + 5 z^2, x^2 + 2 x y + 6 x z + 6 y z + z^2, x^2 + 4 x y
    + 2 x z + 4 y z + z^2, x^2 + 4 x y + 2 x z + 4 y z + 5 z^2, x^2 + 4 x y + 4 x z + 4 y z + 3 z^2,
   x^2 + 4 x y + 6 x z + 4 y z + z^2, x^2 + 4 x y + 6 x z + 4 y z + 5 z^2, x^2 + 6 x y + 2 x z + 2 y z
```

$$+ 5\,z^{2}, x^{2} + 6\,x\,y + 2\,x\,z + 6\,y\,z + z^{2}, x^{2} + 6\,x\,y + 4\,x\,z + 2\,y\,z + 3\,z^{2}, x^{2} + 6\,x\,y$$
$$+ 4\,x\,z + 6\,y\,z + 3\,z^{2}, x^{2} + 6\,x\,y + 6\,x\,z + 2\,y\,z + z^{2}, x^{2} + 6\,x\,y + 6\,x\,z + 6\,y\,z + 5\,z^{2},$$
$$x^{2} + 4\,x\,y + 4\,x\,z + 4\,y^{2} + 3\,z^{2}, x^{2} + 4\,x\,y + 2\,x\,z + 4\,y^{2} + 4\,y\,z + z^{2}, x^{2} + 4\,x\,y + 2\,x\,z$$
$$+ 4\,y^{2} + 4\,y\,z + 5\,z^{2}, x^{2} + 4\,x\,y + 6\,x\,z + 4\,y^{2} + 4\,y\,z + z^{2}, x^{2} + 4\,x\,y + 6\,x\,z + 4\,y^{2}$$
$$+ 4\,y\,z + 5\,z^{2}\}$$

```
> nops(R4);
```

$$40 \qquad\qquad (13)$$

```
> L := [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 := [ ] : M2 := [ ] : M3 := [ ] : M4 := [ ] :

  h1 := x + y + z :
  h2 := x + y + 3·z :
  h3 := x + 3·y + 3·z :
  h4 := x + 3·y + z :

  for i in L do:
  for j in L do:
  for k in L do:
  g := i·x + j·y + k·z :
  g1 := mod(g, 4) :
  if g1 = h1 then M1 := [op(M1), [i, j, k]] : fi:
   if g1 = h2 then M2 := [op(M2), [i, j, k]] : fi:
   if g1 = h3 then M3 := [op(M3), [i, j, k]] : fi:
   if g1 = h4 then M4 := [op(M4), [i, j, k]] : fi:
  od:od:od:

  PP := [ ] :
 U := [1, 3, 5, 7] :
  m := 8 :

  M := [M1, M2, M3, M4] :

  for Mi in M do:
  P := { } :
  for a in Mi do:

  a1 := a[1] : a2 := a[2] : a3 := a[3] :

  Q := {[a1, a2, a3]} :
  for u in U do:
   for b in Mi do:
  b1 := mod((u·b[1]), m) : b2 := mod((u·b[2]), m) : b3 := mod((u·b[3]), m) :
  if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then Q := Q ⋃ {[b[1], b[2], b[3]]} : fi:
  od:od:
  P := P∪ {Q} :
    od:
    PP ≔ [op(PP), P]:
    od:

    Q16 ≔ [ ] :for i in PP[1] do: Q16 ≔ [op(Q16), i[1]] :od: Q16;
    Q17 ≔ [ ] :for i in PP[2] do: Q17 ≔ [op(Q17), i[1]] :od: Q17;
    Q18 ≔ [ ] :for i in PP[3] do: Q18 ≔ [op(Q18), i[1]] :od: Q18;
    Q19 ≔ [ ] :for i in PP[4] do: Q19 ≔ [op(Q19), i[1]] :od: Q19;
    QQ5 ≔ [op(Q16), op(Q17), op(Q18), op(Q19)] :

                        [[1, 1, 1], [1, 1, 5], [1, 5, 1], [1, 5, 5]]
                        [[1, 1, 3], [1, 1, 7], [1, 5, 3], [1, 5, 7]]
                        [[1, 3, 3], [1, 3, 7], [1, 7, 3], [1, 7, 7]]
                        [[1, 3, 1], [1, 3, 5], [1, 7, 1], [1, 7, 5]]                      (14)
> R5 ≔ { } :

    for i in QQ5 do:
    for j in QQ5 do:

    i1 ≔ (i[1])·x + (i[2])·y + (i[3])·z :
    j1 ≔ (j[1])·x + (j[2])·y + (j[3])·z :
    g ≔mod(expand(i1·j1), 8) :
    R5 ≔ R5 ∪ {g} :

    od:od:
> R5;
{x^2 + 7 y^2 + 2 y z + 7 z^2, x^2 + 7 y^2 + 6 y z + 7 z^2, x^2 + 2 x z + 7 y^2 + z^2, x^2 + 6 x z + 7 y^2     (15)
   + z^2, x^2 + 2 x y + y^2 + 7 z^2, x^2 + 6 x y + y^2 + 7 z^2, x^2 + 2 x z + 7 y^2 + 4 y z + 5 z^2, x^2
   + 4 x z + 7 y^2 + 2 y z + 3 z^2, x^2 + 4 x z + 7 y^2 + 6 y z + 3 z^2, x^2 + 6 x z + 7 y^2 + 4 y z
   + 5 z^2, x^2 + 2 x y + 5 y^2 + 4 y z + 7 z^2, x^2 + 4 x y + 3 y^2 + 2 y z + 7 z^2, x^2 + 4 x y
   + 3 y^2 + 6 y z + 7 z^2, x^2 + 6 x y + 5 y^2 + 4 y z + 7 z^2, x^2 + 2 x y + 4 x z + 5 y^2 + 3 z^2,
  x^2 + 4 x y + 2 x z + 3 y^2 + 5 z^2, x^2 + 4 x y + 6 x z + 3 y^2 + 5 z^2, x^2 + 6 x y + 4 x z + 5 y^2
   + 3 z^2, x^2 + 2 x y + 2 x z + y^2 + 2 y z + z^2, x^2 + 2 x y + 2 x z + y^2 + 2 y z + 5 z^2, x^2
   + 2 x y + 2 x z + 5 y^2 + 2 y z + z^2, x^2 + 2 x y + 2 x z + 5 y^2 + 2 y z + 5 z^2, x^2 + 2 x y
   + 4 x z + y^2 + 4 y z + 3 z^2, x^2 + 2 x y + 6 x z + y^2 + 6 y z + z^2, x^2 + 2 x y + 6 x z + y^2
   + 6 y z + 5 z^2, x^2 + 2 x y + 6 x z + 5 y^2 + 6 y z + z^2, x^2 + 2 x y + 6 x z + 5 y^2 + 6 y z
   + 5 z^2, x^2 + 4 x y + 2 x z + 3 y^2 + 4 y z + z^2, x^2 + 4 x y + 4 x z + 3 y^2 + 2 y z + 3 z^2, x^2
   + 4 x y + 4 x z + 3 y^2 + 6 y z + 3 z^2, x^2 + 4 x y + 6 x z + 3 y^2 + 4 y z + z^2, x^2 + 6 x y
   + 2 x z + y^2 + 6 y z + z^2, x^2 + 6 x y + 2 x z + y^2 + 6 y z + 5 z^2, x^2 + 6 x y + 2 x z + 5 y^2
   + 6 y z + z^2, x^2 + 6 x y + 2 x z + 5 y^2 + 6 y z + 5 z^2, x^2 + 6 x y + 4 x z + y^2 + 4 y z
```

$$+ 3 z^2, x^2 + 6 x y + 6 x z + y^2 + 2 y z + z^2, x^2 + 6 x y + 6 x z + y^2 + 2 y z + 5 z^2, x^2 + 6 x y + 6 x z + 5 y^2 + 2 y z + z^2, x^2 + 6 x y + 6 x z + 5 y^2 + 2 y z + 5 z^2\} \qquad 139$$

```
> nops(R5);
```

$$40 \qquad \textbf{(16)}$$

```
> L := [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 := [ ] : M2 := [ ] : M3 := [ ] : M4 := [ ] :

  h1 := y + z :
  h2 := 2· x + y + 3· z :
  h3 := 2· x + y +  z :
  h4 := y + 3· z :

  for i in L do:
  for j in L do:
  for k in L do:
  g := i·x + j·y + k·z :
  g1 := mod(g, 4) :
  if g1 = h1 then M1 := [op(M1), [i, j, k]] : fi:
   if g1 = h2 then M2 := [op(M2), [i, j, k]] : fi:
   if g1 = h3 then M3 := [op(M3), [i, j, k]] : fi:
   if g1 = h4 then M4 := [op(M4), [i, j, k]] : fi:
  od:od:od:

  PP := [ ] :
 U := [1, 3, 5, 7] :
  m := 8 :

  M := [M1, M2, M3, M4] :

  for Mi in M do:
  P := { } :
  for a in Mi do:

  a1 := a[1] : a2 := a[2] : a3 := a[3] :

  Q := {[a1, a2, a3]} :
  for u in U do:
   for b in Mi do:
  b1 := mod((u·b[1]), m) : b2 := mod((u·b[2]), m) : b3 := mod((u·b[3]), m) :
  if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then  Q := Q ∪ {[b[1], b[2], b[3]]} :  fi:
  od:od:
  P := P∪ {Q} :
  od:
  PP := [op(PP), P] :
  od:
```

```
Q20 := [ ] :for i in PP[1] do: Q20 := [op(Q20), i[1]] :od: Q20;
Q21 := [ ] :for i in PP[2] do: Q21 := [op(Q21), i[1]] :od: Q21;
Q22 := [ ] :for i in PP[3] do: Q22 := [op(Q22), i[1]] :od: Q22;
Q23 := [ ] :for i in PP[4] do: Q23 := [op(Q23), i[1]] :od: Q23;
QQ6 := [op(Q20), op(Q21), op(Q22), op(Q23)] :
```

```
                    [[0, 1, 1], [0, 1, 5], [4, 1, 1], [4, 1, 5]]
                    [[2, 1, 3], [2, 1, 7], [6, 1, 3], [6, 1, 7]]
                    [[2, 1, 1], [2, 1, 5], [6, 1, 1], [6, 1, 5]]
                    [[0, 1, 3], [0, 1, 7], [4, 1, 3], [4, 1, 7]]          (17)
```

```
> R6 := { } :

  for i in QQ6 do:
  for j in QQ6 do:

  i1 := (i[1])·x + (i[2])·y + (i[3])·z :
  j1 := (j[1])·x + (j[2])·y + (j[3])·z :
  g := mod(expand(i1·j1), 8) :
  R6 := R6 ⋃ {g} :
  od:od:
```

```
> R6;
{y^2 + 7 z^2, y^2 + 2 y z + z^2, y^2 + 2 y z + 5 z^2, y^2 + 4 y z + 3 z^2, y^2 + 6 y z + z^2, y^2 + 6 y z      (18)
   + 5 z^2, 2 x y + 2 x z + y^2 + 7 z^2, 2 x y + 6 x z + y^2 + 7 z^2, 4 x y + 4 x z + y^2 + 7 z^2, 6 x y
   + 2 x z + y^2 + 7 z^2, 6 x y + 6 x z + y^2 + 7 z^2, 4 x^2 + y^2 + 2 y z + z^2, 4 x^2 + y^2 + 2 y z
   + 5 z^2, 4 x^2 + y^2 + 6 y z + z^2, 4 x^2 + y^2 + 6 y z + 5 z^2, 4 x^2 + 4 x z + y^2 + 7 z^2, 4 x^2
   + 4 x y + y^2 + 7 z^2, 2 x y + 2 x z + y^2 + 2 y z + z^2, 2 x y + 2 x z + y^2 + 4 y z + 3 z^2,
  2 x y + 2 x z + y^2 + 6 y z + 5 z^2, 2 x y + 6 x z + y^2 + 2 y z + 5 z^2, 2 x y + 6 x z + y^2
   + 4 y z + 3 z^2, 2 x y + 6 x z + y^2 + 6 y z + z^2, 4 x y + 4 x z + y^2 + 2 y z + z^2, 4 x y
   + 4 x z + y^2 + 2 y z + 5 z^2, 4 x y + 4 x z + y^2 + 4 y z + 3 z^2, 4 x y + 4 x z + y^2 + 6 y z
   + z^2, 4 x y + 4 x z + y^2 + 6 y z + 5 z^2, 6 x y + 2 x z + y^2 + 2 y z + 5 z^2, 6 x y + 2 x z
   + y^2 + 4 y z + 3 z^2, 6 x y + 2 x z + y^2 + 6 y z + z^2, 6 x y + 6 x z + y^2 + 2 y z + z^2, 6 x y
   + 6 x z + y^2 + 4 y z + 3 z^2, 6 x y + 6 x z + y^2 + 6 y z + 5 z^2, 4 x^2 + 4 x z + y^2 + 4 y z
   + 3 z^2, 4 x^2 + 4 x y + y^2 + 4 y z + 3 z^2, 4 x^2 + 4 x y + 4 x z + y^2 + 2 y z + z^2, 4 x^2
   + 4 x y + 4 x z + y^2 + 2 y z + 5 z^2, 4 x^2 + 4 x y + 4 x z + y^2 + 6 y z + z^2, 4 x^2 + 4 x y
   + 4 x z + y^2 + 6 y z + 5 z^2}
```

```
> nops(R6);
                                       40                                  (19)
```

```
> L ≔ [0, 1, 2, 3, 4, 5, 6, 7] :
  M1 ≔ [ ] : M2 ≔ [ ] : M3 ≔ [ ] : M4 ≔ [ ] :

  h1 ≔ x + y :
  h2 ≔ x + y + 2· z :
  h3 ≔ x + 3· y :
  h4 ≔ x + 3·y + 2 z :

  for i in L do:
  for j in L do:
  for k in L do:
  g ≔ i·x + j·y + k·z :
  g1 ≔ mod(g, 4) :
  if g1 = h1 then M1 ≔ [op(M1), [i, j, k]] : fi:
   if g1 = h2 then M2 ≔ [op(M2), [i, j, k]] : fi:
   if g1 = h3 then M3 ≔ [op(M3), [i, j, k]] : fi:
   if g1 = h4 then M4 ≔ [op(M4), [i, j, k]] : fi:
  od:od:od:

  PP ≔ [ ] :
 U ≔ [1, 3, 5, 7] :
  m ≔ 8 :

  M ≔ [M1, M2, M3, M4] :

  for Mi in M do:
  P ≔ { } :
  for a in Mi do:

  a1 ≔ a[1] : a2 ≔ a[2] : a3 ≔ a[3] :

  Q ≔ {[a1, a2, a3]} :
  for u in U do:
   for b in Mi do:
  b1 ≔ mod((u·b[1]), m) : b2 ≔ mod((u·b[2]), m) : b3 ≔ mod((u·b[3]), m) :
  if ((a1 = b1) and (a2 = b2) and (a3 = b3) ) then Q ≔ Q ⋃ {[b[1], b[2], b[3]]} : fi:
  od:od:
  P ≔ P∪ {Q} :
  od:
  PP ≔ [op(PP), P] :
  od:

  Q24 ≔ [ ] :for i in PP[1] do: Q24 ≔ [op(Q24), i[1]] :od: Q24;
  Q25 ≔ [ ] :for i in PP[2] do: Q25 ≔ [op(Q25), i[1]] :od: Q25;
  Q26 ≔ [ ] :for i in PP[3] do: Q26 ≔ [op(Q26), i[1]] :od: Q26;
  Q27 ≔ [ ] :for i in PP[4] do: Q27 ≔ [op(Q27), i[1]] :od: Q27;
  QQ7 ≔ [op(Q24), op(Q25), op(Q26), op(Q27)] :
```

```
[[1, 1, 0], [1, 1, 4], [1, 5, 0], [1, 5, 4]]
[[1, 1, 2], [1, 1, 6], [1, 5, 2], [1, 5, 6]]
[[1, 3, 0], [1, 3, 4], [1, 7, 0], [1, 7, 4]]
[[1, 3, 2], [1, 3, 6], [1, 7, 2], [1, 7, 6]]                    (20)
```

```
> R7 := { } :

   for i in QQ7 do:
   for j in QQ7 do:

   i1 := (i[1])·x + (i[2])·y + (i[3])·z :
   j1 := (j[1])·x + (j[2])·y + (j[3])·z :
   g := mod(expand(i1·j1), 8) :
   R7 := R7 ⋃ {g} :

   od:od:
```

```
> R7;
{x^2 + 7 y^2, x^2 + 2 x y + y^2, x^2 + 2 x y + 5 y^2, x^2 + 4 x y + 3 y^2, x^2 + 6 x y + y^2, x^2 + 6 x y      (21)
   + 5 y^2, x^2 + 7 y^2 + 4 y z + 4 z^2, x^2 + 4 x z + 7 y^2 + 4 z^2, x^2 + 2 x z + 7 y^2 + 2 y z, x^2
   + 2 x z + 7 y^2 + 6 y z, x^2 + 4 x z + 7 y^2 + 4 y z, x^2 + 6 x z + 7 y^2 + 2 y z, x^2 + 6 x z
   + 7 y^2 + 6 y z, x^2 + 2 x y + y^2 + 4 z^2, x^2 + 2 x y + 5 y^2 + 4 z^2, x^2 + 6 x y + y^2 + 4 z^2, x^2
   + 6 x y + 5 y^2 + 4 z^2, x^2 + 4 x y + 3 y^2 + 4 y z + 4 z^2, x^2 + 4 x y + 4 x z + 3 y^2 + 4 z^2,
  x^2 + 2 x y + 2 x z + y^2 + 2 y z, x^2 + 2 x y + 2 x z + 5 y^2 + 6 y z, x^2 + 2 x y + 4 x z + y^2
   + 4 y z, x^2 + 2 x y + 4 x z + 5 y^2 + 4 y z, x^2 + 2 x y + 6 x z + y^2 + 6 y z, x^2 + 2 x y
   + 6 x z + 5 y^2 + 2 y z, x^2 + 4 x y + 2 x z + 3 y^2 + 2 y z, x^2 + 4 x y + 2 x z + 3 y^2
   + 6 y z, x^2 + 4 x y + 4 x z + 3 y^2 + 4 y z, x^2 + 4 x y + 6 x z + 3 y^2 + 2 y z, x^2 + 4 x y
   + 6 x z + 3 y^2 + 6 y z, x^2 + 6 x y + 2 x z + y^2 + 6 y z, x^2 + 6 x y + 2 x z + 5 y^2 + 2 y z,
  x^2 + 6 x y + 4 x z + y^2 + 4 y z, x^2 + 6 x y + 4 x z + 5 y^2 + 4 y z, x^2 + 6 x y + 6 x z + y^2
   + 2 y z, x^2 + 6 x y + 6 x z + 5 y^2 + 6 y z, x^2 + 2 x y + 4 x z + y^2 + 4 y z + 4 z^2, x^2
   + 2 x y + 4 x z + 5 y^2 + 4 y z + 4 z^2, x^2 + 6 x y + 4 x z + y^2 + 4 y z + 4 z^2, x^2 + 6 x y
   + 4 x z + 5 y^2 + 4 y z + 4 z^2}
```

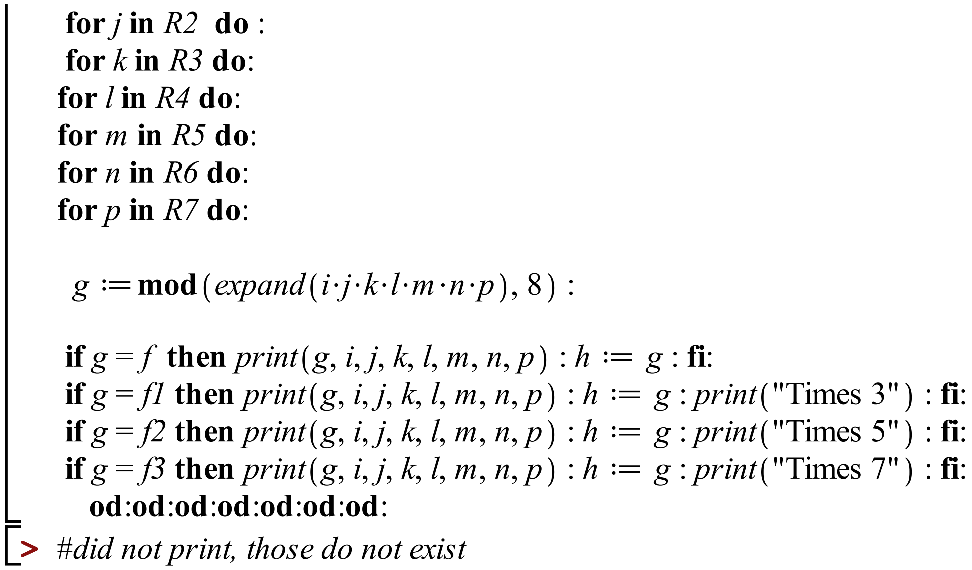
```
>
```

```
> nops(R7);
                              40                                (22)
```

```
> #take a quadratic from each set and multiply these to get a degree 14 polynomial, and check if it is
     congruent to f and f times a unit mod 8
```

```
> h := 0 :

  for i in R1 do:
```



```
 for j in R2  do :
 for k in R3 do:
for l in R4 do:
for m in R5 do:
for n in R6 do:
for p in R7 do:

 g ≔ mod(expand(i·j·k·l·m·n·p), 8) :

 if g = f  then print(g, i, j, k, l, m, n, p) : h ≔ g : fi:
 if g = f1 then print(g, i, j, k, l, m, n, p) : h ≔ g : print("Times 3") : fi:
 if g = f2 then print(g, i, j, k, l, m, n, p) : h ≔ g : print("Times 5") : fi:
 if g = f3 then print(g, i, j, k, l, m, n, p) : h ≔ g : print("Times 7") : fi:
   od:od:od:od:od:od:od:
> #did not print, those do not exist
```