Aspects of Order, Relative Primeness and Quotient Ring Structure for Polynomials over Integer Rings

By

Bridget Anne Walshe
B Sc , University of Victoria, 1999

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Mathematics and Statistics

We accept this thesis as conforming
to the required standard

[redacted]

Dr C R Miers, Supervisor (Department of Mathematics & Statistics)

[redacted]

Dr G MacGillivray, Departmental Member (Department of Mathematics & Statistics)

[redacted]

Dr M Serra, Outside Member (Department of Computer Science)

[redacted]

Dr A Gulliver, External Examiner (Department of Electrical & Computer Engineering)

Supervisor Dr C R Miers

Abstract

Many aspects of polynomials over finite fields have been studied In this thesis we prove results for polynomials over integer rings that are analogous to known results regarding polynomials over finite fields A definition of relatively prime for two polynomials over an integer ring is given Linear algebra and the theory of resultants are used to give two proofs for necessary and sufficient conditions for two polynomials to be relatively prime over certain integer rings We then examine the quotient ring formed by the ring of polynomials over an integer ring mod a monic polynomial f The existence of an order for certain polynomials over the integers mod n is exhibited and a bound is given for the maximum order of polynomials over the integers mod 2^k Finally, we prove theorems that can be used to simplify the calculation of the order of particular polynomials

Examiners

[redacted]

Dr C R Miers, Supervisor (Department of Mathematics & Statistics)

[redacted]

Dr G J MacGillivray, Departmental Member (Department of Mathematics & Statistics)

[redacted]

Dr M Serra, Outside Member (Department of Computer Science)

[redacted]

Dr A Gulliver, External Examiner (Department of Electrical & Computer Engineering)

Contents

List of Tables

Acknowledgements

I would like to thank my supervisor Dr Bob Miers He provided me with the ideas I needed to get started and gave me new directions when I was at an impasse

To Dr Gary MacGillivray and Dr Micaela Serra, my committee members, and to the external examiner Dr Aaron Gulliver, thank you for carefully reading my thesis and providing me with advice for the final draft

Dedication

To Noelle Sisk

CHAPTER 1 INTRODUCTION

The structure of finite fields and the behavior of polynomials over those fields are topics that have been thoroughly researched. There are also many applications of the theory of polynomials over finite fields. However, computations involving finite fields are large and complex. Calculations involving integer rings with operations of addition and multiplication modulo n are more transparent, but if n is not prime, the integer ring Z_n has zero divisors and is not a field. A particular drawback to this is that if n is not prime, only a weak version of the division algorithm is available in the polynomial ring $Z_n[x]$. Nevertheless, the calculation of tables of polynomials of small degree with coefficients in Z_n for small values of n, indicates the presence of a structure theory for $Z_n[x]$, which has certain analogies with that of $GF(q)[x]$. This thesis presents theorems regarding the behavior of polynomials over integer rings that are analogous to existing theorems for polynomials over finite fields. As a small example, the tables empirically predict the existence of the "order" for a monic polynomial in $Z_n[x]$ whose constant term is a unit. At the beginning of Chapter 5, we prove the existence of this order.

Chapter 2 is intended to provide the reader with enough algebraic background to understand the subsequent chapters. Section 2.1 gives the basic definitions and results from algebra that are referred to in this thesis. In Section 2.2 the integer rings Z_n and polynomials over these rings are discussed. These concepts are fundamental for the content of the following chapters. Section 2.3 provides a short background in matrices and linear systems with coefficients in a commutative ring with identity.

In Chapter 3 we define what it means for a pair of polynomials in $Z_n[x]$ to be relatively prime. To wit, $f(x)$ and $g(x)$ are relatively prime in $Z_n[x]$ if there are $s(x)$

and $t(x)$ in $Z_n[x]$ such that $1 = f(x)s(x) + g(x)t(x)$ Our major result in this chapter gives a necessary and sufficient condition, in terms of "reduction of coefficients homomorphisms", for polynomials to be relatively prime A second proof of this result is given by expanding a proof in [C] This second proof provides a method for finding $s(x)$ and $t(x)$

In Chapter 4 the results of Chapter 3 are used to shed light on the group of invertible elements (units) in the quotient ring $Z_n[x]/ < f >$ Here we only assume that $f(x)$ is monic in $Z_n[x]$ The units in this quotient ring are closely related to the polynomials that are relatively prime to $f(x)$ The sharpest results occur when $n = p^k$, p a prime We believe that the main results in this section are new

In Chapter 5 we prove the existence of an order for monic polynomials $f(x)$ in $Z_n[x]$ with $f(0)$ a unit In Section 5 2 known results regarding polynomials over finite fields are used to produce a bound for the order of polynomials over Z_2 In Section 5 3 this bound is generalized to polynomials over the integers mod 2^k This result is also thought to be new In Section 5 4 the calculation of the order of a polynomial is discussed in light of previous results in Chapter 4 and Chapter 5

Finally, Chapter 6 gives suggestions for future study based on the results presented in this thesis and results found in the research process

CHAPTER 2. ALGEBRAIC PRELIMINARIES

2.1 Definitions and Basic Theorems

Most of the definitions and theorems given later in this thesis involve special cases of the following basic algebraic preliminaries. Concrete examples of these objects and their properties will be included as the special cases are introduced. See [G] for a discussion of some of the basic concepts and results.

Definition 2.1.1. A *group* is a nonempty set G and a closed binary operation * defined on G such that

(i) For each $a,b,c \in G$ $a*(b*c) = (a*b)*c$, that is * is associative.

(ii) There exists an identity $1 \in G$ so that for each $a \in G$ $a*1 = a = 1*a$.

(iii) For each $a \in G$ there exists $b \in G$ with $a*b = 1 = b*a$. b is called the inverse of a and is usually denoted a^{-1}.

If the binary operation is denoted *, the group G with operation * is denoted $(G,*)$. We will frequently write ab instead of $a*b$ if no confusion can arise.

If the operation * is commutative for all elements, G is said to be an *abelian* group.

Definition 2.1.2. The *order* of a group G, denoted $\text{ord}(G)$ is the cardinality of the set G.

Definition 2.1.3. A nonempty subset H of G is a *subgroup* if it is a group with the operation inherited from G.

Consider an element a of a group G. Let $< a >= \{a^k | k \in Z\}$ where $a^0 = 1$ and $a^{-k} = (a^{-1})^k$ for positive k. The set $< a >$ is a subgroup of G [G, pp 41].

Definition 2.1.4. Let G be a group written multiplicatively with identity 1 and let $a \in G$. The subgroup $< a >= \{a^k | k \in Z\}$ is called the *cyclic subgroup generated by a*. The *order of a*, denoted $\text{ord}(a)$, is the cardinality of $< a >$.

If $\text{ord}(a)$ is finite then $\text{ord}(a)$ is the smallest positive integer t such that $a^t = 1$.

Theorem 2.1.5. (Lagrange's Theorem) *Let G be a finite group. If H is any subgroup of G then* $\text{ord}(H) | \text{ord}(G)$.

As a consequence if G is finite and $a \in G$ then $\text{ord}(a) | \text{ord}(G)$. If $\text{ord}(a) = s$ and $\text{ord}(G) = st$, then $a^{ord(G)} = a^{st} = (a^s)^t = 1^t = 1$.

Definition 2.1.6. A *ring* is a nonempty set R with binary operations of addition and multiplication defined on R, denoted + and by or by juxtaposition, such that

(i) (R,+) is an abelian group with identity 0.

(ii) For each $a,b,c \in R$ $a(bc) = (ab)c$, that is multiplication is associative.

(iii) The left and right distribution laws hold: $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a,b,c \in R$.

If the operation of multiplication commutes for all elements, R is said to be a *commutative ring*. If there exists an element $1 \in R$ such that $1(a) = (a)1 = a$ for all $a \neq 0$, that is R has a multiplicative identity, then we say R is a ring with identity.

Definition 2.1.7. Let R be a ring with identity 1 and let $a \in R$. If a has a multiplicative inverse, an element a^{-1} of R such that $a^{-1}a = 1 = aa^{-1}$, then a is called a *unit*. The set of all units in R is denoted $U(R)$.

Notice that $1 \in U(R)$ and if $a \in U(R)$ then $a^{-1} \in U(R)$ since $(a^{-1})^{-1} = a$. Moreover, if $a, b \in U(R)$ then $(ab)^{-1} = b^{-1}a^{-1}$ so $ab \in U(R)$. So since multiplication is associative by the definition of a ring, $U(R)$ is a multiplicative group [Gr, pp 49]. $U(R)$ is called the *group of units* of R.

Definition 2.1.8. Let R be a commutative ring with identity 1. If a and b are non-zero elements of R with $ab = 0$, then a and b are said to be *zero divisors*. R is called an *integral domain* if it contains no zero divisors.

Definition 2.1.9. Let R be a commutative ring with identity 1. If every non-zero element of R is a unit, then R is a *field*.

Thus if F is a field, the set $F \setminus \{0\}$, is an abelian group with respect to multiplication.

Let F be any field. Suppose a and b are non-zero elements of F, such that $ab = 0$. Since F is a field we have $b = a^{-1}ab = a^{-1}0 = 0$, a contradiction since b is non-zero. Thus every field is an integral domain.

If R is any ring, the set of polynomials over R can be defined in the usual sense.

Definition 2.1.10. A *polynomial over a ring* R is an expression of the form $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ where $a_0, \ldots, a_m \in R$ and m is a positive integer. Let $R[x]$ denote the set of all such polynomials. $R[x]$, along with usual polynomial multiplication and addition is a ring called the polynomial ring over R [LN, pp 19].

If $f(x) = a_0 + a_1 x + a_2 x^2 + \quad + a_m x^m$ the *degree of f*, denoted deg(f) is the largest integer i such that $a_i \neq 0$ This coefficient a_i is referred to as the *lead coefficient* of f A *monic* polynomial is one whose lead coefficient is equal to 1 A polynomial $f(x)$ is the zero polynomial if and only if $a_i = 0$ for all i

Many of the properties of the ring R are inherited by the polynomial ring $R[x]$

Theorem 2.1 11. [LN, pp 20] *Let R be a ring Then*

(i) $R[x]$ *is commutative if and only if R is commutative*

(ii) $R[x]$ *is a ring with identity if and only if R is a ring with identity*

(iii) $R[x]$ *is an integral domain if and only if R is an integral domain*

When the ring R is a field, the usual Euclidean division algorithm holds for $R[x]$ That is, if F is a field with $f, g \in F[x]$, then there exist polynomials $q, r \in F[x]$ such that

$f(x) = g(x)q(x) + r(x)$ with $\deg(r) < \deg(f)$ or $r(x) = 0$

If F is a field, a polynomial $f \in F[x]$ is called *irreducible* if there no polynomials g and h over F such that $f(x) = g(x)h(x)$, $1 \leq \deg(g), \deg(h)$ For a field F, the polynomial ring $F[x]$ is a unique factorization domain That is every element of $F[x]$ can be written uniquely as a product of irreducible elements

Functions from one ring into another which preserve operations are referred to as homomorphisms

Definition 2.1.12. Let R and S be rings If $\varphi \quad R \to S$ is a function such that

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ and,

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

for all $a, b \in R$ Then φ is a *homomorphism of rings* If φ is a bijection, then φ is called an *isomorphism*, and R and S are said to be *isomorphic*

2.2 The Rings Z_n and $Z_n[x]$

Let n be a positive integer. Define a relation of congruence on the integers by $a \equiv b \pmod{n}$ if and only if $n|(a-b)$. Congruence is an equivalence relation on Z [G, pp 44]. If $Z_n = \{[0],[1], \ldots,[n-1]\}$ where $[i] = \{a | a \equiv i \pmod{n}\}$, then Z_n is a partition of Z into equivalence classes. When two or more sets Z_m and Z_n are discussed, the classes are usually indexed $[a]_m$ and $[a]_n$ respectively.

Theorem 2.2.1. [G, pp 144] *Let n be a positive integer. Define addition and multiplication on Z_n as follows:*

(i) $[a]+[b] = [a+b]$,

(ii) $[a][b] = [ab]$.

Then Z_n is a commutative ring with additive identity [0] and multiplicative identity [1].

Example 2.2.2. $Z_{16} = \{[0],[1],[2], \ldots,[15]\}$

Examples of operations on Z_{16} include:

$[0]+[2] = [2]$

$[4][4] = [16] = [0]$

$[3][11] = [33] = [1]$

For convenience we will refer to the elements of Z_n as 0,1,2, ...,n-1 where the equivalence classes are implied. Following the example we have $(4)(4) = 0$ and $(3)(11) = 1$ as elements of Z_{16}. Further the notation Z_n will imply that n is a positive integer.

If $a, n \in Z^+$ then the greatest common divisor of a and n is defined in the usual way. It is a fact that $\gcd(a,n) = 1$ if and only if there exist $s,t \in \mathbf{Z}^+$ such that $as + nt = 1$.

Now consider a nonzero element a of Z_n. There exists $b \in Z_n$ such that $ab = 1$ if and only if $n|ab-1$, if and only if there exists a positive integer c such that $cn = ab-1$. That is, there exists an inverse b of a if and only if there exists c such that $1 = ab - cn$. Thus the following lemma holds.

Lemma 2.2.3. [G, pp 133] *Let $a \in Z_n$ be nonzero. Then a has a multiplicative inverse, (that is a is a unit), if and only if* $\gcd(a,n) = 1$.

If n is prime, then n is relatively prime to all the non-zero positive integers less than or equal to n so we have

Corollary 2.2.4. *Z_n is a field if and only if n is prime.*

Corollary 2.2.5. *If $n = p^k$ for some prime p and positive integer k, then $a \in Z_n$ is a unit if and only if it is not the case that $p|a$.*

Thus if $n = p^k$, $U(Z_n) = \{0,1,\ p-1, p+1,\ \ldots, 2p-1, 2p+1,\ \ldots, p^k-1\}$. The units of Z_{16} are 1,3,5,7,9,11,13 and 15. Notice further that if n is composite, say $n = ab$, then as elements of Z_n, $ab = 0$. Since all fields are integral domains, Z_n is an integral domain if and only if n is prime.

The Euler function ϕ, counts the number of positive integers which are less than and relatively prime to a given integer.

Definition 2.2.6. Define ϕ $\mathbf{N} \to \mathbf{N}$ by $\phi(n) = |\{a \mid \gcd(a,n) = 1, 1 \le a \le n\}|$

So by Lemma 2.2.3, there are $\phi(n)$ elements in the group of units of Z_n.

The polynomial ring $Z_n[x]$ is the set of all polynomials with coefficients from Z_n, as in Definition 2 1 10 Since Z_n is a commutative ring with identity, Theorem 2 1 11 implies that $Z_n[x]$ will be as well Further, Z_n is an integral domain if and only if n is prime, so $Z_n[x]$ will be an integral domain if and only if n is prime Thus, in the general case, when n may not be prime, it is possible to multiply polynomials f and g and have $\deg(fg) < \deg(f) + \deg(g)$

Example 2.2.7. Let $f(x) = 2x^2 + 1$ and $g(x) = 2x^3 + 2x + 1$ be polynomials over Z_4 The product of f and g is

$$f(x)g(x) = 4x^5 + 4x^3 + 2x^2 + 2x^3 + 2x + 1 = 2x^3 + 2x^2 + 2x + 1$$

Let $h(x) = 2x + 2$ and $k(x) = 3x^5 + 3$ be polynomials over Z_6 The product of h and k is

$$h(x)k(x) = 6x^6 + 6x + 6x^5 + 6 = 0$$

Example 2.2.8 Consider $f(x) = x^4 + x + 1$ as a polynomial over Z_4 It is trivial to check that f has no factors $g, h \in Z_4[x]$ with $1 \le \deg(g), \deg(h) < 4$ However, notice that

$$(2x+1)(2x^5 + x^4 + 2x^2 + 3x + 1) = 4x^6 + 2x^5 + 4x^3 + 6x^2 + 2x^5 + x^4 + 2x^2 + 3x + 1$$

$$= x^4 + x + 1$$

So f factors as the product of two polynomials, one of which has degree greater than 4 The difficulty arises because $\deg(gh) \neq \deg(g) + \deg(h)$ as is the case if g and h have their coefficients in a field Thus our definition of irreducible must include a condition on degrees

Definition 2.2 9 Let $f \in Z_n[x]$ If there exist no polynomials $g, h \in Z_n[x]$ with $1 \le \deg(g), \deg(h) < \deg(f)$ such that $f(x) = g(x)h(x)$, then f is *irreducible over* $Z_n[x]$

Thus $f(x) = x^4 + x + 1$ is irreducible over Z_4

Let n and m be positive integers such that $m|n$. Define a function $\pi_m : Z_n \to Z_m$ by $\pi([a]_n) = [a]_m$, to be referred to as the *reduction of coefficients* mod m *function*. It will be a major tool in what follows.

Lemma 2.2.10. *If m and n are positive integers with $m|n$ then the reduction of coefficients* mod m *function, $\pi_m : Z_n \to Z_m$, is a well-defined homomorphism of rings.*

Proof If $[a_1]_n = [a_2]_n$ then $n|(a_1 - a_2)$. So since $m|n$, $m|(a_1 - a_2)$ and $\pi_m([a_1]_n) = [a_1]_m = [a_2]_m = \pi_m([a_2])$. Therefore π_m is well defined.

For $a, b \in Z_n$

(i) $\pi_m([a]_n + [b]_n) = \pi_m([a+b]_n) = [a+b]_m = [a]_m + [b]_m$ and

(ii) $\pi_m([a]_n[b]_n) = \pi_m([ab]_n) = [ab]_m = [a]_m[b]_m$ □

Now $4|8$ and $4|16$ so $\pi_4 : Z_8 \to Z_4$ and $\pi_4 : Z_{16} \to Z_4$ are well defined. The following are tables of values for the functions.

$\pi_4 : Z_8 \to Z_4$			
a	$\pi_4(a)$	a	$\pi_4(a)$
0	0	4	0
1	1	5	1
2	2	6	2
3	3	7	3

Table 2.2.11

$\pi_4 : Z_{16} \to Z_4$			
a	$\pi_4(a)$	A	$\pi_4(a)$
0	0	8	0
1	1	9	1
2	2	10	2
3	3	11	3

4	0	12	0
5	1	13	1
6	2	14	2
7	3	15	3

Table 2 2 12

Even though $\pi_4 \ Z_8 \to Z_4$ and $\pi_4 \ Z_{16} \to Z_4$ are different functions, the notation π_4 is used for both functions In general the domain of the function π_n is implied by the context

For integers m,n with $m|n$, the function π_m can be defined from $Z_n[x]$ to $Z_m[x]$ by $\pi_m\left(\sum_{i=0}^{k} a_i x^i\right) = \sum_{i=0}^{k} \pi_m(a_i)x^i$

Since $\pi_m \ Z_n \to Z_m$ is a homomorphism, it follows that $\pi_m \ Z_n[x] \to Z_m[x]$ is a homomorphism as well

Lemma 2.2.13. *If m and n are positive integers with $m|n$ then the reduction of coefficients* mod m *function $\pi_m \ Z_n[x] \to Z_m[x]$ is a well-defined homomorphism of rings*

Example 2 2.14 Let $f(x) = 6x^4 + 3x + 4$ be a polynomial over Z_8 and let $g(x) = 6x^4 + 3x + 4$ be a polynomial over Z_{12} Now $2|4$, $2|8$, $4|8$, $3|12$, and $4|12$, so we have

$\pi_3(g(x)) = 0x^4 + 0x + 1 = 1$ where $\pi_3 \ Z_{12} \to Z_3$,

$\pi_4(g(x)) = 2x^4 + 3x + 0 = 2x^4 + 3x$ where $\pi_4 \ Z_{12} \to Z_4$,

$\pi_4(f(x)) = 2x^4 + 3x + 0 = 2x^4 + 3x$ where $\pi_4 \ Z_8 \to Z_4$, and

$\pi_2(f(x)) = 0x^4 + x + 0 = x$ where $\pi_2 \ Z_8 \to Z_2$

We have the following composition

$\pi_2(\pi_4(f(x))) = \pi_2(2x^4 + 3x) = 0x^4 + x = x$

where $\pi_4 : Z_{12} \to Z_4$ and $\pi_2 : Z_4 \to Z_2$.

Notice that for any polynomial over Z_n and positive integer m with $m|n$, the degree of $\pi_m(f(x))$ is less than or equal to the degree of $f(x)$. This fact, and the homomorphic properties of the reduction of coefficients function lead to the following

Lemma 2.2.15. *Let $f(x)$ be a polynomial over Z_n and let m be a positive integer such that $m|n$. If m does not divide the leading coefficient of f(x) and $\pi_m(f(x))$ is irreducible over Z_m, then $f(x)$ is irreducible over Z_n.*

Proof. Let a be the lead coefficient of f. Since m does not divide a, $\pi_m(a) \neq 0$. So $\deg(\pi_m(f(x))) = \deg(f(x))$. Suppose f is not irreducible. Then there exist $g, h \in Z_n[x]$ such that $f(x) = g(x)h(x)$ for some $g, h \in Z_n$ with $1 \leq \deg(g), \deg(h) < \deg(f)$. Since $\pi_m : Z_n \to Z_m$ is a homomorphism we have

$$\pi_m(f(x)) = \pi_m(g(x)h(x)) = \pi_m(g(x))\pi_m(h(x))$$

But $\deg(\pi_m(g(x))) \leq \deg(g)$ and $\deg(\pi_m(h(x))) \leq \deg(h)$ so

$$\deg(\pi_m(g(x))), \deg(\pi_m(h(x)) < \deg(f) = \deg(\pi_m(f(x)))$$

This contradicts the fact that $\pi_m(f(x))$ is irreducible. □

The converse of this lemma does not always hold. That is, if $f(x)$ is irreducible over Z_n, it is not necessarily the case that $\pi_m(f(x))$ is irreducible.

Example 2.2.16. The polynomial $x^4 + 1$ is irreducible over Z_4, but $\pi_2(x^4 + 1) = x^4 + 1 = (x^2 + 1)(x^2 + 1)$ over Z_2.

Since Z_n is a field if and only if n is prime, the usual Euclidean division algorithm will not apply for arbitrary n. There is a generalization of the division algorithm that holds for general commutative rings with identity.

Theorem 2.2.17 [Gr, pp 56] *Suppose R is a commutative ring with identity and $f(x), g(x) \in R[x]$. If $g(x)$ has leading coefficient b, then there exist a nonnegative integer k and $q(x), r(x) \in R[x]$ such that*

$$b^k f(x) = g(x)q(x) + r(x), \qquad (2.1.1)$$

with $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$. If b is not a zero divisor in R, then $q(x)$ and $r(x)$ are unique. If $b \in U(R)$ we may take $k = 0$.

Example 2.2.18. Let $f(x) = x^4 + x + 1$ and $g(x) = 2x^2 + x + 2$ be elements of $Z_6[x]$. We have

$$2^2(x^4 + x + 1) = (2x^2 + x + 2)(2x^2 + 2x) + 4$$

That is,

$$2^2 f(x) = g(x)(2x^2 + 2x) + 4$$

Notice that (2.1.1) implies that if the lead coefficient of $g(x)$ is a unit, then polynomial division by g can take place in the usual sense. Take $f(x) = x^4 + x + 1$ as above but let $g(x) = x^2 + x + 2$. We have

$$x^4 + x + 1 = (x^2 + x + 2)(x^2 + 5x + 5) + (4x + 3), \text{ or}$$

$$f(x) = g(x)(x^2 + 5x + 5) + (4x + 3)$$

2.3. Matrices and Linear Systems over Commutative Rings

Let R be a commutative ring with identity 1. Consider the set of $m \times n$ matrices with entries from R, denoted $M_{m,n}(R)$. If $m = n$ operations of addition, multiplication

and scalar multiplication can be defined on this set to form a ring In this case we write $M_m(R)$ to denote this ring

Theorem 2.3.1. [Mc, pp 8-9] *Let R be a commutative ring with identity 1, and let $r \in R$, $[a_{ij}], [b_{ij}] \in M_m(R)$ Define addition, multiplication and scalar multiplication as follows*

(i) $[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$,

(ii) $[a_{ij}][b_{jk}] = [c_{ik}]$ *where* $c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}$,

(iii) $r[a_{ij}] = [ra_{ij}]$

If $m > 1$, $M_m(R)$ is a non-commutative ring with the $m \times m$ matrix

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \text{ as identity}$$

Definition 2.3.2. Let $A = [a_{ij}]$ be an $m \times n$ matrix The *transpose* of A, denoted A^T, is the $n \times m$ matrix $[a_{ji}]$

Consider the following linear system of m equations in n unknowns

$$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots + a_{2n}x_n = b_2$$

$$\vdots$$

$$a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots + a_{mn}x_n = b_m,$$

where each constant term is an element of the commutative ring R If we let $A = [a_{ij}]$ for $i = 1, \ldots, m$, $j = 1, \ldots, n$, $X = [x_1, x_2, \ldots, x_n]^T$ and $B = [b_1, b_2, \ldots, b_m]^T$, the system can then be represented by the matrix equation $AX = B$ From this point we will consider only the case when A is $m \times m$, i e the system has m equations and m unknowns The

familiar Cramer's Rule from elementary linear algebra extends to a method for solving such a linear system over a commutative ring with identity

To develop the theory of Cramer's rule requires the use of the determinant and the adjoint of A For the purposes of this section, let A denote an $m \times m$ matrix over a commutative ring R with identity

Definition 2.3.3. The determinant function, $\det M_m(R) \to R$ is defined by $\det(A) = \sum_{\sigma} \text{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{m\sigma(m)}$ where the sum is over all permutations σ of $\{1,2, \ldots, n\}$, and $\text{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ even} \\ 0 & \text{if } \sigma \text{ odd} \end{cases}$

A discussion of permutations can be found in [G, pp 29-33]

Theorem 2.3.4. [Mc, pp 19] Let $A, B \in M_m(R)$ If B is obtained from A by adding a multiple of one row (column) of A to another row (column) of A, then $\det(A) = \det(B)$

Definition 2.2.5. The $(i, j) - cofactor$ of the $m \times m$ matrix A is defined to be the determinant of the $(m-1) \times (m-1)$ matrix A' obtained from A be deleting the i^{th} row and j^{th} column of A

Definition 2.3.6. Let A_{ij} be the $(m-1) \times (m-1)$ matrix obtained by deleting the i^{th} row and j^{th} column from A and let $b_{ij} = (-1)^{i+j} \det(A_{ij})$ The *adjoint* of A, denoted, $\text{adj}(A)$, is defined by $\text{adj}(A) = [b_{ij}]^T$

Theorem 2.3.7. [Mc, pp 25]

$$A(\text{adj}(A)) = (\text{adj}(A))A = \det(A)I$$

Corollary 2.3.7.1. [Mc, pp 79-80] *If* $\det(A)$ *is a unit in* R, *the system* $AX = B$ *has a unique solution*

Proof To solve system $AX = B$ multiply through by $\mathrm{adj}(A)$ to get

$$adj(A)AX = adj(A)B$$

which by Theorem 2 3 7 and the definition of adjoint becomes

$$\det(A)\begin{bmatrix} x_1 \\ \\ x_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{m}(-1)^{1+j}\det(A_{j1})b_j \\ \\ \sum_{j=1}^{m}(-1)^{m+j}\det(A_{jm})b_j \end{bmatrix}$$

Since $\det(A)$ is a unit we have

$$x_i = (\det(A))^{-1}\sum_{j=1}^{m}(-1)^{i+j}\det(A_{ji})b_j \quad \text{for each } i = 1, \ldots, m$$

and there exists a unique solution □

Corollary 2.3.7.2. *If* K *is a field, there exists a unique solution to the equation* $AX = B$ *if and only if* $\det(A) \neq 0$

Let $\varphi : R \to S$ be a homomorphism of commutative rings Define $\varphi : M_m(R) \to M_m(S)$ by $\varphi(A) = [\varphi(a_{ij})]$ For example,

$$\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} \varphi(a) & \varphi(b) \\ \varphi(c) & \varphi(d) \end{bmatrix}$$

It is useful to note that ring homomorphisms respect determinants in the following sense

Lemma 2.3.8. [Mc, pp 26] *Let* R *and* S *be commutative rings with identities If* $\varphi : R \to S$ *is a homomorphism, then* $\det(\varphi(A)) = \varphi(\det(A))$

Proof

$\varphi(\det(A)) = \varphi(\sum_{\sigma} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{m\sigma(m)})$

$= \sum_{\sigma} \operatorname{sgn}(\sigma) \varphi(a_{1\sigma(1)}) \varphi(a_{2\sigma(2)}) \cdots \varphi(a_{m\sigma(m)})$ since φ is a homomorphism

$= \det([\varphi(a_{ij})])$

$= \det(\varphi(A))$ □

The reduction of coefficients function $\pi_p : Z_n \to Z_p$ for an integer p with $p|n$ is a ring homomorphism and so we can apply Lemma 2.3.8. This is of particular use when p is a prime.

Corollary 2.3.8.1. Let $A \in M_m(Z_n)$ and let $\pi_p : Z_n \to Z_p$ be the reduction of coefficients mod p function. If $\det(\pi_p(A)) \neq 0$ for each prime p such that $p|n$, then $\det(A)$ is a unit in Z_n.

Proof. Suppose $\det(A)$ is not a unit. Lemma 2.2.3 implies that for some prime divisor p of n, $p|\det(A)$. So $\pi_p(\det(A)) = 0$. But by Lemma 2.3.8, $\det(\pi_p(A)) = \pi_p(\det(A))$ so $\det(\pi_p(A)) = 0$, a contradiction. □

Example 2.3.9. Consider the matrix $A = \begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$ as an element of $M_2(Z_4)$. We have $\det(A) = (2)(3) - (2)(2) = 2 - 0 = 2$. So $\pi_2(\det(A)) = 0$. Now

$\pi_2(A) = \pi_2\left(\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}\right) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, so $\det(\pi_2(A)) = (0)(1) - (0)(0) = 0$

CHAPTER 3. RELATIVELY PRIME POLYNOMIALS

Over a field, relatively prime polynomials are normally defined in terms of the greatest common divisor of polynomials.

Definition 3.1. If f and g are polynomials over a field F, then f and g are said to be relatively prime if and only if a greatest common divisor of f and g is 1.

There is a commonly used equivalent condition for relatively prime polynomials over fields.

Lemma 3.2. *Two polynomials f and g over a field F are relatively prime if and only if there exist polynomials s and t such that $f(x)s(x)+g(x)t(x)=1$.*

We will need the following related result.

Lemma 3.3. *Let f and g be polynomials over a field F. (i) If s_1,t_1 and s_2,t_2 are polynomials over F such that $f(x)s_1(x)+g(x)t_1(x)=1$ and $f(x)s_2(x)+g(x)t_2(x)=1$, then there exist $q_1,q_2 \in F[x]$ such that $s_1 = fq_1 + s_2$ and $t_1 = fq_2 + t_2$. (ii) If f and g are relatively prime there exist unique polynomials s' and t' of degree less than g and f respectively such that $f(x)s'(x)+g(x)t'(x)=1$.*

Proof. (i) Suppose s_1,t_1 and s_2,t_2 satisfy $f(x)s_1(x)+g(x)t_1(x)=1$ and $f(x)s_2(x)+g(x)t_2(x)=1$. Notice that f and g are relatively prime since such polynomials exist. Let $A(x)$ and $B(x)$ be such that

$s_2(x) = s_1(x) - A(x)$ and

$$t_2(x) = t_1(x) - B(x)$$

We have

$$\begin{aligned} 1 &= f(x)s_2(x) + g(x)t_2(x) \\ &= f(x)\big(s_1(x) - A(x)\big) + g(x)\big(t_1(x) - B(x)\big) \\ &= f(x)s_1(x) - f(x)A(x) + g(x)t_1(x) - g(x)B(x) \\ &= 1 - f(x)A(x) - g(x)B(x) \end{aligned}$$

Thus $f(x)A(x) = g(x)B(x)$ So since f and g are relatively prime, it must be that case that $f(x) \mid B(x)$ and $g(x) \mid A(x)$ Say $B(x) = f(x)q_2(x)$ and $A(x) = g(x)q_1(x)$ So

$$s_1(x) = A(x) + s_2(x) = g(x)q_1(x) + s_2(x) \text{ and}$$

$$t_1(x) = B(x) + t_2(x) = f(x)q_2(x) + t_2(x), \text{ as required}$$

(ii) Let f and g be relatively prime By Lemma 3 2 there exist s and t such that $f(x)s(x) + g(x)t(x) = 1$ The Euclidean algorithm gives polynomials q and t' over F such that

$$t(x) = f(x)q(x) + t'(x) \text{ with } \deg(t') < \deg(f)$$

Set $s'(x) = s(x) - g(x)q(x)$ We have

$$\begin{aligned} f(x)s'(x) + g(x)t'(x) &= f(x)\big(s(x) - g(x)q(x)\big) + g(x)\big(t(x) - f(x)q(x)\big) \\ &= f(x)s(x) - f(x)g(x)q(x) + g(x)t(x) - f(x)g(x)q(x) \\ &= 1 \end{aligned}$$

Since $\deg(t') < \deg(f)$ we must have $\deg(s') < \deg(g)$, otherwise the coefficients of the powers of x greater than 0 in $f(x)s'(x) + g(x)t'(x)$ would not cancel Thus, the desired polynomials s' and t' exist If s'' and t'' of degree less than g and f respectively with $f(x)s''(x) + g(x)t''(x) = 1$ exist then (i) implies there exist q_1 and q_2 such that

$$s'(x) = g(x)q_1(x) + s''(x) \text{ and}$$

$$t'(x) = f(x)q_2(x) + t''(x)$$

Since $\deg(s'), \deg(s'') < \deg(g)$ it must be the case that $s'(x) = s''(x)$ Similarly, $t'(x) = t''(x)$ Thus s' and t' are unique □

If R is not a field, the existence of a greatest common divisor for $f, g \in R[x]$ is not assured. Consequently, for the purposes of this thesis, we define relatively prime polynomials over Z_n in terms of the expression in Lemma 3.2.

Definition 3.4. If $f, g \in Z_n[x]$, then f and g are *relatively prime* if and only if there exist polynomials $s, t \in Z_n[x]$ such that

$$f(x)s(x) + g(x)t(x) = 1 \qquad (3.1)$$

If polynomials f, g and h are pairwise relatively prime over a field it follows that fg and h are relatively prime. The same is true for polynomials over Z_n with the definition of relatively prime given above.

Lemma 3.5. *Let $f, g, h \in Z_n[x]$ be pairwise relatively prime. Then the polynomials fg and h are relatively prime.*

Proof. Since f, g and h are relatively prime there exist polynomials $s_1, s_2, s_3, t_1, t_2, t_3 \in Z_n[x]$ such that the following equations hold.

$$fs_1 + gt_1 = 1$$

$$fs_2 + ht_2 = 1$$

$$gs_3 + ht_3 = 1$$

So $(fs_1 + gt_1)(fs_2 + ht_2)(gs_3 + ht_3) = 1$. Thus

$$fg(fs_1s_2s_3 + hs_1s_3t_2 + gs_2s_3t_1 + hs_2t_1t_3) + h(f^2s_1s_2t_3 + fhs_1t_2t_3 + g^2s_3t_1t_2 + ght_1t_2t_3) = 1,$$

and fg and h are relatively prime. □

Given polynomials f and g over Z_n, it is desirable to know when f and g are relatively prime. Since the reduction of coefficients function is a homomorphism we have

Lemma 3.6. *Let* $f, g \in Z_n[x]$ *and let* p *be prime such that* $p|n$ *Set* $\pi_p \; Z_n \to Z_p$ *to be the reduction of coefficients* mod p *function If* f *and* g *are relatively prime over* Z_n *then* $\pi_p(f(x))$ *and* $\pi_p(g(x))$ *are relatively prime over* Z_p

Proof Suppose f and g are relatively prime over Z_n So, there exist polynomials $s, t \in Z_n[x]$ such that

$$f(x)s(x) + g(x)t(x) = 1$$

Apply π_p to both sides to get

$$\pi_p(1) = \pi_p(f(x)s(x) + g(x)t(x))$$

Since π is a homomorphism we have

$$1 = \pi_p(f(x))\pi_p(s(x)) + \pi_p(g(x))\pi_p(t(x))$$

So $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime over $Z_p[x]$ □

So if $f, g \in Z_n[x]$ are relatively prime then it is necessary that $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime for each prime factor p of n We can now show that this condition is also sufficient to find $s(x)$ and $t(x)$ which satisfy (3 1)

Theorem 3.7. *Let* $f, g \in Z_n[x]$ *Then* f *and* g *are relatively prime over* Z_n *if and only if* $\pi_p(f(x))$ *and* $\pi_p(g(x))$ *are relatively prime for all primes* p *such that* $p|n$

Proof Without loss of generality take $\deg(g) \le \deg(f) = m$ It is sufficient to look for solutions $s(x), t(x)$ to (3 1) with $\deg(s), \deg(t) \le m-1$ Let

$$f(x) = \sum_{i=0}^{m} f_i x^i, \; g(x) = \sum_{i=0}^{m} g_i x^i$$

with s and t defined similarly Then

$$f(x)s(x) = \sum_{i=0}^{2m-1} \left(\sum_{j=0}^{i} f_j s_{i-j}\right) x^i \text{ and}$$

$$g(x)t(x) = \sum_{i=0}^{2m-1}(\sum_{j=0}^{i} g_j t_{i-j})x^i ,$$

where $f_j, g_j = 0$ for $j \geq m+1$ and $s_j, t_j = 0$ for $j \geq m$. So a solution to (3.1) can be found by equating coefficients and solving the following system of $2m$ equations

$$\begin{aligned}
x^0 \quad & 1 = f_0 s_0 + g_0 t_0 \\
x^1 \quad & 0 = f_0 s_1 + f_1 s_0 + g_0 t_1 + g_1 t_0 \\
& \vdots \\
x^{m-1} \quad & 0 = f_0 s_{m-1} + f_1 s_{m-2} + \cdots + g_0 t_{m-1} + \cdots + g_{m-1} t_0 \\
x^m \quad & 0 = f_1 s_{m-1} + f_2 s_{m-2} + \cdots + g_1 t_{m-1} + \cdots + g_{m-1} t_1 \\
x^{m+1} \quad & 0 = f_2 s_{m-1} + f_3 s_{m-2} + \cdots + g_2 t_{m-1} + \cdots + g_{m-1} t_2 \\
& \vdots \\
x^{2m-2} \quad & 0 = f_{m-1} s_{m-1} + f_m s_{m-2} + g_{m-1} t_{m-1} + g_m t_{m-2} \\
x^{2m-1} \quad & 0 = f_m s_{m-1} + g_m t_{m-1}
\end{aligned}$$

Consider the $2m \times 2m$ matrix, M, which represents the coefficients of the unknowns $s_{m-1}, \ldots, s_0, t_{m-1}, \ldots, t_0$ in the system

$$M = \begin{bmatrix}
0 & 0 & \cdots & \cdots & 0 & f_0 & 0 & 0 & \cdots & \cdots & 0 & g_0 \\
0 & 0 & \cdots & 0 & f_0 & f_1 & 0 & 0 & \cdots & 0 & g_0 & g_1 \\
 & & & & & \vdots & & & & & & \\
f_0 & f_1 & \cdots & \cdots & \cdots & f_{m-1} & g_0 & g_1 & \cdots & \cdots & \cdots & g_{m-1} \\
f_1 & f_2 & \cdots & \cdots & \cdots & f_m & g_1 & g_2 & \cdots & \cdots & \cdots & g_m \\
f_2 & f_3 & \cdots & \cdots & f_m & 0 & g_2 & g_2 & \cdots & \cdots & g_m & 0 \\
 & & & & & \vdots & & & & & & \\
f_{m-1} & f_m & 0 & 0 & \cdots & 0 & g_{m-1} & g_m & 0 & 0 & \cdots & 0 \\
f_m & 0 & 0 & 0 & \cdots & 0 & g_m & 0 & 0 & 0 & \cdots & 0
\end{bmatrix} \qquad (3.2)$$

If X is the $2m$-column vector of unknowns and T is the $2m$ column vector of constants,

$$X = \begin{bmatrix} s_{m-1} \\ s_{m-2} \\ \vdots \\ s_0 \\ t_{m-1} \\ t_{m-2} \\ \vdots \\ t_0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

The system can be represented by the matrix equation $MX = T$. Showing that f and g are relatively prime is equivalent to showing the existence of a solution to the system.

Fix a prime factor p of n. Consider $\pi_p(f(x))$ and $\pi_p(g(x))$ as elements of $Z_p[x]$. The system $\pi_p(M)X = \pi_p(T)$ corresponds to the equation

$$1 = \pi_p(f(x))s'(x) + \pi_p(g(x))t'(x) \qquad (3.3)$$

So if there exist polynomials $s', t' \in Z_p[x]$ with $\deg(s'), \deg(t') \le m-1$ which satisfy (3.3), then the system $\pi_p(M)X = \pi_p(T)$ has a solution. But Z_p is a field and $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime so part (ii) of Lemma 3.3 implies such s' and t' exist and are unique. So there exists a unique solution C_p to the equation $\pi_p(M)X = \pi_p(T)$. Thus $\det(\pi_p(M)) \neq 0$.

Since p was arbitrary, $\det(\pi_p(M)) \neq 0$ for each prime factor p of n. So by Corollary 2.3.8.1 $\det(M)$ is a unit and there exists a unique solution to $MX = T$ as required. □

Example 3.8. Let $f(x) = 6x^2 + x + 2$, $g(x) = x + 1$ and $h(x) = 4x + 2$ be polynomials over Z_8. We have $\pi_2(f(x)) = x$, $\pi_2(g(x)) = x + 1$ and $\pi_2(h(x)) = 0$. So, $\pi_2(f(x))$ and $\pi_2(g(x))$ are relatively prime over Z_2. Thus by Theorem 3.7 $f(x)$ and $g(x)$ are relatively prime over Z_8. Similarly, $h(x)$ is not relatively prime to $f(x)$ or $g(x)$.

The theory of polynomial resultants can be used provide an alternate proof of Theorem 3.7 and a method of calculating polynomials that satisfy (3.1).

Definition 3.9. Let $A(x)=\sum_{i=0}^{m} a_i x^i$ and $B(x)=\sum_{i=0}^{l} b_i x^i$ be polynomials of degree m and l respectively over a commutative ring with identity. The $m+l$ by $m+l$ matrix

$$L=\begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & 0 & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & a_m & a_{m-1} & a_{m-2} & \cdots & a_0 \\ b_l & b_{l-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_l & b_{l-1} & \cdots & b_1 & b_0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & b_l & b_{l-1} & \cdots & b_0 \end{bmatrix}$$

is called the *Sylvester matrix of A and B*. The *resultant of A and B*, denoted $\mathrm{res}(A,B)$ is defined to be the determinant of L.

Notice that for polynomials f and g with $\deg(g)\le\deg(f)$ the Sylvester matrix of f and g is the transpose of the matrix M of (3.2) with the row order reversed. Wimmer gives a history of the development of the resultant in [W].

Theorem 3.10. [V, pp. 104] *Let F be a field and let f and g be polynomials over F. The resultant of f and g is equal to 0 if and only if f and g have a common non-constant factor.*

This gives the following alternate proof of Theorem 3.7.

Proof of Theorem 3.7. ($\Rightarrow$) Lemma 3.6 gives the necessary condition.

($\Leftarrow$) Suppose $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime for each prime factor p of n. Fix a prime factor p. Since $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime and have at least one non-zero leading coefficient, by Theorem 3.10,

$\text{res}(\pi_p(f),\pi_p(g)) \neq 0$ Let S_p denote the Sylvester matrix of $\pi_p(f(x))$ and $\pi_p(g(x))$ Now $\text{res}(\pi_p(f),\pi_p(g)) = \det(S_p) \neq 0$ for each $p|n$

Since the entries of the Sylvester matrix are the coefficients of the polynomials $f(x)$ and $g(x)$ we have $S_p = \pi_p(S)$ for each prime factor p Thus, for each p, $\det(\pi_p(S)) \neq 0$, and $\det(S) = \text{res}(f,g)$ is a unit by Corollary 2 3 8 1 □

So for polynomials f and g over a field, $\text{res}(f,g) \neq 0$ if and only if f and g are relatively prime The following is a generalization to arbitrary commutative rings with identity

Theorem 3.11. [C] *Let R be a commutative ring with identity and let A and B be polynomials of positive degree over R. Then there exist polynomials S and T over R such that*

$$AS + BT = res(A,B),$$

where $\deg(S) < \deg(B)$ *and* $\deg(T) < \deg(A)$

Proof Let $\deg(A) = k$ and let $\deg(B) = l$ Let L' be the matrix obtained from the Sylvester matrix L of A and B by multiplying the i^{th} column by x^{m+n-i} and adding it to the last column for each i with $1 \leq i < m+n$ That is

$$L' = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & 0 & a_m x^{m+l-1} + a_{m-1}x^{m+l-2} + \cdots + a_0 x^{l-1} \\ 0 & a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & a_m x^{m+l-2} + a_{m-1}x^{m+l-3} + \cdots + a_0 x^{l-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & a_m & a_{m-1} & a_{m-2} & \cdots & a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ b_l & b_{l-1} & \cdots & b_1 & b_0 & 0 & 0 & b_l x^{m+l-1} + b_{l-1}x^{m+l-2} + \cdots + b_0 x^{m-1} \\ 0 & b_l & b_{l-1} & \cdots & b_1 & b_0 & 0 & b_l x^{m+l-2} + b_{l-1}x^{m+l-3} + \cdots + b_0 x^{m-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & b_l & b_{l-1} & \cdots & b_l x^l + b_{l-1}x^{l-1} + \cdots + b_0 \end{bmatrix}$$

$$= \begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & 0 & A(x)x^{l-1} \\ 0 & a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & A(x)x^{l-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & a_m & a_{m-1} & a_{m-2} & \cdots & A(x) \\ b_l & b_{l-1} & \cdots & b_1 & b_0 & 0 & 0 & B(x)x^{m-1} \\ 0 & b_l & b_{l-1} & \cdots & b_1 & b_0 & 0 & B(x)x^{m-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & b_l & b_{l-1} & \cdots & B(x) \end{bmatrix}$$

Since S' is obtained by adding multiples of columns of L to L, by Theorem 2 3 4 we have $\det(L) = \det(L') = \text{res}(A, B)$. By expanding the determinant with respect to the last column of L' we can see that the determinant is equal to

$$A(x)x^{l-1}D_1 - A(x)x^{l-2}D_2 + \cdots + (-1)^{l+1}A(x)D_l + (-1)^{l+2}B(x)x^{m-1}D_{l+1} + (-1)^{l+3}B(x)x^{m-2}D_{l+2} + \cdots + (-1)^{l+m+1}B(x)D_{l+m}$$

$$= A(x)\left(x^{l-1}D_1 - x^{l-2}D_2 + \cdots + (-1)^{l+1}D_l\right) + B(x)\left((-1)^{l+2}x^{m-1}D_{l+1} + (-1)^{l+3}x^{m-2}D_{l+2} + \cdots + (-1)^{l+m+1}D_{l+m}\right)$$

Where each D_i is the cofactor of the last column and the i^{th} row of L', and is therefore a sum and product of elements from R. (Notice that the D_i are actually cofactors of the matrix L since L' and L differ only in the last column.)

The result is obtained if we set

$S(x) = x^{l-1}D_1 - x^{l-2}D_2 + \cdots + (-1)^{l+1}D_l$ and

$T(x) = (-1)^{l+2}x^{m-1}D_{l+1} + (-1)^{l+3}x^{m-2}D_{l+2} + \cdots + (-1)^{l+m+1}D_{l+m}$ □

Let f and g be polynomials over Z_n. If $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime over $Z_p[x]$ for each prime factor p of n, then Theorem 3 7 states that f and g are relatively prime. That is there exist $s, t \in Z_n[x]$ with $f(x)s(x) + g(x)t(x) = 1$. The proof of Theorem 3 11 implies that the coefficients of s and t can be obtained by calculating the cofactors of a certain matrix.

We have

$$s(x) = x^{l-1}D_1 - x^{l-2}D_2 + \cdots + (-1)^{l+1}D_l \text{ and}$$

$$t(x) = (-1)^{l+2}x^{m-1}D_{l+1} + (-1)^{l+3}x^{m-2}D_{l+2} + \cdots + (-1)^{l+m+1}D_{l+m}$$

where $\deg(f) = m$, $\deg(g) = l$ and each D_i is the cofactor of the last column and the i^{th} row of the Sylvester matrix S of f and g

Example 3.12. Let $f(x) = x^3 + x^2 + 1$ and $g(x) = 3x^2 + 1$ be polynomials over Z_4

Since $\pi_2(f(x)) = x^3 + x^2 + 1$ is irreducible over Z_2 and $\deg(\pi_2(f)) > \deg(\pi_2(g))$ we have $\pi_2(f(x)), \pi_2(g(x))$ relatively prime, so the resultant of f and g should be a unit

Since $\deg(f) = 3, \deg(g) = 2$ we have $m = 3, l = 2$ The Sylvester matrix of f and g is

$$S = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 3 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 \end{bmatrix} \text{ and } \operatorname{res}(f,g) = \det(S) = 1$$

So the resultant of f and g is a unit as expected

The 1^{st} cofactor D_1 is equal to

$$\det\left(\begin{bmatrix} 0 & 1 & 1 & 0 \\ 3 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \\ 0 & 0 & 3 & 0 \end{bmatrix}\right) = 1$$

The other cofactors are calculated similarly to get $D_2 = 2, D_3 = 1, D_4 = 1, D_5 = 3$

We have

$$\begin{aligned} s(x) &= x^{2-1}D_1 - x^{2-2}D_2 \\ &= x(1) - (1)2 \\ &= x - 2 \end{aligned}$$

$$\begin{aligned} t(x) &= (-1)^{2+2}x^{3-1}D_3 + (-1)^{2+3}D_4x^{3-2} + (-1)^{2+4}x^{3-3}D_5 \\ &= x^2(1) - x(1) + x(3) \\ &= x^2 - x + 3 \end{aligned}$$

with $f(x)s(x) + g(x)t(x) = 1$

CHAPTER 4 THE RING $Z_n[x]/ < f >$ AND ITS UNITS

Let f be a polynomial over Z_n. Consider the set $< f >= \{g \in Z_n[x] \mid \exists h \in Z_n[x] \text{ such that } g(x) = f(x)h(x)\}$. $< f >$ is a subring of $Z_n[x]$ with the property that if $r(x) \in Z_n[x]$ and $g(x) \in < f >$ then $r(x)g(x) \in < f >$. For each $g \in Z_n[x]$, $g + < f >$ is the set $\{g + h \mid h \in < f >\}$. Such a set is called a *coset of* $< f >$. The following lemma relates *cosets* $g + < f >$ *and* $h + < f >$.

Lemma 4.1 *Let f, g and h be polynomials over* Z_n. *The cosets* $g + < f >$ *and* $h + < f >$ *are equal if and only if* $f(x) \mid g(x) - h(x)$.

Proof ($\Rightarrow$) Suppose $g + < f >= h + < f >$, and let $s \in g + < f >$. We have $s(x) = g(x) + f(x)q_1(x) = h(x) + f(x)q_2(x)$ for some $q_1, q_2 \in Z_n[x]$. Thus $g(x) - h(x) = f(x)(q_2(x) - q_1(x))$.

($\Leftarrow$) If $f(x) \mid g(x) - h(x)$ then there exists a polynomial q such that $g(x) - h(x) = f(x)q(x)$. So

$$\begin{aligned} s(x)g + < f > \Leftrightarrow s(x) &= g(x) + f(x)t(x) \text{ for some } t \in Z_n[x] \\ &= h(x) + f(x)q(x) + t(x) \\ &= h(x) + f(x)(q(x) + t(x)) \\ \Leftrightarrow s(x) &\in h + < f > \quad \square \end{aligned}$$

The set of all cosets of $< f >$ is denoted $Z_n[x]/ < f >$.

Lemma 4.2. *Let f be a monic polynomial over Z_n. Each element $g+<f>$ of $Z_n[x]/<f>$ can be uniquely represented by the remainder of division of g by f in $Z_n[x]$. Moreover $g+<f>=h+<f>$ if and only if g and h have the same remainder.*

Proof. Since f is monic Theorem 2.2.17 implies that if $g \in Z_n[x]$ is an arbitrary polynomial, then division of g by f can take place in the usual sense. That is, there exist unique $q, r \in Z_n[x]$ such that

$$g(x) = f(x)q(x) + r(x) \text{ with } \deg(r) < \deg(f) \text{ or } r(x) = 0$$

Suppose g and h are polynomials with the same remainder upon division by f. That is there exist q_1, q_2 and r such that

$$g(x) = f(x)q_1(x) + r(x) \text{ and}$$

$$h(x) = f(x)q_2(x) + r(x)$$

Thus $g(x) - h(x) = f(x)(q_1(x) - q_2(x))$ and $g+<f>=h+<f>$ by Lemma 4.1.

On the other hand, let g and h be such that $g+<f>=h+<f>$. Let r_1 and r_2 be the remainders of g and h upon division by f. Say,

$$g(x) = f(x)q_1(x) + r_1(x) \text{ and}$$

$$h(x) = f(x)q_2(x) + r_2(x)$$

Since $g+<f>=h+<f>$ we have $g(x) - h(x) = f(x)t(x)$ for some $t \in Z_n[x]$. So

$$\begin{aligned} g(x) &= f(x)t(x) + h(x) \\ &= f(x)t(x) + f(x)q_2(x) + r_2(x) \\ &= f(x)(t(x) + q_2(x)) + r_2(x) \end{aligned}$$

Thus g and h have the same remainder upon division by f. □

If $f \in Z_n[x]$ is monic, operations of addition and multiplication are defined on $Z_n[x]/<f>$ as follows.

$$(g+<f>)+(h+<f>) = (g+h)+<f>,$$

$$(g+<f>)(h+<f>) = (gh)+<f>.$$

It is simple to check that these operations are well defined and $Z_n[x]/ < f >$ forms a ring.

Theorem 4.3. *Let $f \in Z_n[x]$ be monic. The set $Z_n[x]/ < f >$ with the operations defined above is a commutative ring with identity called the quotient ring of $Z_n[x]$ modulo f. The additive and multiplicative identities are $0+ < f >$ and $1+ < f >$ respectively.*

Example 4.4. Consider $f(x) = x^2 + 1$ as a polynomial over Z_4. The possible remainders for the division of a polynomial $g \in Z_4[x]$ by f are all the polynomials over Z_4 of degree less than 2. Thus $Z_4[x]/ < f >= \{h+ < f > | h \in Z_4[x], \deg(h) < 2\}$.

Recall from Chapter 2 that if R is a commutative ring with identity, the set of units in R, $U(R)$, is a multiplicative group. If R is commutative, so is $U(R)$. When f is an irreducible polynomial over Z_p, p a prime, the structure of $U(Z_p[x]/ < f >)$ is well known.

Theorem 4.5. [LN, pp.25,46-47] *If p is prime and $f \in Z_p[x]$ is irreducible of degree m then $Z_p[x]/ < f >$ is the unique finite field of order p^m. Moreover $U(Z_p[x]/ < f >)$ $= (Z_p[x]/ < f >) \setminus \{0+ < f >\})$ is a cyclic abelian group of order $p^m - 1$.*

We now consider $Z_n[x]/ < f >$ where n is arbitrary and f is monic. We do not assume f is irreducible in any sense.

Theorem 4.6. *Let $f, g \in Z_n[x]$ with f monic and for $p|n$ set $\pi_p : Z_n \to Z_p$ to be the reduction of coefficients* mod p *function. The coset $g+ < f >$ is a unit in the ring*

$Z_n[x]/<f>$ *if and only if* $\pi_p(f(x))$ *and* $\pi_p(g(x))$ *are relatively prime over* Z_p *for each prime p such that* $p|n$

Proof The coset $g+<f>$ is invertible if and only if there exists $h+<f>$ such that $gh+<f>=1+<f>$ That is $f(x)|g(x)h(x)-1$ in $Z_n[x]$ Let $r(x)$ be such that $r(x)f(x)=g(x)h(x)-1$ Since $1=g(x)h(x)+(-r(x))f(x)$ we see that $g+<f>$ is a unit in $Z_n[x]/<f>$ if and only if g and f are relatively prime By Theorem 3 7 f and g are relatively prime in $Z_n[x]$ if and only if for each prime p with $p|n$, $\pi_p(f(x))$ and $\pi_p(g(x))$ are relatively prime over Z_p □

Notice that the inverse of $g+<f>$ is $h+<f>$ where the polynomial h satisfies $1=f(x)s(x)+g(x)h(x)$ for some $s\in Z_n[x]$ The method outlined in Example 3 12 can be used to calculate s and h given f and g Thus, this method could be used to calculate the inverse of an element of $Z_n[x]/<f>$

We now use Theorem 4 6 to give conditions on the coefficients of $g(x)$ to ensure $g+<f>$ is a unit

Corollary 4.6.1 *Let* $f,g\in Z_n[x]$ *with* f *monic,* $\deg(f)\geq 1$ *If there exists a prime factor* p *of* n *such that p divides each coefficient of g, then* $g+<f>$ *is not a unit in the ring* $Z_n[x]/<f>$

Proof Since p divides each coefficient of g there exists $r\in Z_n[x]$ such that $g(x)=pr(x)$ Since π_p is a homomorphism we have

$$\pi_p(g(x))=\pi_p(pr(x))=\pi_p(p)\pi_p(r(x))=0$$

So $\pi_p(f(x))(0)=\pi_p(g(x))$ But $\deg(f)\geq 1$, so $\pi_p(f)$ and $\pi_p(g)$ are not relatively prime Therefore by the theorem $g+<f>$ is not a unit □

Corollary 4.6.2. *Let p be prime and let $f, g \in Z_{p^k}[x]$ for some positive integer k, with f monic. If $\pi_p(f)$ is irreducible over Z_p, then $g+<f>$ is a unit if and only if some coefficient of g is a unit. That is, an element $g+<f>$ of $Z_{p^k}[x]/<f>$ is a non-unit if and only if p divides each coefficient of g.*

Proof. Since $\pi_p(f)$ is irreducible over Z_p, every non-zero polynomial h over Z_p with $\deg(h) < \deg(\pi_p(f)) = \deg(f)$ is relatively prime to $\pi_p(f)$. Since g can be replaced by the remainder of g when divided by f in the expression $g+<f>$, we can assume without loss of generality that $\deg(g) < \deg(f)$. Notice that g has at least one coefficient that is a unit if and only if $\pi_p(g(x)) \neq 0$. So $\pi_p(f)$ and $\pi_p(g)$ are relatively prime if and only if some coefficient of g is a unit. Therefore, by Theorem 4.6, $g+<f>$ is a unit if and only if g has some coefficient a unit. Furthermore, g has no coefficient a unit, if and only if p divides each coefficient of g. □

Example 4.7. Consider $f(x) = x^4 + x + 1$ as a polynomial over Z_4.
$\pi_2(f(x)) = x^4 + x + 1$ is irreducible over Z_2, so by Corollary 4.6.2, every element of $Z_4[x]/<f>$ is a unit except those of the form $g+<f>$ where $g(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ with each $a_i = 0$ or 2.

There is a function Φ analogous to the Euler ϕ function which counts the number of polynomials relatively prime to a given polynomial over a field.

Definition 4.8. Let F be a finite field. The function $\Phi: F[x] \to \mathbf{N}$ is defined by

$$\Phi(f) = \left|\{g \in F[x] \mid \deg(g) < \deg(f) \text{ and } \gcd(f, g) = 1\}\right|$$

See Lidl and Niederreiter [LN, pp. 115] for a discussion of the function.

Theorem 4.9 *Let p be prime and let $f, g \in Z_{p^k}[x]$ for some positive integer k, with f monic*

(i) $$\left|U(Z_{p^k}[x]/<f>)\right| = p^{(k-1)\deg(f)}\Phi(\pi_p(f)) \qquad (4.1)$$

(ii) *In particular, if $\pi_p(f)$ is irreducible, then*

$$\left|U(Z_{p^k}[x]/<f>)\right| = p^{(k-1)\deg(f)}(p^{\deg(f)}-1)$$

Proof Consider an arbitrary element a of Z_p. For any $c \in Z_{p^k}$, $\pi_p(c) = a$ if and only if $p|c-a$. So the elements of Z_{p^k} that reduce to a are

$$a, a+p, a+2p, \ldots, a+(p^{k-1}-1)p$$

Thus there are a total of p^{k-1} elements that reduce to a. So, for $g \in Z_p[x]$ with $\deg(g) < \deg(f)$, there are $(p^{k-1})^{\deg(f)}$ polynomials h with degree less than f over Z_{p^k} such that $\pi_p(h) = g$. Now, $\Phi(\pi_p(f))$ counts the number of polynomials over Z_p with degree less than $\deg(f)$ which are relatively prime to f. (Note that $\deg(f) = \deg(\pi_p(f))$ since f is monic.) So the number of polynomials $h \in Z_{p^k}[x]$ such that $\pi_p(h)$ and $\pi_p(f)$ are relatively prime is $p^{(k-1)\deg(f)}\Phi(\pi_p(f))$. But by Corollary 4.6.2 this is equal to the number of units in $Z_{p^k}[x]/<f>$. If $\pi_p(f)$ is irreducible, $\Phi(\pi_p(f)) = p^{\deg(f)} - 1$ since $\pi_p(f)$ is relatively prime to every non-zero polynomial over Z_p of degree less than f.

Therefore $\left|U(Z_{p^k}[x]/<f>)\right| = p^{(k-1)\deg(f)}(p^{\deg(f)}-1)$. □

CHAPTER 5 THE ORDER OF POLYNOMIALS

5.1. Definition of Order

For any polynomial f over a finite field F_q with $f(0) \neq 0$, there will always exist a positive integer e such that $f(x) \mid x^e - 1$ [LN, pp 77] The smallest such e is defined to be the *order* of f over F_q An analogous definition can be used for certain polynomials over Z_n

Lemma 5.1.1. [M] *If $f \in Z_n[x]$ is monic, of degree $m \geq 1$ and $f(0)$ is a unit, then there exists a positive integer e such that $f(x) \mid x^e - 1$*

Proof Let g be any polynomial over Z_n Since the lead coefficient of f is 1, by Theorem 2 2 17 there exist unique $q, r \in Z_n[x]$ such that $g(x) = f(x)q(x) + r(x)$ with $\deg(r) < \deg(f) = m$ or $r(x) = 0$ Thus $Z_n[x]/ < f >$ contains $n^m - 1$ non-zero cosets But $\{x^k + < f > \mid k = 0,1, \ldots, n^m - 1\}$ is a set of n^m non-zero cosets So there must exist $r < s$ such that $x^r + < f >= x^s + < f >$ That is $f(x) \mid x^r - x^s$ or

$$f(x) \mid x^r (x^{s-r} - 1) \qquad (5.1.1)$$

Now if $f(x) = c_0 + c_1 x + \cdots + c_m x^m$, then

$$\begin{aligned} 0 = f(x) - f(x) &= c_o^{-1}(f(x) - f(x)) \\ &= c_o^{-1} f(x) - c_o^{-1}(c_0 + c_1 x + \cdots + c_m x^m) \\ &= c_o^{-1} f(x) - c_o^{-1} c_0 - c_o^{-1}(c_1 x + \cdots + c_m x^m) \end{aligned}$$

Thus $1 = c_0^{-1} f(x) - c_0^{-1} x(c_1 + \cdots + c_m x^{m-1})$ So we have $s, t \in Z_n[x]$ such that

$$1 = f(x)s(x) + xt(x)$$

If $f(x)|x^r$, say $f(x)q(x) = x^r$ then we have

$$1 = f(x)s(x) + f(x)q(x)t(x),$$

a contradiction since $\deg(f) \geq 1$. Thus f does not divide x^r so to satisfy (5.1.1) we must have $f(x)|x^{s-r} - 1$. □

Suppose f is such that $f(0)$ is not a unit. If $f|x^e - 1$, then there exists $g(x)$ such that $f(x)g(x) = x^e - 1$. But this implies that $f(0)g(0) = -1$, a contradiction since $f(0)$ is not a unit. Thus there exists such an e if and only if $f(0)$ is a unit.

Definition 5.1.2. Let $f \in Z_n[x]$ be monic of degree at least 1 with $f(0)$ a unit. The *order* of f, denoted $\text{ord}(f)$ is the smallest positive integer e such that $f|x^e - 1$.

Example 5.1.3. Let $f(x) = x^2 + 1$ be a polynomial over Z_4. We have $(x^2 + 1)(x^2 + 3) = x^4 + 3 = x^4 - 1$. Thus $f(x)|x^4 - 1$.

If $g(x) = x^2 + 2$ over Z_4. We see that if $g(x)q(x) = x^e - 1$ for some polynomial q and positive integer e we must have $(2)(q_0) = 1$, where q_0 is the constant coefficient of q. This is impossible since 2 is not a unit of Z_4. Thus there is no positive integer e such that $g(x)|x^e - 1$.

The orders of degree 2 and 3 monic polynomials over Z_2, Z_4 and Z_8 are listed in Tables A.1 through A.6.

Much is known regarding the order of polynomials over finite fields. Lidl and Niederreiter give a summary of many useful results [LN, pp. 76-84]. Since Z_n is a field if and only if n is prime these results are applicable for the case n prime. In particular, $n = 2$ will be considered, and extended to the case $n = 2^k$.

5.2 The Order of Polynomials Over Z_2

The following theorem which counts the number if monic irreducible polynomials of a given degree and order implies a bound on the maximum order of an irreducible over Z_2

Theorem 5.2.1. [LN, pp 78] *The number of monic irreducible polynomials in $GF(q)$ of degree m and order e is equal to $\phi(e)/m$ if $e \geq 2$ and m is the multiplicative order of q modulo e, equal to 2 if $m = e = 1$, and equal to 0 in all other cases. In particular, the degree of an irreducible polynomial in $GF(q)[x]$ of order e must be equal to the multiplicative order of q modulo e. (Here ϕ is the Euler function defined in Section 2.2)*

Corollary 5.2.1.1. *The order of an irreducible polynomial of degree $m \geq 1$ over Z_2 is less than or equal to $2^m - 1$. Further for each positive integer m there exists an irreducible polynomial over Z_2 of degree m and order $2^m - 1$*

Proof. Notice that the multiplicative order of 2 modulo $2^m - 1$ is m. Note that any polynomial f over Z_2 must be monic. If $m \geq 2$ then, by Theorem 5.2.1, there are $\phi(2^m - 1)/m$ monic polynomials over Z_2 of degree m and order $2^m - 1$. If $m = 1$ then by the theorem there are 2 monic polynomials of degree 1 and order 1. So in either case there is at least one monic irreducible polynomial of degree m and order $2^m - 1$. Since the degree of an irreducible polynomial in $GF(2)[x]$ of order e must be equal to the multiplicative order of 2 modulo e, there can be no polynomials of degree m and any order greater than $2^m - 1$. □

Any polynomial over a field can be factored into a product of powers of irreducible polynomials. In the finite field case, there are theorems regarding the calculation of the order of a polynomial from the orders of its factors. These results can

be used to extend the above bound to all polynomials over Z_2 with nonzero constant coefficients.

Theorem 5.2.2. [LN, pp. 79] *Let p be prime and let $g \in GF(p^k)[x]$ be irreducible with $g(0) = 0$ and $\text{ord}(g) = e$, and let $f = g^b$ for some positive integer b. Let t be the smallest integer with $p^t \geq b$. Then $\text{ord}(f) = ep^t$.*

This, combined with the inequality in Lemma 5.2.3, can be used to show that the order of polynomials over Z_2 of the form $f = g^b$ for some irreducible g is less than $2^{\deg(f)} - 1$. We will then show that the order of any polynomial f over Z_2 is less than $2^{\deg(f)} - 1$.

Lemma 5.2.3. *If b and m are positive integers such that $b|m$ and $b > 3$, then $(2^{m/b} - 1)2b \leq 2^m - 1$.*

Proof. Notice that $(2^{m/b} - 1)2b \leq 2^m - 1$ if and only if $2b \leq \dfrac{2^m - 1}{2^{m/b} - 1}$. Further,

$$\frac{2^m - 1}{2^{m/b} - 1} = 2^{m-m/b} + 2^{m-2m/b} + \cdots + 2^{m-(b-1)m/b} + 1 \qquad (5.2.1)$$

$$= 2(\underbrace{2^{m-1-m/b} + 2^{m-1-2m/b} + \cdots + 2^{m-1-(b-1)m/b}}_{*}) + 1$$

Consider the first $\left\lceil \frac{b}{2} \right\rceil$ terms of *. Each of the exponents is greater than $\underbrace{m - 1 - \left\lceil \frac{b}{2} \right\rceil \frac{m}{b}}_{**}$.

Now,

$$m - 1 - \left\lceil \frac{b}{2} \right\rceil \frac{m}{b} = 2mb - 2b - 2b\left\lceil \frac{b}{2} \right\rceil \frac{m}{b}$$

$$> 2mb - 2b - (b+1)m.$$

Thus if $m > \frac{2b}{b-1}$, then ** is greater than 0. Since $b|m$, $m \geq b$. Further $b > \frac{2b}{b-1}$ if and only if $b(b-3) > 0$ if and only if $b > 3$. Thus since $b > 3$, $m > \frac{2b}{b-1}$ and ** is greater than 0, so the exponents of the first $\left\lceil \frac{b}{2} \right\rceil$ terms of * are greater than 0, and hence each term is at least 2. Thus * is greater than $2\left\lceil \frac{b}{2} \right\rceil \geq b$. Therefore, (5.2.1) is greater than or equal to $2b$ as required. □

Lemma 5.2.4. *Suppose g is an irreducible polynomial over Z_2 with $g(0) \neq 0$. If $f = g^b$ for some positive integer b, then* $\text{ord}(f) \leq 2^m - 1$ *where* $m = \deg(f)$.

Proof. Notice that $b|m$ and $\deg(g) = m/b$. By Corollary 5.2.1.1, $\text{ord}(g) \leq 2^{m/b} - 1$.

If $b = 1$ then $f = g$ so $\text{ord}(f) \leq 2^{m/b} - 1$.

If $b = 2$ then, by Theorem 5.2.2, $\text{ord}(f) = \text{ord}(g)2 \leq (2^{m/2} - 1)2 = 2^{m/2+1} - 2$. Now $m/2 + 1 \leq m$ since $m \geq 2$. Thus $2^{m/2+1} - 2 \leq 2^m - 1$ and the statement is true for $b = 2$.

If $b = 3$ then $\text{ord}(f) = \text{ord}(g)2^2 \leq (2^{m/3} - 1)2^2 \leq 2^{m/3+2} - 4$. Further $m/3 + 1 \leq m$ since $m \geq 3$. Thus the statement is true for $b = 3$.

So assume $b > 3$. Let t be as in Theorem 5.2.2 that is the smallest t such that $2^t \geq b$. Note that $2^t \leq 2b$ otherwise $2^{t-1} > b$, contrary to the definition of t. Now $\text{ord}(f) = \text{ord}(g)2^t \leq (2^{m/b} - 1)2b \leq 2^m - 1$ by Lemma 5.2.3. □

Consider an arbitrary polynomial f over a field. If f is not of the form g^b, for some irreducible g, then f has at least two distinct irreducible factors. Since distinct irreducibles are relatively prime, f can be factored into two relatively prime

polynomials. Thus, the only case left to consider is when f has more than one distinct irreducible factor. The following theorem addresses this case.

Theorem 5.2.5. [LN, pp. 79] *Let $g_1, g_2, \ldots, g_k$ be pairwise relatively prime nonzero polynomials over $GF(q)$, and let $f = g_1 g_2 \cdots g_k$. Then* $\mathrm{ord}(f)$ *is equal to the least common multiple of* $\mathrm{ord}(g_1), \mathrm{ord}(g_2), \ldots, \mathrm{ord}(g_k)$.

The bound in Corollary 5.2.1.1 can now be extended to arbitrary polynomials f over Z_2 with $f(0) \neq 0$.

Lemma 5.2.6. *The maximum order of any monic polynomial f of degree $m \geq 1$ over Z_2 with $f(0) \neq 0$ is $2^m - 1$.*

Proof. (By strong induction on the degree m of f.)

If $m = 1$, f is irreducible and the result holds by Corollary 5.2.1.1. Assume the statement is true for polynomials of degree less than or equal to $m-1$. Let $f \in Z_2[x]$ be of degree m. If f is irreducible, then the result holds. Otherwise either $f = g^b$ for some irreducible polynomial g with $g(0) \neq 0$, or f can be factored into two relatively prime polynomials h_1 and h_2, each of degree at least 1, $h_1(0) \neq 0, h_2(0) \neq 0$.

In the former case, Lemma 5.2.4 applies.

In the later case say $\deg(h_1) = s$, so $\deg(h_2) = m - s$. Thus by Theorem 5.2.5 and the induction assumption,

$\mathrm{ord}(f) = \mathrm{lcm}(\mathrm{ord}(h_1), \mathrm{ord}(h_2)) \leq \mathrm{ord}(h_1)\mathrm{ord}(h_2)$

$\leq (2^s - 1)(2^{m-s} - 1) = 2^m - 2^s - 2^{m-s} - 1 \leq 2^m - 1$ as required. □

5.3. The Order of Polynomials Over Z_{2^k}

Let f be a monic polynomial over Z_{2^k} with $f(0)$ a unit Consider the polynomial $\pi_{2^{k-1}}(f)$, where $\pi_{2^{k-1}}$ is the reduction of coefficients $\bmod 2^{k-1}$ function Since $\pi_{2^{k-1}}$ is a homomorphism, $\pi_{2^{k-1}}(f)$ is a monic polynomial over $Z_{2^{k-1}}$ with $\pi_{2^{k-1}}(f(0))$ a unit Thus, it is possible to use a proof by induction to find an extension of the bound in Lemma 5 2 6 which applies to polynomials over Z_{2^k} We will do this in Theorem 5 3 3 The following lemma shows that the order of f in $Z_{2^k}[x]$ is at most twice the order of $\pi_{2^{k-1}}(f)$ in $Z_{2^{k-1}}[x]$

Lemma 5.3.1. *Let k be a positive integer and let $f \in Z_{2^k}[x]$ be monic with $f(0)$ a unit If $\pi_{2^{k-1}}\ Z_{2^k}[x] \to Z_{2^{k-1}}[x]$ is the reduction of coefficients $\bmod 2^{k-1}$ function and the order of $\pi_{2^{k-1}}(f)$ is t, then the order of f is at most $2t$ Specifically, $f(x) \mid x^{2t}-1$*

Proof By Theorem 2 2 17 there exist unique $q, r \in Z_{2^k}[x]$ such that $x^t - 1 = f(x)q(x) + r(x)$ So since $\pi_{2^{k-1}}$ is a homomorphism,

$$x^t - 1 = \pi_{2^{k-1}}(f(x))\pi_{2^{k-1}}(q(x)) + \pi_{2^{k-1}}(r(x))$$

But the order of $\pi_{2^{k-1}}(f)$ is t, so $x^t - 1 = \pi_{2^{k-1}}(f(x))s(x)$ for some $s(x) \in Z_{2^{k-1}}[x]$ Thus by the uniqueness property of the division algorithm, $s(x) = \pi_{2^{k-1}}(q(x))$ and $\pi_{2^{k-1}}(r(x)) = 0$ Hence

$$x^t - 1 = \pi_{2^{k-1}}(f(x))\pi_{2^{k-1}}(q(x)) \qquad (5\ 3\ 1)$$

Now $f(x)(r(x)q(x) + q(x)(x^t + 1))$

$$= f(x)r(x)q(x) + f(x)q(x)(x^t + 1) + r(x)(x^t + 1) - r(x)(x^t + 1)$$

$$= f(x)r(x)q(x) + (f(x)q(x) + r(x))(x^t + 1) - r(x)(x^t + 1)$$

$$= f(x)r(x)q(x) + (x^t - 1)(x^t + 1) - r(x)(x^t + 1)$$

$$= (x^{2t} - 1) + r(x)(f(x)q(x) - (x^t + 1))$$

Thus if $r(x)(f(x)q(x)-(x^t+1))=0$ in $Z_{2^k}[x]$, then $f(x)|x^{2t}-1$

We proceed to prove this

Let π_2 be the reduction of coefficients modulo 2 function Notice that for all $g \in Z_{2^k}[x]$

$$\pi_2(\pi_{2^{k-1}}(g(x)))=\pi_2(g(x))$$

Apply π_2 to (5 3 1) to get

$$x^t-1=\pi_2(f(x))\pi_2(q(x))$$

Further over Z_2 we have $-1=1$, so

$$x^t+1=\pi_2(f(x))\pi_2(q(x))$$

Thus $\pi_2(f(x)q(x)-(x^t+1))=0$ So 2 divides each coefficient of $f(x)q(x)-(x^t+1)$ Since $\pi_{2^{k-1}}(r(x))=0$, $2^{k-1}|r_i$ for each coefficient r_i of $r(x)$ Therefore 2^k divides each coefficient of $r(x)(f(x)q(x)-(x^t+1))$, and this expression is equal to zero in $Z_{2^k}[x]$ as required □

Example 5.3.2 The order of x^2+1 is 2 over Z_2, 4 over Z_4 and 4 over Z_8, indicating that the bound may not be achieved

For each k the order of a polynomial over Z_{2^k} is at most twice the order of the corresponding reduced coefficient polynomial over $Z_{2^{k-1}}$ Thus, given the bound for polynomials of degree m over Z_2, the order of a polynomial over Z_{2^k} can be at most $2^{k-1}(2^m-1)$ as we now show

Theorem 5.3.3. *Let $f \in Z_{2^k}[x]$ be monic, of degree m, such that $f(0)$ is a unit The order of f over Z_{2^k} is at most $2^{k-1}(2^m-1)$*

Proof (By induction on k) If $k = 1$, by Lemma 5.2.6, the maximum order of a polynomial of degree m over Z_{2^1} is $2^m - 1 = 2^{1-1}(2^m - 1)$. So the statement is true for $k = 1$. Assume the statement is true for some positive integer k. Let $f \in Z_{2^{k+1}}[x]$ be monic of degree m such that $f(0)$ is a unit. Now, $\pi_{2^k}(f(x))$ is a monic polynomial over Z_{2^k}. So by the induction assumption, the order of $\pi_{2^k}(f(x))$ is at most $2^{k-1}(2^m - 1)$. Thus, by Lemma 5.3.1, the order of f is at most $2(2^{k-1}(2^m - 1)) = 2^{(k+1)-1}(2^m - 1)$. So the statement is true for $k+1$. □

In the appendix we list the orders of monic polynomials of degree 2 and 3 over Z_2, Z_4 and Z_8. By examining these tables we see that the order of f over Z_{2^k} is twice the order of $\pi_{2^{k-1}}(f)$ over $Z_{2^{k-1}}$ in most cases, and that the orders of the two polynomials are equal infrequently. Thus the following would seem to hold.

Conjecture A.8: *For each positive integer k there exists a monic polynomial in $Z_{2^k}[x]$ of degree m and order $2^{k-1}(2^m - 1)$.*

5.4. Calculating the Order of a Polynomial Over Z_n

Many of the theorems used to calculate the order of polynomials over finite fields can be adapted to calculate the order of polynomials over Z_n. The following corresponds to a lemma in Lidl and Niederreiter [LN, pp. 78]. The proof has been included for completeness.

Lemma 5.4.1. *Let $f \in Z_n[x]$ be monic with $f(0)$ a unit. If* ord$(f) = e$, *then $f(x) \mid x^t - 1$ if and only if $e \mid t$.*

Proof If $\text{ord}(f) = e$ divides t, then $f(x) \mid x^e - 1$ and $x^e - 1$ divides $x^t - 1$, so $f(x) \mid x^t - 1$

Conversely, if $f(x) \mid x^t - 1$ it must be the case that $t \geq e$, so there exist positive integers m and r such that $t = me + r$ with $0 \leq r < e$ Now,

$$x^t - 1 = x^{me+r} - x^r + x^r - 1 = (x^{me} - 1)x^r + (x^r - 1)$$

So since $f(x) \mid x^t - 1$ and $f(x) \mid x^e - 1$ it must be the case that $f(x) \mid x^r - 1$, which is only possible if $r = 0$ Therefore $t = me$, as required □

An analogous result to Theorem 5 2 5 holds for polynomials over Z_n

Lemma 5 4.2 *Let* $g_1, g_2, \ldots, g_s \in Z_n[x]$ *be monic, pairwise relatively prime polynomials with* $g_i(0)$ *a unit for each* i *Then* $\text{ord}(g_1 g_2 \cdots g_s)$ *is the least common multiple of* $\text{ord}(g_1), \text{ord}(g_2), \ldots, \text{ord}(g_s)$

Proof Consider polynomials $g_1, g_2, g_3 \in Z_n[x]$ By Lemma 3 5, if g_1, g_2 and g_3 are pairwise relatively prime, then $g_1 g_2$ and g_3 are relatively prime Thus the lemma follows by induction from the case $s = 2$, which is proven here

Let $c = \text{lcm}(\text{ord}(g_1), \text{ord}(g_2))$ Now $\text{ord}(g_1), \text{ord}(g_2) \mid c$, so by Lemma 5 4 1 $g_1(x), g_2(x) \mid x^c - 1$ Say,

$$x^c - 1 = g_1(x)q(x) = g_2(x)p(x) \qquad (5\,4\,1)$$

Since g_1 and g_2 are relatively prime, by there exist $s, t \in Z_n[x]$ such that

$$g_1(x)s(x) + g_2(x)t(x) = 1$$

By multiplying through by $p(x)$ we get

$$g_1(x)s(x)p(x) + g_2(x)t(x)p(x) = p(x) \qquad (5\,4\,2)$$

Substituting the RHS of (5 4 1) into (5 4 2) we have $g_1(x)(s(x)p(x)+q(x)t(x))=p(x)$

Therefore, $x^c-1=g_2(x)p(x)=g_2(x)f(x)(s(x)p(x)+q(x)t(x))$ and $g_1(x)g_2(x)\mid x^c-1$

So $\text{ord}(g_1g_2)\mid c$

Suppose d is such that $g_1(x)g_2(x)\mid x^d-1$ Then $g_1(x)\mid x^d-1$, so $\text{ord}(g_1)\mid d$

Similarly $\text{ord}(g_2)\mid d$ Thus $d\geq \text{lcm}(\text{ord}(g_1),\text{ord}(g_2))=c$ Therefore $\text{ord}(g_1g_2)=c$ □

Example 5.4.3. Let $f(x)=x^2+2x+1$ and $g(x)=x^2+3x+3$ be polynomials over Z_4 We have $\pi_2(f(x))=x^2+1$ and $\pi_2(g(x))=x^2+x+1$ The latter of these polynomials is irreducible over Z_2, so they are relatively prime over Z_2 Therefore, by Theorem 3 7, f and g are relatively prime over Z_4 By looking at Table A 2 we see that $\text{ord}(f)=4$ and $\text{ord}(g)=6$ Thus we have $\text{ord}(fg)=\text{lcm}(4,6)=12$

Lemma 5 3 1 implies a technique for calculating the order of a monic polynomial f over Z_{2^k} with $f(0)$ a unit Let the order of $\pi_{2^{k-1}}(f(x))$ over $Z_{2^{k-1}}$ be t By the Lemma 5 3 1 $f(x)\mid x^{2t}-1$ The following shows that the order of f must be a multiple of t

Lemma 5.4.4 *If $f\in Z_{2^k}[x]$ is monic such that the order of $\pi_{2^{k-1}}(f(x))$ over $Z_{2^{k-1}}$ is t, then the order of f over Z_{2^k} is a multiple of t*

Proof Let c be a positive integer such that $f(x)\mid x^c-1$ over Z_{2^k} So there exists $q\in Z_{2^k}[x]$ such that

$$f(x)q(x)=x^c-1$$

Since $\pi_{2^{k-1}}$ is a homomorphism we have the following

$$\begin{aligned}\pi_{2^{k-1}}(f(x))\pi_{2^{k-1}}(q(x)) &= \pi_{2^{k-1}}(x^c-1)\\ &= x^c-1\end{aligned}$$

So $\pi_{2^{k-1}}(f(x)) \mid x^c - 1$ over $Z_{2^{k-1}}$. Therefore since the order of $\pi_{2^{k-1}}(f(x))$ is t, Lemma 5.4.1 implies that $t \mid c$, and thus the order of f, must be a multiple of t. □

Thus $\text{ord}(f) = t$ or $2t$. By applying the same procedure to $\pi_{2^{k-1}}(f(x))$, it can be shown that $\text{ord}(\pi_{2^{k-1}}(f)) = t'$ or $2t'$, where $\text{ord}(\pi_{2^{k-2}}(\pi_{2^{k-1}}(f))) = t'$. Notice that for any integers $i \le j$, $\pi_{2^i}(\pi_{2^j}(f(x))) = \pi_{2^i}(f(x))$. So $\text{ord}(f) = t'$, $2t'$ or $4t'$ where $t' = ord(\pi_{2^{k-2}}(f(x)))$. This procedure can be continued by induction to obtain the following.

Theorem 5.4.5. *Let $f \in Z_{2^k}[x]$ be monic with $f(0)$ a unit. Suppose the order of $\pi_2(f(x))$ is e. Then the order of f is of the form $2^i e$ for some integer i, $0 \le i \le k-1$.*

Thus given the order of $\pi_2(f(x))$, there are only $k-1$ possible orders for f over Z_{2^k}. Since Z_2 is a field $\pi_2(f(x))$ factors uniquely into a product of powers of irreducible polynomials. The order of $\pi_2(f(x))$ can be calculated by its factors.

Theorem 5.4.6. [LN, pp 80] *Let p be prime, k a positive integer and let $f \in GF(p^k)[x]$ be a polynomial of positive degree and with $f(0) \neq 0$. Let $f = af_1^{b_1} \cdots f_s^{b_s}$, where $a \in GF(p^k)$, $b_1, b_2, \ldots, b_s$ positive integers, and $f_1, f_2, \ldots, f_s$ are distinct monic irreducible polynomials in $GF(p^k)[x]$, be the unique factorization of f in $GF(p^k)[x]$. Then $\text{ord}(f) = ep^t$, where $e = \text{lcm}(\text{ord}(f_1), \ldots, \text{ord}(f_s))$ and t is the smallest integer with $p^t \ge \max(b_1, \ldots, b_s)$.*

Notice that $\pi_2(f)$ is monic so the a in the theorem is equal to 1. Thus if the canonical factorization of $\pi_2(f)$ is $f_1^{b_1} f_2^{b_2} \cdots f_s^{b_s}$, then $ord(\pi_2(f)) = e2^t$ where $e = \text{lcm}(\text{ord}(f_1), \ldots, \text{ord}(f_s))$ and t is the smallest integer such that $2^t \ge \max(b_1, b_2, \ldots, b_s)$.

Example 5.4.7. Let $f(x) = (x^2 + x + 1)^2 (x^3 + 4x^2 + x + 3)$ be a polynomial over Z_8. Since π_2 is a homomorphism we have

$$\begin{aligned}\pi_2(f(x)) &= \pi_2(x^2 + x + 1)^2 \pi_2(x^3 + 4x^2 + x + 3) \\ &= (x^2 + x + 1)^2 (x^3 + x + 1)\end{aligned}$$

and $f_1(x) = x^2 + x + 1$ and $f_2(x) = x^3 + x^2 + x + 1$ are irreducible over Z_2. Now $\text{ord}(f_1) = 2$ and $\text{ord}(f_2) = 7$, so $e = \text{lcm}(2,7) = 14$. Since $f(x) = f_1(x)^2 f_2(x)$, $b_1 = 2$ and $b_2 = 1$. So $t = 1$ satisfies $2^t \geq \max(b_1, b_2)$. Therefore $ord(\pi_2(f(x)) = e2^t = (14)2 = 28$. Since $f \in Z_8[x]$, by Theorem 5.4.5 the order of f is equal to 28, $2(28) = 56$ or $2^2(28) = 112$.

The orders of irreducible polynomials of small degree over Z_2 have been calculated and are available in table form. Lidl and Niederreiter give these calculations for polynomials up to degree 11 [LN, pp. 385-87].

Consider a monic polynomial f over Z_{p^k} where p is prime and k is a positive integer. If $\pi_p(f(x))$ is irreducible, Theorem 4.9 and Lagrange's Theorem imply the following restriction on the order of f.

Theorem 5.4.8. *Let p be prime and let k be a positive integer. Suppose $f \in Z_{p^k}[x]$ is monic and with $f(0)$ a unit. If $\pi_p(f)$ is irreducible, then the order of f must divide $p^{(k-1)\deg(f)}(p^{\deg(f)} - 1)$.*

Proof. By the argument given in the proof of Lemma 5.1.1, x and $f(x)$ are relatively prime. Thus $x + < f >$ is a unit in the quotient ring $Z_n[x]/ < f >$. If $\left|U(Z_{p^k}[x]/ < f >)\right| = c$, by Lagrange's Theorem (Theorem 2.1.5), we have

$(x+<f>)^c = 1+<f>$ That is, $f(x) \mid x^c - 1$ So by Lemma 5 4 1 $\text{ord}(f) \mid c$ Since $\pi_p(f)$ is irreducible $c = \left| U(Z_{p^k}[x]/<f>) \right| = p^{(k-1)\deg(f)}(p^{\deg(f)} - 1)$ by Theorem 4 9 □

CHAPTER 6. FUTURE DIRECTIONS

The results of this thesis and the research carried out in the process of writing this thesis suggest possible areas for future study

If f and g are polynomials over the finite field $GF(q)$, such that they are both irreducible of degree m, then the quotient rings $GF(q)[x]/ < f >$ and $GF(q)[x]/ < g >$ are isomorphic to the unique finite field of order q^m [LN, pp 25,46] Thus $GF(q)[x]/ < f >$ and $GF(q)[x]/ < g >$ are isomorphic The same is not always true for polynomials over $Z_n[x]$

Example 6.1. Let $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + x + 3$ are both irreducible over Z_4 Over Z_2 $\pi_2(f(x)) = x^3 + x + 1$ is irreducible and $\pi_2(g(x)) = x^3 + x^2 + x + 1 = (x+1)^3$ Thus $\pi_2(f(x))$ is relatively prime to every polynomial of degree less than 3, so, as in Corollary 4 5 2 every element of $Z_4[x]/ < f >$ is a unit except those of the form where 2 divides each coefficient of h Since $\pi_2(g(x))$ is not relatively prime to $x+1$, all polynomials k over Z_4 such that $\pi_2(k) = x+1$ are not relatively prime to g Thus, the non-units in the ring $Z_4[x]/ < g >$ include all of the form $k+ < f >$ where $\pi_2(k) = x+1$ as well as those of the form $h+ < f >$ where 2 divides each coefficient of h So $Z_4[x]/ < f >$ has fewer units than $Z_4[x]/ < g >$, and the two rings cannot be isomorphic

In general we have the following

Lemma 6.2 *If $f, g \in Z_{p^k}[x]$ for some prime p and positive integer k, are monic of degree m such that $\pi_p(f(x))$ is irreducible and $\pi_p(g(x))$ is not, then $Z_{p^k}[x]/<f>$ and $Z_{p^k}[x]/<g>$ are not isomorphic.*

Possible necessary and sufficient conditions for two polynomials f and g to form isomorphic quotient rings could be investigated.

If f is a monic polynomial over Z_n then, as mentioned in Chapter 4, the group of units in the quotient ring formed by f, $U(Z_n[x]/<f>)$, is a finite abelian group. When n is prime Z_n is a finite field, and it is known that this group is cyclic [LN, pp 47]. The calculation of maximum possible multiplicative orders of elements of the group $U(Z_n[x]/<f>)$ would give a classification of its structure. Notice that a monic polynomial f over Z_n will always have a root in the quotient ring $Z_n[x]/<f>$ since $f(x)|f(x)$ so $f(x+<f>) = 0+<f>$.

It is clear that roots of the polynomial f have multiplicative order less than $\text{ord}(f)$.

Lemma 6.3. *Let $f \in Z_n[x]$ be monic of order e. If $\alpha+<f>$ is a root of f in the quotient ring $Z_n[x]/<f>$, then $(\alpha+<f>)^e = 1+<f>$.*

Proof. If $\alpha+<f>$ is a root of f, that is $f(\alpha+<f>) = 0+<f>$, then $f(x)|f(\alpha)$. Now since $\text{ord}(f) = e$, there exists $q \in Z_n[x]$ such that $f(x)q(x) = x^e - 1$. So we have $f(\alpha)q(\alpha) = \alpha^e - 1$. But $f(x)|f(\alpha)$, so $f(x)|\alpha^e - 1$ as required. □

When n is prime and Z_n is a finite field, f will always factor linearly over $Z_n[x]/<f>$. In the following example $f \in Z_4[x]$ factors linearly over $Z_4[x]/<f>$.

Example 6.4. Let $f(x) = x^4 + x + 1$ be an irreducible polynomial over Z_4. The cosets $x + < f >$, $2x^2 + x + 3 + < f >$, $3x^2 + 3 + < f >$ and $3x^2 + 2x + 2 + < f >$ are all roots of f over $Z_4[x]/< f >$. Thus

$$f(x) = (x - (x + < f >))(x - (2x^2 + x + 3 + < f >))$$
$$(x - (3x^2 + 3 + < f >))(x - (3x^2 + 2x + 2 + < f >)).$$

This example suggests that some polynomials f over Z_n factor linearly over $Z_n[x]/< f >$. A classification of which polynomials have this property could be explored.

BIBLIOGRAPHY

[B] J Barton, Polynomials over integer rings, Undergraduate Paper, University of Canterbury, New Zealand, 1997

[C] G E Collins, The calculation of multivariate polynomial resultants, J AMC 18, No 4 (1971), pp 515-532

[G] F M Goodman, "Algebra Abstract and Concrete", Prentice-Hall, Upper Saddle River, New Jersey, 1998

[Gr] L C Grove "Algebra", Academic Press, New York, 1983

[LN] R Lidl and H Niederreiter, "Introduction to Finite Fields and their Applications", Cambridge University Press, Cambridge, 1994

[Mc] B R McDonald, "Linear Algebra over Commutative rings", Marcel Dekker Inc , New York, 1984

[M] C R Miers, University of Victoria, British Columbia, personal correspondence

[V] B L van der Waerden, "Algebra", Volume I, Frederick Ungar Publishing Co , New York, 1970

[W] H K Wimmer, On the history of the Bezoutian and the resultant matrix, Linear Algebra Appl 128, 27-34 (1990)

APPENDIX

The following tables give the order of degree two and three monic polynomials over Z_2, Z_4 and Z_8. On the left hand column the polynomial is represented in the form $a_3a_2a_1a_0$ to represent the polynomial $a_3x^3 + a_2x^2 + a_1x + a_0$. The number on the right hand side of the column is the order of the polynomial on the left. Some of the calculations included were taken from tables produced in [B]. The remainder of the calculations were performed using MATLAB.

101	2	111	3

Table A.1 Z_2, Degree 2

101	4	111	3	121	4	131	6
103	2	113	6	123	4	133	6

Table A.2 Z_4, Degree 2

101	4	121	4	141	4	161	8
103	4	123	8	143	4	163	8
105	4	125	8	145	4	165	8
107	2	127	8	147	4	167	8
111	3	131	12	151	6	171	6
113	12	133	12	153	12	173	12
115	6	135	6	155	6	175	6
117	12	137	12	157	12	177	12

Table A.3 Z_8, Degree 2

1001	3	1101	7
1011	7	1111	4

Table A 4 Z_2, Degree 3

1001	6	1101	14	1201	6	1301	14
1003	3	1103	14	1203	6	1303	14
1011	14	1111	4	1211	14	1311	8
1013	14	1113	8	1213	7	1313	4
1021	6	1121	14	1221	6	1321	14
1023	6	1123	14	1223	6	1323	7
1031	14	1131	8	1231	14	1331	8
1033	14	1133	8	1233	14	1333	8

Table A 5 Z_4, Degree 3

1001	6	1101	28	1201	12	1301	28
1003	6	1103	28	1203	12	1303	28
1005	12	1105	28	1205	12	1305	28
1007	3	1107	28	1207	12	1307	28
1011	28	1111	4	1211	14	1311	16
1013	28	1113	16	1213	14	1313	4
1015	28	1115	8	1215	14	1315	16
1017	28	1117	16	1217	14	1317	8
1021	12	1121	14	1221	6	1321	28
1023	12	1123	28	1223	6	1323	14
1025	12	1125	14	1225	6	1325	28
1027	12	1127	28	1227	6	1327	7
1031	28	1131	16	1231	28	1331	16
1033	28	1133	16	1233	28	1333	16
1035	28	1135	16	1235	28	1335	16
1037	28	1137	8	1237	28	1337	16
1041	6	1141	28	1241	12	1341	28
1043	6	1143	28	1243	12	1343	28
1045	6	1145	28	1245	12	1345	28
1047	6	1147	28	1247	12	1347	28
1051	28	1151	8	1251	14	1351	16
1053	28	1153	16	1253	14	1353	8
1055	28	1155	8	1255	14	1355	16
1057	28	1157	16	1257	14	1357	8
1061	12	1161	14	1261	6	1361	28
1063	6	1163	28	1263	6	1363	14
1065	12	1165	14	1265	6	1365	28
1067	12	1167	28	1267	6	1367	14
1071	28	1171	16	1271	28	1371	16
1073	28	1173	16	1273	28	1373	16
1075	28	1175	16	1275	28	1375	16
1077	28	1177	16	1277	28	1377	16

Table A 6 Z_8, Degree 3

1401	6	1501	28	1601	12	1701	28
1403	6	1503	28	1603	12	1703	28
1405	6	1505	28	1605	12	1705	28
1407	6	1507	28	1607	12	1707	28
1411	28	1511	8	1611	14	1711	16
1413	28	1513	16	1613	14	1713	8
1415	28	1515	4	1615	14	1715	16
1417	28	1517	16	1617	14	1717	4
1421	12	1521	14	1621	6	1721	28
1423	12	1523	28	1623	6	1723	14
1425	12	1525	14	1625	6	1725	28
1427	12	1527	28	1627	6	1727	14
1431	28	1531	16	1631	28	1731	16
1433	28	1533	16	1633	28	1733	16
1435	28	1535	16	1635	28	1735	16
1437	28	1537	16	1637	28	1737	16
1441	6	1541	28	1641	12	1741	28
1443	6	1543	28	1643	12	1743	28
1445	6	1545	28	1645	12	1745	28
1447	6	1547	28	1647	12	1747	28
1451	28	1551	8	1651	14	1751	16
1453	28	1553	16	1653	14	1753	8
1455	28	1555	8	1655	14	1755	16
1457	28	1557	16	1657	7	1757	8
1461	12	1561	14	1661	6	1761	28
1463	12	1563	28	1663	6	1763	14
1465	12	1565	14	1665	6	1765	28
1467	12	1567	28	1667	6	1767	14
1471	28	1571	16	1671	28	1771	16
1473	28	1573	16	1673	28	1773	16
1475	28	1575	16	1675	28	1775	16
1477	28	1577	16	1677	28	1777	16

Table A 7 Z_8, Degree 3 cont

Vita

Surname Walshe Given Names Bridget Anne

Place of Birth Victoria, British Columbia, Canada

Educational Institutions Attended:

University of Victoria	1994 to 2001

Degrees Awarded:

B Sc , University of Victoria	1999

Honours and Awards:

University of Victoria Fellowship	1999 to 2001
MacMillan Bloedel Post-Secondary Scholarship	1994 and 1995
Governor General's Bronze Medal	1994
University of Victoria Entrance Scholarship	1994
British Columbia Provincial Scholarship Award	1994
Boyd Memorial Science Scholarship	1994
Lake Cowichan Teacher's Association Scholarship	1994

University of Victoria partial copyright license

I hereby grant the right to lend my thesis to users of the University of Victoria Library, and to make single copies only for such users or in response to a request from the Library of any other university, or similar institution, on its behalf or for one of its users. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by me or a member of the University designated by me. It is understood that copying or publication of this thesis for financial gain by the University of Victoria shall not be allowed without my written permission.

Title of Thesis:

Aspects of Order, Relative Primeness and Quotient Ring Structure for Polynomials over Integer Rings

Author: [redacted]

Bridget Anne Walshe

August 21, 2001