Rose-Hulman Undergraduate Mathematics Journal

Volume 16
Issue 1

Article 5

The Multiplicative Structure of the Group of Units of $\mathbb{Z}_p[?]/\langle ?(?)\rangle$ where ?(?) is Reducible

Erika Gerhold
Salisbury University

Jennifer Ferralli
Salisbury University

Jason Jachowski
Salisbury University

Rose-Hulman Undergraduate Mathematics Journal

The Multiplicative Structure of the Group of Units of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ where $f(x)$ is Reducible

Erika Gerhold[a] Jason Jachowski[b]
Jennifer Ferralli (Larson)[c]

Volume 16, No. 1, Spring 2015

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Salisbury University
[b]Salisbury University
[c]Salisbury University

Rose-Hulman Undergraduate Mathematics Journal
Volume 16, No. 1, Spring 2015

The Multiplicative Structure of the Group of Units of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ where $f(x)$ is Reducible

Erika Gerhold Jason Jachowski Jennifer Ferralli (Larson)

Abstract. Factor rings of the form $\mathbb{Z}_p[x]/\langle f(x)\rangle$, with p prime and $f(x)$ irreducible in $\mathbb{Z}_p[x]$ form a field, with cyclic multiplicative group structure. When $f(x)$ is reducible in $\mathbb{Z}_p[x]$ this factor ring is no longer a field, nor even an integral domain, and the structure of its group of units is no longer cyclic. In this paper we develop concise formulas for determining the cyclic group decomposition of the multiplicative group of units for $\mathbb{Z}_p[x]/\langle f(x)\rangle$ that is only dependent on the multiplicities and degrees of the irreducible factors of $f(x)$, and p.

Acknowledgements: The authors wish to thank Dr. Donald Spickler for all of his advice and guidance on this project.

1 Introduction

If R is a ring with identity, we will let $U(R)$ denote that group of units of that ring. We will also let G represent the group of units of $\mathbb{Z}_p[x]/\langle f(x)\rangle$. That is, $G = U\left(\mathbb{Z}_p[x]/\langle f(x)\rangle\right)$ with $\mathbb{Z}_p[x]$ the polynomials in x with coefficients in $\mathbb{Z}_p$. It is well known that factor rings of the form $\mathbb{Z}_p[x]/\langle h(x)g(x)\rangle$, where $h(x)$ and $g(x)$ are relatively prime, are isomorphic to $\mathbb{Z}_p[x]/\langle h(x)\rangle \times \mathbb{Z}_p[x]/\langle g(x)\rangle$ [3]. This reduces the problem of finding the decomposition of G to finding the decomposition of the unit group for rings of the form $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ where $f(x)$ is irreducible. Throughout the paper we will let $r = \deg(f(x))$, the degree of $f(x)$.

Since G is a finite Abelian group, G is isomorphic to a direct product of cyclic groups. That is, $G \cong \mathbb{Z}_{a_1}^{c_1} \times \mathbb{Z}_{a_2}^{c_2} \times \cdots \times \mathbb{Z}_{a_m}^{c_m}$, where $\mathbb{Z}_{a_i}^{c_i}$ represents the Cartesian product of $\mathbb{Z}_{a_i}$ with itself, having c_i factors [2]. Our goal is to determine the size of the cyclic factors of this decomposition. In general, if two finite groups have equal numbers of elements of equal orders, it does not follow that the two groups are isomorphic. In the case of finite Abelian groups, however, this condition is sufficient for isomorphism [4]. This allows us to take a combinatorial approach to the problem. In Section 2, we will develop formulas for the number of elements of each order in G. Then in Section 3, we consider the number of elements of each order in the cyclic group decomposition. Combining these in Section 4, we will be able to determine the factors in the decomposition of G, which gives us our main theorem.

Theorem 1. *Let p be a prime and $f(x)$ an irreducible polynomial of degree r in $\mathbb{Z}_p[x]$. Let n be any positive integer and define $s = \lceil \log_p(n) \rceil$. Define $q_i = \left\lceil \frac{n}{p^{(s-1)-i}} - 1 \right\rceil$ for $i = 0, \ldots, (s-1)$ and $q_i = 0$ for $i < 0$. The group of units G is isomorphic to*

$$G = U\left(\mathbb{Z}_p[x]/\langle f(x)\rangle\right) \cong \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^{c_{s-1}} \times \mathbb{Z}_{p^2}^{c_{s-2}} \times \cdots \times \mathbb{Z}_{p^s}^{c_0}$$

where $c_i = r(q_i - 2q_{i-1} + q_{i-2})$.

We will conclude with generalizations and examples in Section 5.

2 Element Orders in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$

Throughout the paper we will slightly abuse notation. Since we are examining elements of $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ exclusively, we will say that $g(x)$ is an element of $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$, meaning that $g(x)$ is a coset representative, that is, $g(x)+\langle f^n(x)\rangle \in \mathbb{Z}_p[x]/\langle f^n(x)\rangle$. The continual use of the coset notation makes the content of the paper more difficult to read. Also, throughout the remainder of the paper we will assume that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_p[x]$, unless otherwise stated.

The number of units in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ where $f(x)$ is irreducible of degree r is the total number of elements of $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ minus the number of zero-divisors in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$. The total number of elements in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ is p^{rn}. Since $f(x)$ is irreducible, any zero divisor, $g(x)$, must be of the form $g(x) = h(x)f(x)$ where the degree of $h(x)$ is at most

$r(n-1)-1$, and there are $p^{r(n-1)}$ such elements. So in our notation, $|G| = p^{rn} - p^{r(n-1)} = (p^r-1)p^{r(n-1)}$. The following discussion will show that $G \cong \mathbb{Z}_{p^r-1} \times H$ where H is a p-group of order $p^{r(n-1)}$.

Lemma 1. *$G = U(\mathbb{Z}_p[x]/\langle f^n(x)\rangle)$ has a cyclic subgroup of order p^r-1.*

Proof. Let the map $\phi : \mathbb{Z}_p[x]/\langle f^n(x)\rangle \to \mathbb{Z}_p[x]/\langle f(x)\rangle$ be defined by $\phi(g(x)+\langle f^n(x)\rangle) = g(x)+\langle f(x)\rangle$. It is an easy exercise to show that ϕ is a surjective ring homomorphism.

Let $k(x)$ be a generator for the multiplicative group of units in $\mathbb{Z}_p[x]/\langle f(x)\rangle$. Since ϕ is surjective, there exists a $g(x) \in \mathbb{Z}_p[x]/\langle f^n(x)\rangle$ with $\phi(g(x)) = k(x)$. Let the order of $g(x)$ be m. Then $1 = \phi(g^m(x)) = \phi(g(x))^m = k^m(x)$. So m is a multiple of the order of $k(x)$, that is, $(p^r-1)|m$. Since $\langle g(x)\rangle$ is a cyclic subgroup of order m and $(p^r-1)|m$ there is a cyclic subgroup of $\langle g(x)\rangle$ of order p^r-1. Consequently this is also a cyclic subgroup of order p^r-1 in G. □

This allows us to write $G \cong \mathbb{Z}_{p^r-1} \times H$ where H is a p-group of order $p^{r(n-1)}$ and hence has the form,

$$H = \mathbb{Z}_p^{c_{s-1}} \times \mathbb{Z}_{p^2}^{c_{s-2}} \times \cdots \times \mathbb{Z}_{p^s}^{c_0}.$$

We may now concentrate our efforts on H. Since H is a p-group we need only consider elements of G of prime power order.

Lemma 2. *The set*

$$K = \left\{ g(x) \mid g(x) = 1 + a_1(x)f(x) + a_2(x)f^2(x) + \cdots + a_{n-1}(x)f^{n-1}(x) \right\}$$

is the entire set of elements of G with order a power of p.

Proof. Let $g(x)$ be any polynomial in G of order p^b. We can write $g(x) = a_0(x) + a_t(x)f^t(x) + a_{t+1}(x)f^{t+1}(x) + \cdots + a_{n-1}(x)f^{n-1}(x)$ where t is the smallest positive power of $f(x)$ in $g(x)$ and $a_i(x)$ is a polynomial with degree less than $\deg(f(x)) = r$, for all i.

First observe that if

$$g(x) = 1 + a_t(x)f^t(x) + a_{t+1}(x)f^{t+1}(x) + \cdots + a_{n-1}(x)f^{n-1}(x),$$

then $g(x)$ is a unit in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ and hence $g(x) \in G$. To see this, rewrite $g(x)$ as $g(x) = 1 - h(x)f^t(x)$ for some $t \geq 1$. We can build $(g(x))^{-1}$ as follows. Let $h_1(x) = 1 + h(x)f^t(x)$. Then $g(x)h_1(x) = 1 - h^2(x)f^{2t}(x)$. If $2t \geq n$, then $g(x)h_1(x) = 1$ which implies that $h_1(x) = (g(x))^{-1}$. If $2t < n$, let $h_2(x) = 1 + h^2(x)f^{2t}(x)$. Then $g(x)h_1(x)h_2(x) = 1 - h^4(x)f^{4t}(x)$ and if $4t \geq n$, we can stop with $h_1(x)h_2(x) = (g(x))^{-1}$. If not, continue until $2^\alpha t \geq n$, then $(g(x))^{-1} = \prod_{i=1}^{\alpha} h_i(x)$. This shows that $g(x) \in G$.

Furthermore, $g(x) = 1 + a_t(x)f^t(x) + a_{t+1}(x)f^{t+1}(x) + \cdots + a_{n-1}(x)f^{n-1}(x)$ has order a power of p. To see this, let us first consider $g^p(x)$. By the multinomial theorem,

$$\begin{aligned} g^p(x) &= \left(1 + a_t(x)f^t(x) + a_{t+1}(x)f^{t+1}(x) + \cdots + a_{n-1}(x)f^{n-1}(x)\right)^p \\ &= \sum_{k_0+k_t+\cdots+k_{n-1}=p} \binom{p}{k_0, k_t, \ldots, k_{n-1}} \prod_{i=0,t,\ldots,n-1} \left(a_i(x)f^i(x)\right)^{k_i} \end{aligned}$$

where we consider $a_0(x) = 1$. Since $\binom{p}{k_0,k_t,\ldots,k_{n-1}} = \frac{p!}{k_0!k_t!\cdots k_{n-1}!}$ is divisible by p, unless $k_i = p$, all but these terms vanish from the sum. This simplifies the expression to

$$\begin{aligned} g^p(x) &= 1^p + (a_t(x)f^t(x))^p + (a_{t+1}(x)f^{t+1}(x))^p + \cdots + (a_{n-1}(x)f^{n-1}(x))^p \\ &= 1 + a_t^p(x)f^{tp}(x) + a_{t+1}^p(x)f^{(t+1)p}(x) + \cdots + a_{n-1}^p(x)f^{(n-1)p}(x). \end{aligned}$$

Repeated applications of this gives an expression for $g^{p^b}(x)$,

$$g^{p^b}(x) = 1 + a_t^{p^b}(x)f^{tp^b}(x) + \cdots + a_{n-1}^{p^b}(x)f^{(n-1)p^b}(x).$$

Let b be large enough so that $tp^b \geq n$, then all of the terms, except for 1, will vanish. Therefore, $g^{p^b}(x) = 1$ and the order of $g(x)$ must divide p^b. Hence, the order of $g(x)$ is a power of p. So $g(x)$ will correspond to an element in H via the isomorphism $G \cong \mathbb{Z}_{p^r-1} \times H$.

We will now show that the set of all the elements of this form constitutes all of H, via the isomorphism. Let

$$K = \left\{ g(x) \mid g(x) = 1 + a_1(x)f(x) + a_2(x)f^2(x) + \cdots + a_{n-1}(x)f^{n-1}(x) \right\}.$$

Counting the elements gives us $|K| = (p^r)^{n-1} = p^{r(n-1)} = |H|$. Since the order counts match, the isomorphism maps K onto H. □

One corollary of this is that if we let $t = 1$, and the order of $g(x)$ be p^b, we find that the maximum order of any polynomial in K is $p^{\lceil \log_p(n) \rceil}$, where $\lceil \log_p(n) \rceil$ denotes the ceiling of $\log_p(n)$. This can be seen as follows. As we saw above, if $g(x) = 1 + a_1(x)f(x) + a_2(x)f^2(x) + \cdots + a_{n-1}(x)f^{n-1}(x)$ and p^b is the order of $g(x)$ then $1 = g^{p^b}(x) = 1 + a_1^{p^b}(x)f^{p^b}(x) + a_2^{p^b}(x)f^{2p^b}(x) + \cdots + a_{n-1}^{p^b}(x)f^{(n-1)p^b}(x)$. So b must be the smallest positive number such that $p^b \geq n$, that is, $b \geq \log_p(n)$ and so $b = \lceil \log_p(n) \rceil$.

Consequently, the maximum order of any element in K is $p^{\lceil \log_p(n) \rceil}$. The number $\lceil \log_p(n) \rceil$ plays a prominent role in the calculations that follow, so throughout the paper we will denote it as s. Since the remainder of the decomposition is a p-group, all the elements are of order p^y with $y \leq s$. By our above observations, the order of any element in K is completely dependent on the smallest positive power t of $f(x)$.

Our next result establishes a range for t in which all polynomials in K with smallest positive power t of $f(x)$ in that range have the same order.

Lemma 3. *The order of* $g(x) = 1 + a_t(x)f^t(x) + a_{t+1}(x)f^{t+1}(x) + \cdots + a_{n-1}(x)f^{n-1}(x)$ *for* $\left\lceil \frac{n}{p^{s-i}} - 1 \right\rceil + 1 \leq t \leq \left\lceil \frac{n}{p^{s-i-1}} - 1 \right\rceil$ *is* p^{s-i} *for* $0 \leq i \leq s-1$.

Proof. We know $g(x)$ has order p^{s-i} if $s-i$ is the smallest integer such that $t \geq \frac{n}{p^{s-i}}$. Since $t \in \mathbb{Z}$, we have $t \geq \left\lceil \frac{n}{p^{s-i}} \right\rceil = \left\lceil \frac{n}{p^{s-i}} - 1 \right\rceil + 1$. Also since $s-i$ is the smallest integer such that $t \geq \frac{n}{p^{s-i}}$ we must have $t < \frac{n}{p^{s-i-1}}$, which implies $t \leq \left\lceil \frac{n}{p^{s-i-1}} - 1 \right\rceil$. □

This lemma sets up intervals of t where the order of any polynomial with lowest power of $f(x)$ in that interval are all the same. These intervals will also play a prominent role in our calculations, so throughout the remainder of the discussion we will let $q_i = \left\lceil \frac{n}{p^{(s-1)-i}} - 1 \right\rceil$. We will also define $q_i = 0$ when $i < 0$. In this notation, our above lemma can be restated as follows. The order of $g(x) = 1 + a_t(x)f^t(x) + a_{t+1}(x)f^{t+1}(x) + \cdots + a_{n-1}(x)f^{n-1}(x)$ where $q_{i-1} + 1 \leq t \leq q_i$ is p^{s-i}.

Given the ranges of t from the above lemma it is now fairly easy to determine the number of elements of K with order p^{s-i} for all i.

Theorem 2. *The number of units in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ with order p^{s-i} is*

$$O_i = (p^r - 1) \sum_{j=1+q_{i-1}}^{q_i} p^{r(n-1-j)} = p^{r(n-1-q_i)} \left(p^{r(q_i - q_{i-1})} - 1\right)$$

where $r = \deg(f(x))$.

Proof. By Lemma 3, $g(x) = 1 + a_t(x)f^t(x) + \cdots + a_{n-1}(x)f^{n-1}(x)$ where $1 + q_{i-1} \leq t \leq q_i$ will have order p^{s-i}. Let the number of elements with order p^{s-i} be denoted as O_i. First assume that $a_{q_{i-1}+1}(x) \neq 0$, there are $p^r - 1$ possibilities for $a_{q_{i-1}+1}(x)$ and p^r possibilities for each of $a_{q_{i-1}+2}(x), a_{q_{i-1}+3}(x), \ldots, a_{n-1}(x)$. The total number of these is $(p^r - 1)p^{r((n-1)-(1+q_{i-1}))}$. By the same method, assuming $a_{q_{i-1}+1}(x) = 0$ and $a_{q_{i-1}+2}(x) \neq 0$ we have $(p^r - 1)p^{r((n-1)-(2+q_{i-1}))}$ elements. Continuing this process through q_i gives

$$\begin{aligned}
O_i &= (p^r - 1)p^{r((n-1)-(1+q_{i-1}))} + (p^r - 1)p^{r((n-1)-(2+q_{i-1}))} \\
&\qquad + \cdots + (p^r - 1)p^{r((n-1)-q_i)} \\
&= (p^r - 1) \sum_{j=1+q_{i-1}}^{q_i} p^{r(n-1-j)} \\
&= (p^r - 1)p^{r(n-1-q_i)} \left(1 + p^r + \cdots + p^{r(q_i - q_{i-1} - 1)}\right) \\
&= (p^r - 1)p^{r(n-1-q_i)} \left(\frac{1 - p^{r(q_i - q_{i-1})}}{1 - p^r}\right) \\
&= p^{r(n-1-q_i)} \left(p^{r(q_i - q_{i-1})} - 1\right).
\end{aligned}$$

□

The proofs of the main results of this paper are simplified considerably by using sums of the elements of particular orders instead of the number of elements of one order. Specifically, we will count of the number of elements of order p^k where $s - m \leq k \leq s$, for fixed m.

Corollary 1. *The number of units with order p^k in $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ where $s - m \leq k \leq s$ is $p^{r(n-1)} - p^{r(n-1-q_m)}$.*

Proof. By Theorem 2, the number of elements of order p^{s-i} is

$$O_i = (p^r - 1) \sum_{j=1+q_{i-1}}^{q_i} p^{r(n-1-j)}.$$

Now simply take the sum of the orders from $i = 0$ to $i = m$,

$$\begin{aligned}
\sum_{i=0}^{m} O_i &= (p^r - 1) \sum_{i=0}^{m} \left(\sum_{j=1+q_{i-1}}^{q_i} p^{r(n-1-j)} \right) \\
&= (p^r - 1) \sum_{j=1}^{q_m} p^{r(n-1-j)} \\
&= (p^r - 1) p^{r(n-1-q_m)} (1 + p^r + p^{2r} + \cdots + p^{r(q_m-1)}) \\
&= (p^r - 1) p^{r(n-1-q_m)} \frac{p^{rq_m} - 1}{p^r - 1} \\
&= p^{r(n-1-q_m)} (p^{rq_m} - 1) \\
&= p^{r(n-1)} - p^{r(n-1-q_m)}.
\end{aligned}$$

□

3 Element Orders in H

We will now consider element orders in the cyclic decomposition. In the last section we have established formulas for the number of units of order p^{s-i} in the polynomial factor ring. In this section we wish to find similar formulas for elements of order p^{s-i} in

$$\mathbb{Z}_p^{c_{s-1}} \times \mathbb{Z}_{p^2}^{c_{s-2}} \times \cdots \times \mathbb{Z}_{p^s}^{c_0}.$$

Then from there we will be able to determine each c_i in the cyclic decomposition.

If a, b and c are positive integers with $b \leq a$ and p prime, then the number of elements of $\mathbb{Z}_{p^a}^c$ of order p^b is $p^{bc} - p^{(b-1)c}$. If we consider the set of all the elements of $\mathbb{Z}_{p^a}^c$ with order p^b or less we obtain a subgroup isomorphic to $\mathbb{Z}_{p^b}^c$. Similarly, if we consider the set of all the elements of $\mathbb{Z}_{p^a}^c$ with order strictly less than p^b we obtain a subgroup isomorphic to $\mathbb{Z}_{p^{b-1}}^c$. So the number of elements of $\mathbb{Z}_{p^a}^c$ of order exactly p^b will be the difference of the orders of these two subgroups, specifically $p^{bc} - p^{(b-1)c}$. A more detailed discussion of the element counts can be found in the Jones and Finch paper [1].

So if we consider the $\mathbb{Z}_{p^s}$ factors in our decomposition, $\mathbb{Z}_{p^s}^{c_0}$, the number of elements of order p^s will be $p^{sc_0} - p^{(s-1)c_0}$ where we recall that $s = \lceil \log_p(n) \rceil$. Generalizing this slightly gives us the following result.

Theorem 3. *The number of elements of order p^{s-i} in*

$$H = \mathbb{Z}_p^{c_{s-1}} \times \mathbb{Z}_{p^2}^{c_{s-2}} \times \cdots \times \mathbb{Z}_{p^s}^{c_0}$$

is $O_i = p^{r(n-1)-\sum_{j=0}^{i-1}(i-j)c_j} - p^{r(n-1)-\sum_{j=0}^{i}(i-j+1)c_j}$, where $|H| = p^{r(n-1)}$.

Proof. From our above discussion, the number of elements of order p^{s-i} in $\mathbb{Z}_{p^s}^{c_0} \times \cdots \times \mathbb{Z}_{p^{s-i}}^{c_i}$ is

$$p^{(s-i)\left(\sum_{j=0}^{i} c_j\right)} - p^{(s-i-1)\left(\sum_{j=0}^{i} c_j\right)}.$$

Also the number of elements in the remainder of the decomposition of H is

$$p^{r(n-1)-sc_0-(s-1)c_1-\cdots-(s-i)c_i}.$$

This yields

$$\begin{aligned} O_i &= p^{r(n-1)-sc_0-(s-1)c_1-\cdots-(s-i)c_i}\left(p^{(s-i)\left(\sum_{j=0}^{i} c_j\right)} - p^{(s-i-1)\left(\sum_{j=0}^{i} c_j\right)}\right) \\ &= p^{r(n-1)-sc_0-(s-1)c_1-\cdots-(s-i)c_i} \\ &\qquad \left(p^{sc_0+(s-1)c_1+\cdots+(s-i)c_i-ic_0-(i-1)c_1-\cdots-(i-i)c_i}\right. \\ &\qquad\qquad \left. - p^{sc_0+(s-1)c_1+\cdots+(s-i)c_i-(i+1)c_0-ic_1-\cdots-(i-i+1)c_i}\right) \\ &= p^{r(n-1)-\sum_{j=0}^{i-1}(i-j)c_j} - p^{r(n-1)-\sum_{j=0}^{i}(i-j+1)c_j}. \end{aligned}$$

□

As with the orders of the polynomial elements it will be easier to compare the sums of the O_i.

Corollary 2. *The number of elements of order p^k with $s - m \leq k \leq s$ is*

$$\sum_{i=0}^{m} O_i = p^{r(n-1)} - p^{r(n-1)-\sum_{j=0}^{m}(m-j+1)c_j}.$$

Proof. By Theorem 3,

$$\begin{aligned} O_m &= p^{r(n-1)-\sum_{j=0}^{m-1}(m-j)c_j} - p^{r(n-1)-\sum_{j=0}^{m}(m-j+1)c_j} \\ O_{m-1} &= p^{r(n-1)-\sum_{j=0}^{m-2}(m-j-1)c_j} - p^{r(n-1)-\sum_{j=0}^{m-1}(m-j)c_j} \\ O_{m-2} &= p^{r(n-1)-\sum_{j=0}^{m-3}(m-j-2)c_j} - p^{r(n-1)-\sum_{j=0}^{m-2}(m-j-1)c_j} \\ &\vdots \\ O_1 &= p^{r(n-1)-\sum_{j=0}^{m-m}(m-(m-1)-j)c_j} - p^{r(n-1)-\sum_{j=0}^{m-(m-1)}(m-(m-1)-j+1)c_j} \\ &= p^{r(n-1)-c_0} - p^{r(n-1)-2c_0-c_1} \\ O_0 &= p^{r(n-1)} - p^{r(n-1)-c_0}. \end{aligned}$$

This turns into a nice telescoping sum giving,

$$\sum_{i=0}^{m} O_i = p^{r(n-1)} - p^{r(n-1)-\sum_{j=0}^{m}(m-j+1)c_j}.$$

□

4 Equating the Counts

Using Corollary 1 and Corollary 2, we simply equate the expressions to construct a recursive formula for c_i.

Lemma 4. $c_i = rq_i - \sum_{j=0}^{i-1}(i-j+1)c_j$.

Proof. From Corollaries 1 and 2,

$$p^{r(n-1)} - p^{r(n-1)-\sum_{j=0}^{i}(i-j+1)c_j} = p^{r(n-1)} - p^{r(n-1-q_i)}$$

which implies that $\sum_{j=0}^{i}(i-j+1)c_j = rq_i$, and therefore

$$c_i = rq_i - \sum_{j=0}^{i-1}(i-j+1)c_j.$$

□

With a little manipulation, this recursive formula can be converted into a closed form calculation of c_i that is only dependent on the numbers q_j, which in turn are only dependent on p, n, and r (the degree of $f(x)$).

Theorem 4. $c_i = r(q_i - 2q_{i-1} + q_{i-2})$.

Proof. We will proceed by induction. Our base cases will be the verifications of c_0, c_1, and c_2. Recall that we define $q_i = 0$, and hence $c_i = 0$, if $i < 0$. Using $c_i = rq_i - \sum_{j=0}^{i-1}(i-j+1)c_j$ we obtain,

$$\begin{aligned}
c_0 &= rq_0 \\
c_1 &= rq_1 - (1+1)c_0 = rq_1 - 2c_0 = rq_1 - 2rq_0 = r(q_1 - 2q_0) \\
c_2 &= rq_2 - [(2-0+1)c_0 + (2-1+1)c_1] \\
&= rq_2 - 3rq_0 - 2(rq_1 - 2rq_0) \\
&= rq_2 - 2rq_1 + rq_0 \\
&= r(q_2 - 2q_1 + q_0).
\end{aligned}$$

For the inductive step, assume that $c_j = r(q_j - 2q_{j-1} + q_{j-2})$ for all $j \leq i$, then

$$\begin{aligned}
c_{i+1} &= rq_{i+1} - \sum_{j=0}^{i}((i+1)-j+1)r(q_j - 2q_{j-1} + q_{j-2}) \\
&= rq_{i+1} - [(i+2)rq_0 + (i+1)r(q_1 - 2q_0) \\
&\quad + ir(q_2 - 2q_1 + q_0) \\
&\quad + (i-1)r(q_3 - 2q_2 + q_1) \\
&\quad \vdots \\
&\quad + 4r(q_{i-2} - 2q_{i-3} + q_{i-4}) \\
&\quad + 3r(q_{i-1} - 2q_{i-2} + q_{i-3}) \\
&\quad + 2r(q_i - 2q_{i-1} + q_{i-2})] \\
&= rq_{i+1} - [(i+2)rq_0 - 2(i+1)rq_0 + irq_0 \\
&\quad + (i+1)rq_1 - 2irq_1 + (i-1)rq_1 \\
&\quad \vdots \\
&\quad + 4rq_{i-2} - 6rq_{i-2} + 2rq_{i-2} \\
&\quad + 3rq_{i-1} - 4rq_{i-1} + 2rq_i] \\
&= r(q_{i+1} - 2q_i + q_{i-1}).
\end{aligned}$$

□

5 The General Case

These formulas, along with our original reductions, give us a quick way to compute the multiplicative group structure of the group of units of $Z_p[x]/\langle f(x)\rangle$ for all polynomials $f(x)$. Say $f(x)$ factors in $\mathbb{Z}_p[x]$, as

$$f(x) = f_1^{\alpha_1}(x)f_2^{\alpha_2}(x)\cdots f_k^{\alpha_k}(x)$$

where $f_i(x)$ are all irreducible and the $f_i(x)$ are relatively prime to each other. Then we have a ring isomorphism,

$$\mathbb{Z}_p[x]/\langle f(x)\rangle \cong \mathbb{Z}_p[x]/\langle f_1^{\alpha_1}(x)\rangle \times \mathbb{Z}_p[x]/\langle f_2^{\alpha_2}(x)\rangle \times \cdots \times \mathbb{Z}_p[x]/\langle f_k^{\alpha_k}(x)\rangle$$

where our results may be applied to each of the factors.

Example 1. Say we wanted to determine the structure of the group of units of

$$\mathbb{Z}_3[x]/\left\langle (x^2+1)^7(x^3+x^2+x+2)^{15}(x+2)^{28}\right\rangle.$$

We know that

$$\mathbb{Z}_3[x]/\left\langle\left((x^2+1)^7(x^3+x^2+x+2)^{15}(x+2)^{28}\right)\right\rangle \cong \mathbb{Z}_3[x]/\left\langle(x^2+1)^7\right\rangle \times \mathbb{Z}_3[x]/\left\langle(x^3+x^2+x+2)^{15}\right\rangle \times \mathbb{Z}_3[x]/\left\langle(x+2)^{28}\right\rangle.$$

For the first factor, $s = \lceil \log_p(n) \rceil = \lceil \log_3(7) \rceil = 2$ giving

$$\begin{aligned} q_0 &= \left\lceil \frac{7}{3^{2-1-0}} - 1 \right\rceil = 2 \\ q_1 &= \left\lceil \frac{7}{3^{2-1-1}} - 1 \right\rceil = 6. \end{aligned}$$

By Theorem 4 we have

$$\begin{aligned} c_0 &= rq_0 = 4 \\ c_1 &= r(q_1 - 2q_0) = 2(6 - (2)2) = 4. \end{aligned}$$

So,

$$U\left(\mathbb{Z}_3[x]/\left\langle(x^2+1)^7\right\rangle\right) \cong \mathbb{Z}_8 \times \mathbb{Z}_{3^2}^4 \times \mathbb{Z}_3^4.$$

For the second factor, $s = \lceil \log_p(n) \rceil = \lceil \log_3(15) \rceil = 3$ giving

$$\begin{aligned} q_0 &= \left\lceil \frac{15}{3^{3-1-0}} - 1 \right\rceil = 1 \\ q_1 &= \left\lceil \frac{15}{3^{3-1-1}} - 1 \right\rceil = 4 \\ q_2 &= \left\lceil \frac{15}{3^{3-1-2}} - 1 \right\rceil = 14 \end{aligned}$$

and thus,

$$\begin{aligned} c_0 &= rq_0 = 3 \\ c_1 &= r(q_1 - 2q_0) = 3(4 - (2)1) = 6 \\ c_2 &= r(q_2 - 2q_1 + q_0) = 3(14 - (2)4 + 1) = 21. \end{aligned}$$

So,

$$U\left(\mathbb{Z}_3[x]/\left\langle(x^3+x^2+x+2)^{15}\right\rangle\right) \cong \mathbb{Z}_{26} \times \mathbb{Z}_{3^3}^3 \times \mathbb{Z}_{3^2}^6 \times \mathbb{Z}_3^{21}.$$

For the final factor, $s = \lceil \log_p(n) \rceil = \lceil \log_3(28) \rceil = 4$ giving

$$\begin{aligned} q_0 &= \left\lceil \frac{28}{3^{4-1-0}} - 1 \right\rceil = 1 \\ q_1 &= \left\lceil \frac{28}{3^{4-1-1}} - 1 \right\rceil = 3 \\ q_2 &= \left\lceil \frac{28}{3^{4-1-2}} - 1 \right\rceil = 9 \\ q_3 &= \left\lceil \frac{28}{3^{4-1-3}} - 1 \right\rceil = 27 \end{aligned}$$

and thus,

$$\begin{aligned} c_0 &= rq_0 = 1 \\ c_1 &= r(q_1 - 2q_0) = 1(3 - (2)1) = 1 \\ c_2 &= r(q_2 - 2q_1 + q_0) = 1(9 - (2)3 + 1) = 4 \\ c_3 &= r(q_3 - 2q_2 + q_1) = 1(27 - (2)9 + 3) = 12. \end{aligned}$$

So,

$$U\left(\mathbb{Z}_3[x]/\left\langle (x+2)^{28}\right\rangle\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^4} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{3^2}^4 \times \mathbb{Z}_3^{12}.$$

Combining the three gives us the isomorphism,

$$U\left(\mathbb{Z}_3[x]/\left\langle (x^2+1)^7(x^3+x^2+x+2)^{15}(x+2)^{28}\right\rangle\right) \cong \mathbb{Z}_{26} \times \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^4} \times \mathbb{Z}_{3^3}^4 \times \mathbb{Z}_{3^2}^{14} \times \mathbb{Z}_3^{37}.$$

Example 2. In the special case where $p \geq n > 1$, the situation simplifies significantly. Here $s = \lceil \log_p(n) \rceil = 1$, giving $q_0 = n - 1$, so the group of units of $\mathbb{Z}_p[x]/\langle f^n(x)\rangle$ will be isomorphic to $\mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^{r(n-1)}$.

Example 3. If we apply our result to $\mathbb{Z}_p[x]/\langle f(x)\rangle$, where $f(x)$ is irreducible in $\mathbb{Z}_p[x]$. We have, $s = \lceil \log_p(1) \rceil = 0$, which implies that there is no decomposition for H, hence there is no H. So the group of units of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ will be isomorphic to $\mathbb{Z}_{p^r-1}$, as expected.

6 Open Questions and Future Work

One possible continuation of this work would be to examine the structure of $\mathbb{Z}_m[x]/\langle f^n(x)\rangle$ for m composite. Although we do not have a conjecture to the multiplicative group structure of units of this ring at present, our preliminary analysis shows that there are some similarities to the prime case, but there is a definite splitting of cases that did not happen with the prime modulus.

References

[1] C. Finch and L. Jones, *A curious connection between fermat numbers and finite groups*, American Mathematical Monthly, 109 (2002), pp. 517–524.

[2] J. A. Gallian, *Contemporary Abstract Algebra*, New York: Houghton Mifflin Company, 2002.

[3] S. Mac Lane and G. Birkhoff, *Algebra*, New York: MacMillan Publishing Co., Inc., 1979.

[4] J. J. Rotman, *An Introduction to the Theory of Groups*, Newton: Allyn and Bacon, Inc., 1984.