Groups of Units of $\mathbb{Z}_p[x]$ Modulo $f(x)$

A THESIS

SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL

OF THE UNIVERSITY OF MINNESOTA

BY

Karlee Westrem

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

Master of Science

Advisor: Dr. Joseph Gallian

May 15, 2020

Acknowledgments

I want to thank Dr. Gallian for working with me as well as the UMD math department for supporting my research. I want to thank Jiangyi Qiu, Noah Wong, and Hongru Zhao for the polynomial calculator computer programs. Thank you to Dr. John Greene and Dr. Douglas Dunham for serving on my committee. I would also like to thank Caleb Ji and Shahriyar Roshan Zamir for beneficial conversations about the thesis topic.

Abstract

The set $\mathbb{Z}_p[x]$ consists of all polynomials with coefficients in the field $\mathbb{Z}_p$, where p is prime. If a polynomial $f(x)$ is irreducible over $\mathbb{Z}_p$ then $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is a field. If $f(x)$ is a reducible polynomial, then every non-zero element in $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is either a zero-divisor or a unit. If we exclude the zero-divisors and zero, we have a finite Abelian group under multiplication denoted by $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. Since every finite Abelian group is a direct product of cyclic groups of prime-power order, we can find the isomorphism class for $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. We investigate the structure of $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ for a prime p and various $f(x)$. We conclude with some result on the structure of a certain family of subgroups of $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$.

Contents

1 Group of units of modulo $f(x)$

1.1 Introduction

The problem was inspired by previous research completed by Dr. Joseph Gallian and his master's student Shahriyar Roshan Zamir [2]. Their research investigated the structure of certain subgroups of the group $U(n)$, the set of all positive integers less than n and relatively prime to n with multiplication mod n. We have expanded their research by considering groups of units where the elements are polynomials. In this paper, we assume the reader is familiar with the topics in Gallian's book [1].

For a prime p, the ring $\mathbb{Z}_p[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}_p$, n is a nonnegative integer$\}$. If $f(x)$ is an irreducible polynomial over the field $\mathbb{Z}_p$, then $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is a finite field with every nonzero element being a unit (has a multiplicative inverse) ([1], 295). If $f(x)$ is a reducible polynomial in $\mathbb{Z}_p[x]$, then every non-zero element in the factor ring $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \{a_n x^n + \cdots + a_1 x + a_0 + \langle f(x)\rangle \,|\, a_n, \ldots, a_0 \in \mathbb{Z}_p\}$ where $n <$ deg $f(x)$ is either a unit or is a zero-divisor. The units of the factor ring form a finite Abelian group under multiplication called the group of units mod $f(x)$ and denoted by $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. Since every finite Abelian group is a direct product of cyclic groups of prime-power order, we seek the structure for $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ for various functions $f(x)$.

1.2 Background Information

Definition 1.1. *([1], 46) The group $U(n)$ under multiplication is the set consisting of all positive integers less than or equal to n and relatively prime to n where $n \in \mathbb{N}$. The group $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ consists of all nonzero polynomials $g(x) + \langle f(x)\rangle$ such that deg$(g(x)) <$ deg$(f(x))$ and $g(x)$ and $f(x)$ are relatively prime.*

Definition 1.2. *([1], 237) A zero-divisor is a nonzero element a of a commutative ring R*

such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition 1.3. *([1], 239) A field is a commutative ring R with unity in which every nonzero element is a unit.*

Theorem 1.4. *([1], Exercise 7, 243) In a finite commutative ring R with unity, every nonzero element of R is a unit or zero-divisor.*

Definition 1.5. *([1], 391) Let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called Sylow p-subgroup of G.*

Definition 1.6. *([1], 156) Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.*

Theorem 1.7. *([1], 212) Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.*

For any finite Abelian group G and an integer k written as $k = n_1 + n_2 + \cdots + n_t$ where each n_i is a positive integer, $\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}$ is an Abelian group of order p^k. The uniqueness portion of the Fundamental Theorem guarantees that distinct partitions of k yield distinct isomorphism classes.

For the remainder of the paper, we will just use the coset representatives to describe the elements of the multiplicative group $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ with the convention that all products of cosets are taken mod $f(x)$. Before finding the isomorphism class for $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ for any prime p and various functions $f(x)$, let's consider an example.

Example 1.8.

Suppose $p = 5$ and $f(x) = (x-1)(x-2)$. We want to find the isomorphism class of $U\left(\frac{\mathbb{Z}_5[x]}{\langle (x-1)(x-2)\rangle}\right)$. There are 25 elements in $\frac{\mathbb{Z}_5[x]}{\langle (x-1)(x-2)\rangle} = \{ax + b \mid a, b \in \mathbb{Z}_5\}$. We determine there are 8 zero divisors and zero, namely the set $\{0, x-1, 2(x-1), 3(x-1), 4(x-$

$1), x-2, 2(x-2), 3(x-2), 4(x-2)\}$. So $|G| = \left|U\left(\frac{\mathbb{Z}_5[x]}{\langle(x-1)(x-2)\rangle}\right)\right| = 25-9 = 16$. By the Fundamental Theorem of Finite Abelian Groups, G is isomorphic to one of

$\mathbb{Z}_{16}$

$\mathbb{Z}_8 \oplus \mathbb{Z}_2$

$\mathbb{Z}_4 \oplus \mathbb{Z}_4$

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

A useful fact is that two finite Abelian groups are isomorphic if and only if they have the same number of elements of each order ([1], 214). By calculating the orders of the elements, we find that the group has no elements of order 8 and exactly 3 elements of order 2. So, the isomorphism class is $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. □

Example 1.9.

Suppose $p = 7$ and $f(x) = (x-1)^2$. There are 49 elements in $\frac{\mathbb{Z}_p[x]}{\langle(x-1)^2\rangle}$ with 6 non-units and zero. Since $\left|U\left(\frac{\mathbb{Z}_7[x]}{\langle(x-1)^2\rangle}\right)\right| = 49-7 = 42 = 2{\cdot}3{\cdot}7$, we know the only possibility for G to be isomorphic to is $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$. □

We study the case when $p = 2$ separately, since it requires a different pattern then for odd prime p case.

2 $\mathbb{Z}_2$ Case

Suppose $p = 2$ and $2 \leq k \leq 9$ and $f(x)$ is a reducible polynomial. By examining computer data for the orders of elements we have:

$$
\begin{aligned}
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^2\rangle}\Big) &\approx \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^3\rangle}\Big) &\approx \mathbb{Z}_4 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^4\rangle}\Big) &\approx \mathbb{Z}_4 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^5\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^6\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^7\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^8\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle x^9\rangle}\Big) &\approx \mathbb{Z}_{16} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \qquad \square
\end{aligned}
$$

When $p = 2$ and $2 \leq k \leq 5$ for a quadratic irreducible polynomial $x^2 + x + 1$, we have:

$$
\begin{aligned}
U\Big(\frac{\mathbb{Z}_2[x]}{\langle (x^2+x+1)^2\rangle}\Big) &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle (x^2+x+1)^3\rangle}\Big) &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle (x^2+x+1)^4\rangle}\Big) &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle (x^2+x+1)^5\rangle}\Big) &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle (x^2+x+1)^6\rangle}\Big) &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
U\Big(\frac{\mathbb{Z}_2[x]}{\langle (x^2+x+1)^7\rangle}\Big) &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \qquad \square
\end{aligned}
$$

Next, we will generalize to the case when $f(x)$ is a reducible polynomial and each linear factor is raised to a power i for any prime p.

3 Reducible Polynomial $f(x)$ over $\mathbb{Z}_p$

For any prime p, we have:

1. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)\rangle}\right) \approx \mathbb{Z}_{p-1}$
2. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)(x-b)\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1}$
3. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)(x-b)(x-c)\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1}$
4. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)^2\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p$
5. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)^3\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ for odd prime p.
   When $p = 2$, we have $U\left(\frac{\mathbb{Z}_2[x]}{\langle(x-a)^3\rangle}\right) \approx \mathbb{Z}_4$
6. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)^4\rangle}\right)$
   For $p = 2 : \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4$
   For $p = 3 : \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$
   For $p > 3 : \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
7. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)^5\rangle}\right)$
   For $p = 2 : \quad \approx \mathbb{Z}_2 \oplus \mathbb{Z}_8$
   For $p = 3 : \quad \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$
   For $p > 3 : \quad \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
8. $U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)^2(x-b)\rangle}\right) \approx U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-a)^2\rangle}\right) \oplus U\left(\frac{\mathbb{Z}_p[x]}{\langle(x-b)\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p$
   For $p = 2 : \approx \mathbb{Z}_2$
   For $p > 2 : \quad \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p$

9. $U\left(\frac{\mathbb{Z}_p[x]}{\langle (x-a)^2(x-b)^2\rangle}\right) \approx U\left(\frac{\mathbb{Z}_p[x]}{\langle (x-a)^2\rangle}\right) \oplus U\left(\frac{\mathbb{Z}_p[x]}{\langle (x-b)^2\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

   For $p = 2$: $\quad \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$

   For $p > 2$: $\quad \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ □

Our next theorem generalizes for $f(x)$ is a single linear factor and any prime p.

Theorem 3.1. *For a prime p and $a \in \mathbb{Z}_p$ we have $U\left(\frac{\mathbb{Z}_p[x]}{\langle x-a\rangle}\right) \approx \mathbb{Z}_{p-1}$.*

Proof. Note the elements of $U\left(\frac{\mathbb{Z}_p[x]}{\langle x-a\rangle}\right)$ are constant functions of the form $t + \langle x-a\rangle$ where $t \in \mathbb{Z}_p$. Define $\phi : U\left(\frac{\mathbb{Z}_p[x]}{\langle x-a\rangle}\right) \to U(p)$ were $\phi(t + \langle x-a\rangle) = t$. A routine argument shows ϕ is an isomorphism and that $U(p)$ is cyclic follows from the fact that $\mathbb{Z}_p$ is a field ([1], 368). □

Our second theorem reduces the problem of determining the structure of $\frac{F[x]}{\langle f_1(x)f_2(x)\cdots f_n(x)\rangle}$ to the case where the $f_i(x)$'s are relatively prime.

Theorem 3.2. *Let $f(x)$ and $g(x)$ be polynomials over $F[x]$ where F is a field. If $f(x)$ and $g(x)$ are relatively prime, then $\frac{F[x]}{\langle f(x)g(x)\rangle} \approx \frac{F[x]}{\langle f(x)\rangle} \oplus \frac{F[x]}{\langle g(x)\rangle}$.*

Proof. By the First Isomorphism Theorem for Rings, it suffices to prove there is a ring homomorphism ϕ from $F[x]$ onto $\frac{F[x]}{\langle f(x)\rangle} \oplus \frac{F[x]}{\langle g(x)\rangle}$ with Ker $\phi = \langle f(x)g(x)\rangle$. By Theorem 16.5 in ([1], 283), Ker $\phi = \langle f(x)g(x)\rangle$ provided that deg$f(x)g(x)$ is an element of the Ker ϕ of minimum degree. Consider the ϕ mapping given by $\phi(a(x)) = (a(x) + \langle f(x)\rangle,\ a(x) + \langle g(x)\rangle)$ where $a(x), f(x), g(x) \in F[x]$. We want to show that ϕ is operation-preserving. For all $a(x), b(x) \in F[x]$ we have, $\phi(a(x)+b(x)) = (a(x)+b(x) + \langle f(x)\rangle\,,\ a(x)+b(x) + \langle g(x)\rangle)$

$= (a(x) + \langle f(x)\rangle\,,\ a(x) + \langle g(x)\rangle) + (b(x) + \langle f(x)\rangle\,,\ b(x) + \langle g(x)\rangle) = \phi(a(x)) + \phi(b(x))$

and $\phi(a(x)b(x)) = (a(x)b(x)\ +\ \langle f(x)\rangle\,,\ a(x)b(x)\ +\ \langle g(x)\rangle)$

$= \Big((a(x) + \langle f(x)\rangle)(b(x) + \langle f(x)\rangle)\ ,\ \ (a(x) + \langle g(x)\rangle)(b(x) + \langle g(x)\rangle)\Big)$

$= \Big(a(x) + \langle f(x)\rangle\,,\ a(x) + \langle g(x)\rangle\Big)\Big(b(x) + \langle f(x)\rangle\,,\ b(x) + \langle g(x)\rangle\Big) = \phi(a(x))\phi(b(x)).$

Therefore ϕ is operation-preserving. Onto follows from the Chinese Remainder Theorem for polynomial rings over a field [4]. Suppose $k(x)$ is an element of Ker ϕ of minimum degree. We will show $\langle f(x)g(x)\rangle = \langle k(x)\rangle$. Observe that, $\phi(f(x)g(x)) = (f(x)g(x) + \langle f(x)\rangle\,,\, f(x)g(x)+\langle g(x)\rangle) = (0,0)$. So $f(x)g(x) \in$ Ker $\phi = \langle k(x)\rangle$. Since $k(x) \in$ Ker ϕ, this means $k(x) + \langle f(x)\rangle = 0 + \langle f(x)\rangle$. So $k(x) \in \langle f(x)\rangle$. Thus, $k(x) = f(x)i(x)$, and deg$(k(x)) \geq$ deg$(f(x))$. Similarly, $k(x) + \langle g(x)\rangle = 0 + \langle g(x)\rangle$.

So $k(x) \in \langle g(x)\rangle$, which means $k(x) = g(x)j(x)$ and deg$(k(x)) \geq$ deg$(g(x))$. Observe that $k(x) = f(x)i(x)$ and $k(x) = g(x)j(x)$ implies $k(x) = f(x)g(x)h(x)$, so $k(x)$ is a common multiple of $f(x)$ and $g(x)$. But since $f(x)$ and $g(x)$ are relatively prime $f(x), g(x)$ is the least common multiple of $f(x)$ and $g(x)$. It follows that $k(x)$ is a multiple of $f(x)g(x)$, so $k(x) \in \langle f(x)g(x)\rangle$. Thus $f(x)g(x)$ is a polynomial of minimum degree and $\langle f(x)g(x)\rangle =$ Ker ϕ from ([1], Theorem 16.5). Therefore $\frac{F[x]}{\langle (f(x))(g(x))\rangle} \approx \frac{F[x]}{\langle f(x)\rangle} \oplus \frac{F[x]}{\langle g(x)\rangle}$. $\square$

When $F = \mathbb{Z}_p$, we don't need the Chinese Remainder Theorem to show the mapping ϕ is onto from Theorem 3.2. For $\phi : \frac{\mathbb{Z}_p[x]}{\langle f(x)g(x)\rangle} \to \frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle g(x)\rangle}$ and $f(x)$ and $g(x)$ are relatively prime, we have $\left|\frac{\mathbb{Z}_p[x]}{\langle f(x)g(x)\rangle}\right| = p^k$ where $k =$deg $f(x)+$ deg $g(x)$. So $\left|\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle g(x)\rangle}\right| = \left|\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right|\left|\frac{\mathbb{Z}_p[x]}{\langle g(x)\rangle}\right| = p^{\deg(f(x))}p^{\deg(g(x))} = p^k$.
Therefore $\left|\frac{\mathbb{Z}_p[x]}{\langle f(x)g(x)\rangle}\right| = \left|\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle g(x)\rangle}\right|$, and ϕ is onto.
By induction, we have the following.

Corollary 3.3. *If $f_1(x), \ldots, f_n(x)$ are relatively polynomials over the field $F[x]$, then $\frac{F[x]}{\langle f_1(x)\cdots f_n(x)\rangle} \approx \frac{F[x]}{\langle f_1(x)\rangle} \oplus \cdots \oplus \frac{F[x]}{\langle f_n(x)\rangle}$.*

The next theorem is central to our goal.

Theorem 3.4. *([1], Exercise 24, 233) If $R_1, R_2, \ldots, R_n$ are commutative rings with unity, then $U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) \approx U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$.*

Corollary 3.5. *If $f_1(x), f_2(x), \ldots, f_n(x)$ are relatively prime polynomials from $F[x]$ where F is a field, then $U\left(\frac{F[x]}{\langle f_1(x)\cdots f_n(x)\rangle}\right) \approx U\left(\frac{F[x]}{\langle f_1(x)\rangle} \oplus \cdots \oplus \frac{F[x]}{\langle f_n(x)\rangle}\right) \approx U\left(\frac{F[x]}{\langle f_1(x)\rangle}\right) \oplus \cdots \oplus U\left(\frac{F[x]}{\langle f_n(x)\rangle}\right)$*

Corollary 3.6. *Let $a_1, \ldots, a_n$ be distinct elements in $\mathbb{Z}_p$. Then $U\left(\frac{\mathbb{Z}_p[x]}{\langle (x-a_1)(x-a_2)\cdots(x-a_n)\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \cdots \oplus \mathbb{Z}_{p-1}$.*

Proof. From Corollary 3.3, Theorem 3.4 and Corollary 3.5, we have $U\left(\frac{\mathbb{Z}_p[x]}{\langle (x-a_1)(x-a_2)\cdots(x-a_n)\rangle}\right) \approx U\left(\frac{\mathbb{Z}_p[x]}{\langle x-a_1\rangle}\right) \oplus \cdots \oplus U\left(\frac{\mathbb{Z}_p[x]}{\langle x-a_n\rangle}\right) \approx \mathbb{Z}_{p-1} \oplus \cdots \oplus \mathbb{Z}_{p-1}$. □

In light of Corollary 3.6, we will hence forth will limit ourselves to rings of the form $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ for special cases of $f(x)$. The value of Theorem 3.7 is that we can determine the structure of $\frac{\mathbb{Z}_p[x]}{\langle (x-a)^k\rangle}$ by focusing on the case $\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}$, which is easy to handle when finding the order of elements.

Theorem 3.7. *For all $k > 1$ and all $a \in \mathbb{Z}_p$, $\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}$ is isomorphic to $\frac{\mathbb{Z}_p[x]}{\langle (x-a)^k\rangle}$.*

Proof. Let ϕ be the mapping from $\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}$ to $\frac{\mathbb{Z}_p[x]}{\langle (x-a)^k\rangle}$ given by $\phi(f(x) + \langle x^k\rangle) = f(x-a) + \langle (x-a)^k\rangle$. We first show that ϕ is well-defined. Suppose $f(x) + \langle x^k\rangle = g(x) + \langle x^k\rangle$ where $f(x),\ g(x) \in \frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}$. Our goal is to show $\phi(f(x)) = \phi(g(x))$. From $f(x) + \langle x^k\rangle = g(x) + \langle x^k\rangle$, we have $f(x-a) + \langle (x-a)^k\rangle = g(x-a) + \langle (x-a)^k\rangle$ by replacing x by $x-a$. Therefore $\phi(f(x)) = \phi(g(x))$ and ϕ is well-defined.

To prove ϕ is onto, observe that for $g(x) + \langle (x-a)^k\rangle \in \mathbb{Z}_p[x]/\langle (x-a)^k\rangle$ we have $\phi(g(x+a) + \langle x^k\rangle) = g(x+a-a) + \langle (x+a-a)^k\rangle = g(x) + \langle x^k\rangle$. Thus, ϕ is onto. That ϕ is one-to-one follows from $\left|\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right| = \left|\frac{\mathbb{Z}_p[x]}{\langle (x-a)^k\rangle}\right|$. Finally to show operation preserving under multiplication, note that, $\phi(f(x)g(x) + \langle x^k\rangle) = f(x-a)g(x-a) + \langle (x-a)^k\rangle = (f(x-a) + \langle (x-a)^k\rangle(g(x-a) + \langle (x-a)^k\rangle) = \phi((f(x) + \langle x^k\rangle)\phi((g(x) + \langle x^k\rangle)$. Therefore ϕ is an isomorphism. □

Our first goal is to determine the order of $U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$. To do so, we instead determine the number of non-units in $\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}$ where $k > 1$.

Theorem 3.8. *For $G = U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$, where $k > 1$, the number of non-units (zero + zero divisors) is p^{k-1}.*

Proof. Suppose that $f(x) + \langle x^k \rangle$ is a zero-divisor and $(f(x) + \langle x^k \rangle)(g(x) + \langle x^k \rangle) = f(x)g(x) + \langle x^k \rangle = 0 + \langle x^k \rangle$ for some $g(x) + \langle x^k \rangle \in \frac{\mathbb{Z}_p[x]}{\langle x^k \rangle}$. Then $f(x)g(x) \in \langle x^k \rangle$, which means $f(x)g(x) = h(x)x^k$. From deg $f(x) \leq k-1$ and deg $g(x) \leq k-1$, we know that deg $f(x)g(x) =$ deg $f(x)+$ deg $g(x) \leq 2k-2$. This means deg$(h(x)x^k) \leq 2k-2$. Since deg$(x^k) = k$, we know deg $h(x) \leq k-2$. Thus $h(x) = c_{k-2}x^{k-2} + c_{k-1}x^{k-1} + \cdots + c_1x + c_0$ with $c_{k-2}, \ldots, c_0 \in \mathbb{Z}_p$. So we have p choices for each coefficient and therefore $p^{k-1} - 1$ zero divisors in $\frac{\mathbb{Z}_p[x]}{\langle x^k \rangle}$. All other non-zero elements in $\frac{\mathbb{Z}_p[x]}{\langle x^k \rangle}$ are units. □

Corollary 3.9. $\left| U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k \rangle}\right) \right| = (p-1)p^{k-1}$.

It follows from Theorem 3.8 the isomorphism class decomposition of $G = U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k \rangle}\right)$ consists of $\mathbb{Z}_{p-1}$ and the factorization of the Sylow p-subgroup of G. To simplify the notation, for a prime p and an integer $k > 1$, we will use $G_{p,k}$ to denote the group $U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k \rangle}\right)$ and $Syl(G_{p,k})$ to denote the Sylow p-subgroup of $G_{p,k}$.

In the following example we investigate the structure of $G_{p,k}$ when $p = 3$ and $2 \leq k \leq 12$, which were obtained by computer calculations. The general case follows a similar pattern.

Example 3.10.

$$
\begin{aligned}
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^5\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^6\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^8\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^9\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\Big) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3
\end{aligned}
$$

Following we determine the structure of $Syl(G_{p,k})$. First, we need an important fact about powers of the form $(a_1 + \cdots + a_m)^{p^k}$ in a ring of prime characteristic p.

Definition 3.11. *([1], 240) The characteristic of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.*

Theorem 3.12. *For elements $a_1, a_2, \ldots, a_m$ from a commutative ring of prime characteristic p, we have $(a_1 + \cdots + a_m)^{p^k} = {a_1}^{p^k} + {a_2}^{p^k} + \cdots + {a_m}^{p^k}$.*

Proof. By induction on m it suffices to prove the case when $m = 2$. Observe that, for $a_1, a_2 \in R$ we have, $(a_1 + a_2)^{p^k} = \binom{p^k}{0}{a_1}^{p^k}{a_2}^0 + \binom{p^k}{1}{a_1}^{p-1}{a_2}^1 + \cdots + \binom{p^k}{p^k}{a_1}^0{a_2}^{p^k} = {a_1}^{p^k} + {a_2}^{p^k}$ as all other coefficients are a multiple of p. □

Another useful fact is the following.

Theorem 3.13. *Fermat's Little Theorem ([1], 143) For every integer a and every prime p, a^p mod $p = a$ mod p.*

From Theorem 3.12 and Theorem 3.13 in $\mathbb{Z}_p$ we have the following.

Corollary 3.14. *For a prime p and $a_1, a_2, \ldots, a_m$, we have $(a_1 + a_2 + \cdots a_m)^p = a_1 + a_2 + \cdots + a_m$.*

Having characteristic p for $G_{p,k}$ helps with proving statements about orders of elements in the group. Our first task is to determine the exponent of $Syl(G_{p,k})$. That is, the smallest positive integer p^i where $a^{p^i} = 1$ for all $a \in G_{p,k}$. We denote this integer by $exp(Syl(G_{p,k}))$. Knowing the order of elements in $Syl(G_{p,k})$ will allow us to determine the isomorphism class of $G_{p,k}$ for odd prime p.

Theorem 3.15. *For an odd prime p and an integer k with $p^{i-1} < k \leq p^i$, the exponent of $Syl(G_{p,k}) = p^i$.*

Proof. We may view $G_{p,k} = \{c_{k-1}x^{k-1} + \cdots + c_1x + c_0 \,|\, c_{k-1}, \ldots, c_0 \in \mathbb{Z}_p, c_0 \neq 0\}$, where multiplication is done modulo $\langle x^k \rangle$. If $c_0 = 0$, then the polynomial $c_{k-1}x^{k-1} + \cdots + c_1x$ has a factor of x meaning the polynomial would be a zero-divisor and not in the set. For $c_0 = 1$, observe that, $(c_{k-1}x^{k-1} + \cdots + c_1x + c_0)^{p^i} = (c_{k-1})^{p^i}x^{p^i(k-1)} + \cdots + (c_1)^{p^i}x^{p^i} + c_0^{p^i} = (c_{k-1})^{p^i}(0) + \cdots + (c_1)^{p^i}(0) + 1 = 1$. Therefore, the order of every element of the form $c_{k-1}x^{k-1} + \cdots + c_1x + 1$ in $G_{p,k}$ divides p^i. To complete the proof, it suffices to show that $G_{p,k}$ has an element of order p^i. Consider the element $x + 1 \in G_{p,k}$. We know $x + 1 \in G_{p,k}$ as $x + 1$ does not have a factor of x. We want to show that $x + 1$ has order p^i. From Theorem 3.12, we have, $(x + 1)^{p^{i-1}} = x^{p^{i-1}} + 1^{p^{i-1}} = x^{p^{i-1}} + 1 \neq 1$. But $(x + 1)^{p^i} = x^{p^i} + 1^{p^i} = 0 + 1 = 1$. Therefore $x + 1$ has order p^i. □

Corollary 3.16. *For an odd prime p, $exp(Syl(G_{p,k})) = p^i$ where i is the smallest positive integer such that $p^i \geq k$. For any given p, k, it follows that $i = \lceil \log_p k \rceil$.*

Proof. We know from Theorem 3.15, $p^i = exp(Syl(G_{p,k}))$. We can give an explicit formula for i. Note that, $i = \log_p p^i \geq \log_p k > \log_p p^{i-1} = i - 1$. Thus $i = \lceil \log_p k \rceil$. □

Now that we know $exp(Syl(G_{p,k}))$, we can make a general statement about the structure of the isomorphism class for $G_{p,k}$. For future reference we will want to know the order of the element $x+1 \in G_{p,k}$.

Theorem 3.17. *Let p be a prime and k such that $p^{i-1} < k \leq p^i$. For the element $x+1 \in G_{p,k}$ and $c_0 \in U(p)$, we have $|c_0(x+1)| = |c_0|p^i$.*

Proof. Since $(x+1)^{p^i} = x^{p^i}+1 = 1$ and $(x+1)^{p^{i-1}} = x^{p^{i-1}}+1 \neq 1$, we know $|x+1| = p^i$. Because $c_0 \in U(p) \approx \mathbb{Z}_{p-1}$, $|c_0|$ divides $p-1$. Therefore $|c_0|$ and $|x+1|$ are relatively prime and $|c_0(x+1)| = |c_0||x+1| = |c_0|p^i$. □

Corollary 3.18. *For $g(x) \in G_{p,k}$, where $p^i \geq k$ and $g(x)$ has a constant term $c_0 \in U(p)$, we have $|g(x)| = |c_0|p^i$.*

Example 3.19.

If $g(x) = 2x^3+x+3 \in G_{5,4}$, then $|g(x)| = |3|5 = 4{\cdot}5$. □

Theorem 3.20. *For prime p and an integer k with $p^{i-1} < k \leq p^i$, we have $G_{p,k} \approx \mathbb{Z}_{p-1} \oplus Syl(G_{p,k})$.*

Proof. We must show that every element in $G_{p,k}$ can uniquely written in the form ab where a is in Z_{p-1} and b is in $Syl(G_{p,k})$. Every element has the form $c_{k-1}x^{k-1} + \cdots + c_1x + c_0$ where $c_i \in U(p)$ for $0 \leq i \leq k-1$ and $c_0 \neq 1$. Since c_0 has a multiplicative inverse, we factor out c_0 from $c_{k-1}x^{k-1}+\cdots+c_1x+c_0$, to obtain $c_0(c_0^{-1}c_{k-1}x^{k-1}+\cdots+c_0^{-1}c_1x+1) = ab$ where $a = c_0 \in \mathbb{Z}_{p-1}$ and $b = c_0^{-1}c_{k-1}x^{k-1} + \cdots + c_0^{-1}c_1x + 1 \in Syl(G_{p,k})$. □

As a corollary of Theorem 3.20, we obtain the structure of $G_{p,k}$ for $p \leq k$. But first we define the rank of $Syl(G_{p,k})$, denoted by $rk(Syl(G_{p,k}))$, as the number of terms in the factorization of $Syl(G_{p,k})$. We determine the rank of $Syl(G_{p,k})$ by finding the number of elements of order p in $G_{p,k}$. The rank and the exponent of $G_{p,k}$ together determine the structure of $G_{p,k}$.

Corollary 3.21. *If $k \leq p$, then $G_{p,k} \approx \mathbb{Z}_{p-1} \oplus \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k-1}$.*

Proof. We know that there is no element of order p^2 since the exponent of $Syl(G_{p,k})$ is p for $k \leq p$. Since $\mathbb{Z}_p^* = U(p) \approx \mathbb{Z}_{p-1}$, this is the subgroup of constant polynomials. For the $Syl(G_{p,k})$, all the elements are of the form $c_{k-1}x^{k-1} + \cdots + c_1x + 1$. Observe that, by Theorem 3.12 and Corollary 3.14, we have $(c_{k-1}x^{k-1}+\cdots+c_1x+1)^p = c_{k-1}x^{(k-1)p}+\cdots+ c_1x^p + 1 = 1$ as $k \leq p$. Thus, we have $p^{k-1} - 1$ elements of order p and $rk(Syl(G_{p,k})) = k - 1$, which gives us $k - 1$ $\mathbb{Z}_p$ terms in the external direct product. □

Next, we want to determine the isomorphism class for any general p, k where $p < k$. Let's consider a few examples of the isomorphism class for $p = 3$ and $p < k$.

Example 3.22.

Suppose $k = p = 3$. We want to find the isomorphic class for $G_{3,3}$. Since $exp(Syl(G_{p,k})) = p^i$ where $p^{i-1} < k \leq p^i$, this implies that $exp(G_{3,3}) = 3$ because $1 < 3 \leq 3^1$. Consider the number of elements of order 3. We know $G_{3,3} = \{c_2x^2 + c_1x + c_0 \mid c_2, c_1, c_0 \in \mathbb{Z}_3, c_0 \neq 0\}$ and if $c_0 = 1$, we have, $(c_2x^2+c_1x+1)^3 = c_2x^6+c_1x^3+1 = 1$. So there are $3^2 = 9-1 = 8$ elements of order 3 and $G_{3,3} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. □

Example 3.23.

Suppose $k = 4$ and $p = 3$. To find the isomorphic class for $G_{3,4}$, note that $3 < k \leq 3^2$. So the exponent of $Syl(G_{3,4}) = 9$ giving us at least one $\mathbb{Z}_9$ in the external direct product. For $c_0 = 1$ and $k \leq 2 \cdot 3$, it follows that $(c_3x^3 + c_2x^2 + 1)^3 = c_3(x^3)^3 + c_2(x^2)^3 + 1 = 1$. This means there are $3^{3-1} - 1 = 3^2 - 1$ elements of order 3. Therefore $rk(Syl(G_{3,4})) = 2$ and $G_{3,4} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$. □

In order to find the isomorphism class of $G_{p,k}$, it suffices to determine the isomorphism class of $Syl(G_{p,k})$, the Sylow p-subgroup of $G_{p,k}$. The following theorems are useful for finding $rk(Syl(G_{p,k}))$ for $p < k$. We consider two cases.

Theorem 3.24. *For $k \neq 0$ mod p, $rk(Syl(G_{p,k+1})) = rk(Syl(G_{p,k})) + 1$*

Proof. First observe that if the isomorphism class of $Syl(G_{p,k})$ for any subgroup of $G_{p,k}$ of order a power of p is $\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \cdots \oplus \mathbb{Z}_{p^{n_s}}$ then $rk(Syl(G_{p,k})) = s$. In $G_{p,k}$, let $H_p = \{x \in Syl(G_{p,k}) \mid x^p = e\}$. Then $|H_p| = p^s$ $rk(Syl(G_{p,k}) = s$. Thus we can find s by finding $|H_p|$. We know $|G_{p,k}| = p^{k-1}(p-1)$ where $p^{k-1} = |Syl(G_{p,k})|$. We first observe that every non-identity element in H_p has order p. Let m_p be the smallest integer such that $k \leq m_p p$. If $m_p \leq k-1$, then $(c_{k-1}x^{k-1} + \cdots + c_{m_p}x^{m_p} + 1)^p = c_{k-1}x^{(k-1)p} + \cdots + c_{m_p}x^{m_p p} + \cdots + 1 = 1$, so elements of the form $c_{k-1}x^{k-1} + \cdots + c_{m_p}x^{m_p} + 1$ are in $Syl(G_{p,k})$. Conversely, for any element with a term $c_t x^t$ with $t < m_p$, we have $x^{tp} \neq 0$. For $c_{k-1}, \ldots, c_1 \in \mathbb{Z}_p$, there are p choices for each coefficient. This means we have $p^{(k-1)-(m_p-1)} - 1 = p^{k-m_p} - 1$ elements of order p in $Syl(G_{p,k})$. Therefore $|H_p| = p^{k-m_p} = p^s$, implying that $k - m_p = s = rk(Syl(G_{p,k}))$.

Now we want to show $rk(Syl(G_{p,k+1})) = k - m_p + 1$. The order of $G_{p,k+1} = p^{k+1} - p^k = p^k(p-1)$ and $|Syl(G_{p,k+1})| = p^k$, which means the number of elements of order p is $p^{k-(m_p-1)} - 1 = p^{k-m_p+1} - 1$. Thus $rk(Syl(G_{p,k+1})) = k - m_p + 1 = rk(Syl(G_{p,k})) + 1$. □

Theorem 3.25. *For $k = 0$ mod p, $rk(Syl(G_{p,k+1})) = rk(Syl(G_{p,k}))$.*

Proof. If $k = 0$ mod p, then $k = m_p p$. From the proof of Theorem 3.24, we have $rk(Syl(G_{p,k})) = k - m_p$ when $k \leq m_p p$. Also, $k + 1 = 1$ mod p implies $m_p p < k + 1 \leq (m_p + 1)p$. When $c_0 = 1$, it follows $(c_k x^k + \cdots + c_{m+1}x^{m_p+1} + c_0)^p = c_k x^{kp} + \cdots + c_{m+1}x^{(m_p+1)p} + 1 = 1$. So there are $p^{k-m_p} - 1$ elements of order p and $rk(Syl(G_{p,k+1})) = k - m_p = rk(Syl(G_{p,k}))$. □

Following is the algorithm for finding the rank of $G_{p,k}$ for odd prime p.

3.1 Algorithm for Isomorphism Class of $G_{p,k}$

1. If $k = 1$, then $rk(Syl(G_{p,k})) = 0$ and $|G_{p,k}| = p^{k-1}(p-1) = p - 1$. Thus, $G_{p,k} \approx \mathbb{Z}_{p-1}$.

2. For $k = 2, rk(Syl(G_{p,k})) = 1$ and $|G_{p,k}| = p^{k-1}(p-1) = p(p-1)$. So $G_{p,k} \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p$.

3. When $k = 3$, $rk(Syl(G_{p,k})) = 2$ and $|G_{p,k}| = p^{k-1}(p-1) = p^2(p-1)$, which means $G_{p,k} \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

4. When $2 < k \leq p^2$ and $k \neq 1 \bmod p$, add $\mathbb{Z}_p$ to the previous case.

5. If $2 < k \leq p^2$ and $k = 1 \bmod p$, replace $\mathbb{Z}_p$ with $\mathbb{Z}_{p^2}$ in the previous case.

6. When $p^2 < k \leq p^3$ and $k = 1 \bmod p$, add $\mathbb{Z}_p$ to the previous case.

7. When $p^2 < k \leq p^3$ and $k \neq 1 \bmod p$, the rank remains the same as the previous one but we replace one $\mathbb{Z}_{p^2}$ with $\mathbb{Z}_{p^3}$ because p^3 is the $exp(Syl(G_{p,k}))$. If one $\mathbb{Z}_{p^3}$ already exists, then we replace one of the $\mathbb{Z}_p$ with $\mathbb{Z}_{p^2}$. □

To generalize for p and k with $p < k$, let m_p be the unique integer such that $(m_p - 1)p < k \leq m_p p$. Our next task is to show that if there are exactly $p^{k-m_p} - 1$ elements of order p and $rk(Syl(G_{p,k})) = k - m_p$, we are able to find the isomorphism class for $G_{p,k}$ given any values of p, k with $p < k$. Let's consider an example using the formula for $rk(Syl(G_{p,k}))$.

Example 3.26.

Let $p = 3$ and $k = 16$. Since $3 < 16$, the value of $m_3 = 6$. This means $rk(Syl(G_{3,16})) = k - m_3 = 16 - 6 = 10$, the number of terms in the isomorphism class of the $Syl(G_{3,16})$. To determine the order of each component in the external direct product, we can find the number of elements of orders of powers of 3. Since $(c_{15}x^{15} + \cdots + c_6x^6 + 1)^3 = 1$, we have $3^{10} - 1$ elements of order 3. Also, $(c_{15}x^{15} + \cdots + c_2x^2 + 1)^9 = 1$, resulting in $3^{14} - (3^{10} - 1)$ elements of order 9. And lastly, $(c_{15}x^{15} + \cdots + c_1x + 1)^9 = 1$, which means there are $3^{15} - (3^{14} - (3^{10} - 1))$ elements of order 27. This forces $G_{3,16}$ to be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \underbrace{\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3}_{6}$. □

Example 3.27.

If $p = 3$ and $k = 19$, then $6 \cdot 3 < 19 \leq 7 \cdot 3$. So the $rk(Syl(G_{3,19})) = k - m_{19} = 19 - 7 = 12$. Using Theorem 3.15 we have $exp(Syl(G_{3,19})) = 27$. We can find an element in $G_{3,19}$ of order 27 that generates the subgroup $\mathbb{Z}_{27}$. Note that, $(x+1)^{27} = x^{27}+1 = 0+1 = 1$, whereas $(x+1)^9 = x^9 + 1 \neq 1$. To determine the isomorphism class of $Syl(G_{3,19})$, it suffices to find the number of elements of order $3, 9$, and 27. Elements of order 3 have the form $c_{18}x^{18} + \cdots + c_7x^7 + 1$. Therefore we have $3^{18-6} - 1 = 3^{12} - 1$ elements of order 3. Similarly, elements of order 9 have the form, $(c_{18}x^{18} + \cdots + c_3x^3 + 1)$. There are $3^{16} - (3^{12} - 1)$ elements of order 9 as when $c_8 = c_7 = \cdots = c_3 = 0$, we are counting the elements of order 3. For the elements of order 27, we have $3^{18} - (3^{16} - (3^{12} - 1))$. Therefore, $G_{3,19} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \underbrace{\mathbb{Z}_3 \oplus \cdots \oplus \mathbb{Z}_3}_{7}$. □

The advantage of knowing the order of specific elements in $G_{p,k}$, is that it allows us to find the internal direct product of $G_{p,k}$. The next theorem tells us that if we know the internal direct product, we also know the isomorphism class of the external direct product.

Definition 3.28. *([1], 184) Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the internal direct product of $H_1, H_2, \ldots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if*

1. $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i\}$,
2. $(H_1H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ *for* $i = 1, 2, \ldots, n-1$.

Theorem 3.29. *([1],185) If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then $G \approx H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$.*

Example 3.30.

Suppose $p = 3$ and $3 \leq k \leq 10$. We determine the external and internal direct product for $G_{3,k}$.

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle$

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle$

Note that the subgroup $\langle x^3+1\rangle$ is contained in $\langle x+1\rangle$.

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^5\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^4+1\rangle$

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^6\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle$

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle$

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^8\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle \times \langle x^7+1\rangle$

Note that $\langle x^6+1\rangle$ is contained in $\langle x^2+1\rangle$.

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^9\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle \times \langle x^7+1\rangle \times \langle x^8+1\rangle$

$U\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \langle 2\rangle \times \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle \times \langle x^7+1\rangle \times \langle x^8+1\rangle$ □

In general, for the internal direct product of $G_{p,k}$, the terms of the form $\langle 1+x^{pt}\rangle$ are not present. This is because they are contained in the earlier terms in the product. Next, we give the algorithm for finding the internal and external product of $G_{p,k}$ given any p and k.

3.2 Algorithm for Internal/External Direct Product

The following is an algorithm for the internal and external direct product of $G_{p,k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$.

Case 1:

1. If $k \leq p$, then $U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right) \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k-1} \oplus \mathbb{Z}_{p-1}$

Case 2: For $p < k$.

1. For the given values p, k, find the smallest positive integer m_p, such that $k \leq m_p p$. Then $rk(Syl(G_{p,k})) = k - m_p$. Then there is a total of $k - m_p + 1$ terms in the internal and external direct product.

2. To find the internal direct product of $G_{p,k}$, fill the first slot of the internal direct product with $\langle c_0 \rangle$ such that $c_0 \in U(p)$ such that $|c_0| = p - 1$.

3. Fill the $k - m_p = rk(Syl(G_{p,k}))$ remaining slots with $\langle x^i + 1 \rangle$ where $1 \leq i$ and skipping when i is a multiple of p. Continue this process until all $k - m_p$ slots are filled.

4. If there are slots remaining, fill the slots with $\langle x^i + x + 1 \rangle$ where $2 \leq i$ and skipping when i is a multiple of p.

5. We now have the internal direct of $G_{p,k}$. For each term, find the order of each subgroup generator.

6. The order of each tells us the isomorphism class, giving us the construction of external direct product. □

Here is an example to illustrate the method.

Example 3.31.

Consider the case when $p = 5$ and $k = 11$. We want to find the external direct product of $G_{5,11}$ using the fact that $k = 11 \leq m_p p = 3 \cdot 5$. There are $k - m_p + 1 = 11 - 3 + 1 = 9$ terms. We will find the internal direct product first. The first term is an element $c_0 \in U(p)$ where $|c_0| = p - 1$. Then we will fill the remaining 8 spots with $x^i + 1$ skipping values i that are multiples of 5. This gives us

$$\langle 2 \rangle \times \langle x+1 \rangle \times \langle x^2+1 \rangle \times \langle x^3+1 \rangle \times \langle x^4+1 \rangle \times \langle x^6+1 \rangle \times \langle x^7+1 \rangle \times \langle x^8+1 \rangle \times \langle x^9+1 \rangle.$$

To obtain the external direct product, we find the orders of each generator. Since $2 \in U(5)$ such that $|2| = 4$, the first term of the external direct product is $\mathbb{Z}_4$. Computing the remainder of orders of the elements utilizing the fact that $x^k = x^{11} = 0$ gives us, $|x+1| = |x^2+1| = 25$ and $|x^3+1| = |x^4+1| = |x^6+1| = |x^7+1| = |x^8+1| = |x^9+1| = 5$.

From Theorem 3.29, the internal direct product is isomorphic to the external direct product, which means

$$\begin{aligned} & G_{5,11} \\ & \approx \langle 2 \rangle \times \langle x+1 \rangle \times \langle x^2+1 \rangle \times \langle x^3+1 \rangle \times \langle x^4+1 \rangle \times \langle x^6+1 \rangle \\ & \qquad \times \langle x^7+1 \rangle \times \langle x^8+1 \rangle \times \langle x^9+1 \rangle \\ & \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \end{aligned} \qquad \square$$

We mentioned that the above results pertaining to the isomorphism class of groups of the form $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}\right)$ carry over to all finite fields where we replace p with q where q is a prime power. Our results involving the internal direct product rely on the specified prime p and the specific polynomial $f(x)$ for $\frac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}$. Note, that the previous results pertained to reducible polynomials over $\mathbb{Z}_p$. The next theorem explains why.

Theorem 3.32. *([1], 295) Let F be a field and $p(x)$ be an irreducible polynomial over F. Then $\frac{F[x]}{\langle p(x) \rangle}$ is a field, and when F is finite, the nonzero elements form a cyclic group.*

In the next section, we investigate the case when $f(x)$ is a degree 2 irreducible polynomial over $\mathbb{Z}_p$. For $f(x)^k$ with $k > 1$, the factor ring $\frac{\mathbb{Z}_p[x]}{\langle f(x)^k \rangle}$ is a not field, since $f(x)$ is a zero-divisor in $\mathbb{Z}_p$.

4 $U\left(\frac{\mathbb{Z}_p[x]}{\langle (f(x))^k \rangle}\right)$ where $f(x)$ is a quadratic irreducible over $\mathbb{Z}_p$

In Section 3, our results handle $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}\right)$ for all $f(x)$ of degrees 2 and 3 and all polynomials of degree 4 or 5 except those that have a factor of the form $(g(x))^2$ where $g(x)$ has degree 2 irreducible polynomial over $\mathbb{Z}_p$. In this section we investigate $G_{p,2k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k \rangle}\right)$ for the case when $f(x)$ is a quadratic irreducible over $\mathbb{Z}_p$. Before we begin with $f(x) = x^2 + 1$,

we first need a lemma.

Lemma 4.1. *If p is a prime of the form $1 + 4t$, then $x^2 + 1$ is reducible over $\mathbb{Z}_p$.*

Proof. Suppose $p = 4t + 1$ for some $t \in \mathbb{N}$. We want to show that $x^2 + 1$ is reducible in $\mathbb{Z}_p$. For any element $c_0 \in U(p) \approx \mathbb{Z}_{p-1} \approx \mathbb{Z}_{4t}$ and the order of c_0 divides $4t$. But since $\mathbb{Z}_{4t}$ is cyclic, there exists an element for each divisor of $4t$. In particular, there exists an element $c_0 \in \mathbb{Z}_{4t}$ such that $|c_0| = 4$. So ${c_0}^4 = 1$, which implies ${c_0}^4 - 1 = 0$ and $({c_0}^2 - 1)({c_0}^2 + 1) = 0$. If ${c_0}^2 - 1 = 0$, then $|c_0| = 2$ which is a contradiction as $|c_0| = 4$. So ${c_0}^2 + 1 = 0$ implies $-{c_0}^2 = 1$ and $(x - c_0)(x + c_0) = x^2 - {c_0}^2 = x^2 + 1$. Thus c_0 is a zero of the polynomial $x^2 + 1$ and therefore $x^2 + 1$ is reducible in $\mathbb{Z}_p$. □

Because $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is a field when $f(x)$ is irreducible over $\mathbb{Z}_p$, we consider $f(x)^k$ for $k \geq 2$ and find the isomorphism class for the Sylow p-subgroup of $G_{p,2k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$. We first determine the order of this group.

Theorem 4.2. *When $f(x)$ an irreducible polynomial of degree 2 over $\mathbb{Z}_p$ and $k > 1$, we have $|G_{p,2k}| = \left|U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)\right| = p^{2k-2}(p^2 - 1)$.*

Proof. Suppose $g(x) \in \frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}$ and $g(x)$ is a zero-divisor. Then deg $g(x) \leq 2k - 1$ and $g(x)$ must have $f(x)$ as a factor. So $g(x) = (c_{2k-3}x^{2k-3} + \cdots + c_1x + c_0)f(x)$. We have p choices for each coefficient, giving us p^{2k-2} terms that are zero-divisors or zero. Therefore the order of $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ is $p^{2k} - p^{2k-2}$. □

We begin with an illustrative example of $p = 3$ and $3 \leq k \leq 6$, which were obtained by computer calculations. The general case follows the same pattern.

Example 4.3.

$$U\Big(\frac{\mathbb{Z}_3[x]}{\langle(x^2+1)^2\rangle}\Big) \approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$
$$U\Big(\frac{\mathbb{Z}_3[x]}{\langle(x^2+1)^3\rangle}\Big) \approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$
$$U\Big(\frac{\mathbb{Z}_3[x]}{\langle(x^2+1)^4\rangle}\Big) \approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$
$$U\Big(\frac{\mathbb{Z}_3[x]}{\langle(x^2+1)^5\rangle}\Big) \approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$
$$U\Big(\frac{\mathbb{Z}_3[x]}{\langle(x^2+1)^6\rangle}\Big) \approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \qquad \square$$

In each case, observe that $rk(Syl(G_{p,2k})) = n$, where the number of elements of order 3 is $3^n - 1$. As before, for a fixed k and p, let m_p be the smallest integer such that $k \leq m_p p$. Then $2k \leq 2m_p p$.

Theorem 4.4. *Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}_p$ and deg$f(x) = 2$. For $k \leq m_p p$ and $m_p < k$, the $rk(Syl(G_{p,2k})) = 2k - 2m_p$.*

Proof. Consider the elements of the form $f(x)^{m_p}(h(x)) + 1$ for $h(x) \in \frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}$. The degree of such an element is deg $(h(x)) + 2m_p < 2k$, which implies deg $(h(x)) < 2k - 2m_p$. So, the elements $f(x)^{m_p}(h(x)) + 1 = f(x)^{m_p}(c_{2k-2m_p-1}x^{2k-2m_p-1} + \cdots + c_0) + 1$. There are p choices for each of the $2k - 2m_p$ coefficients, giving us $p^{2k-2m_p} - 1$ elements of order p. Thus, $rk(Syl(G_{p,2k})) = 2k - 2m_p$. $\square$

The next two results are analogous of Theorem 3.24 and Theorem 3.25.

Corollary 4.5. *If $G_{p,2k} = U\Big(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\Big)$ and $p|k$, then $rk(Syl(G_{p,2k})) = rk(Syl(G_{p,2k+1}))$.*

Proof. We know from Theorem 4.4 that $rk(Syl(G_{p,2k})) = 2k - 2m_p$ where $k \leq m_p p$. Since $k = 0$ mod p, this implies $k = m_p p$. Then $k + 1 = 1$ mod p, so $k + 1 < (m_p + 1)p$. It follows that the non-identity elements in $G_{p,2(k+1)}$ of the form $f(x)^{m_p+1}h(x) + 1$ have order p. We know deg $(f(x)^{m_p+1}h(x) + 1) =$ deg $(f(x)^{m_p+1})+$ deg $(h(x)) = 2(m_p + 1)+$

deg $h(x) < 2(k+1)$. Thus deg $h(x) < 2k - 2m_p$ and we have $p^{2k-2m_p} - 1$ elements of order p and $rk(Syl(G_{p,2(k+1)})) = rk(Syl(G_{p,2k}))$. □

Corollary 4.6. *If* $G_{p,2k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ *and* $p \nmid k$, *then* $rk(Syl(G_{p,2k}))+2 = rk(Syl(G_{p,2k+1}))$.

Proof. The $rk(Syl(G_{p,2k})) = 2k - 2m_p$. Since $k \neq 0 \bmod p$, then $k+1 \neq 0 \bmod p$ or $k+1 = 0 \bmod p$. But $k \leq m_p p$ implies $k+1 \leq m_p p$ since $k \neq 0 \bmod p$. Then $(f(x)^{m_p}h(x)+1)^p = f(x)^{m_p p}h(x)^p + 1 = 1$. Since $f(x)^{m_p}h(x)+1 \in G_{p,2k}$, deg $(f(x)^{m_p}h(x)+1) = 2m_p +$ deg $h(x) < 2(k+1)$ so deg $h(x) < 2k - 2m_p + 2$. Therefore there are $p^{2k-2m_p+2} - 1$ elements of order p and $rk(Syl(G_{p,2(k+1)})) = rk(Syl(G_{p,2k})) + 2$. □

The following theorem gives us insight of the structure of the external direct product consisting of $Syl(G_{p,2k})$ and the cyclic subgroup of order $p^2 - 1$.

Theorem 4.7. *For* $G_{p,2k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$, *where* $f(x)$ *is an irreducible polynomial of degree* 2 *over* $\mathbb{Z}_p$, $G_{p,2k}$ *has an element of order* $p^2 - 1$.

Proof. Consider the group homomorphism ϕ from the group $G_{p,2k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ to $\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)^* \approx GF(p^2)^*$ given by $\phi(g(x) + \langle f(x)^k\rangle) = g(x) + \langle f(x)\rangle$. We will prove that ϕ is onto. Let $g(x) + \langle f(x)\rangle \in U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. The pre-image of $g(x) + \langle f(x)\rangle$ is $g(x) + \langle f(x)^k\rangle$, which is an element of $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$, since deg $g(x) <$ deg $f(x) <$ deg $f(x)^k$.

Since $GF(p^2)^*$ is a cyclic group of order $p^2 - 1$, let $\phi(g(x))$ be an element in $\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)^*$ such that $|\phi(g(x))| = p^2 - 1$. From property 3 of Theorem 10.1 ([1], pg 196), $|\phi(g(x))|$ divides $|g(x)|$. But we know $\left|U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)\right| = p^{2k-2}(p^2-1)$. So $|g(x)| = p^i(p^2-1)$ for $0 \leq i \leq 2k-2$. It follows that $|(g(x))^{p^i}| = p^2 - 1$. Therefore $G_{p,2k} = U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ has an element of order $p^2 - 1$. □

Corollary 4.8. *For prime* p *and an integer* k *with* $p^{i-1} < k \leq p^i$, *we have* $G_{p,2k} = \mathbb{Z}_{p^2-1} \oplus Syl(G_{p,2k})$.

Proof. Following from Theorem 4.7, we have a cyclic subgroup of order $p^2 - 1$, giving a $\mathbb{Z}_{p^2-1}$ term in the external direct product. All elements of the form $(x^2 + a)^t h(x) + 1$ will

make up the $Syl(G_{p,2k})$ subgroup, where $t \leq k-1$ and $h(x) \in \mathbb{Z}_p[x]$. These elements will have order that divides p^i since $((x^2+a)^t h(x)+1)^{p^i} = (x^2+a)^{tp^i} h(x)^{p^i} + 1 = 1$. □

4.1 Algorithm for isomorphism class of $G_{p,2k}$ where deg $f(x) = 2$, $f(x)$ is irreducible, and $1 \leq k < p^3$

1. If $k = 1$, then $G_{p,2k} \approx \mathbb{Z}_{p^2-1}$.

2. If $k = 2 < p$, $rk(Syl(G_{p,2k})) = 2$ and $|G_{p,2k}| = p^{2k-2}(p^2-1) = p^2(p^2-1)$. So $G_{p,2k} \approx \mathbb{Z}_{p^2-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

3. If $k = 3 < p$, we have $rk(Syl(G_{p,2k})) = 4$ and $|G_{p,2k}| = p^{2k-2}(p^2-1) = p^4(p^2-1)$, which means $G_{p,2k} \approx \mathbb{Z}_{p^2-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

4. If $k \leq k < p$, continue by adding two $\mathbb{Z}_p$ to the previous case.

5. If $p < k \leq p^2$ and $k \neq 1 \bmod p$, add two $\mathbb{Z}_p$ to the previous case.

6. If $p < k \leq p^2$ and $k = 1 \bmod p$, replace two of the $\mathbb{Z}_p$ with $\mathbb{Z}_{p^2}$ in the previous case.

7. When $p^2 < k \leq p^3$ and $k = 1 \bmod p$, add two $\mathbb{Z}_p$ to the previous case.

8. If $p^2 < k \leq p^3$ and $k \neq 1 \bmod p$, the rank remains the same as the previous. Replace two $\mathbb{Z}_{p^2}$ with $\mathbb{Z}_{p^3}$ because $p^3 = exp(Syl(G_{p,2k}))$. If two $\mathbb{Z}_{p^3}$ already exist, then replace two $\mathbb{Z}_p$ with two $\mathbb{Z}_{p^2}$.

□

Analogous to the reducible case, we will use the internal direct product to gives us the external direct product for all p and k. All odd primes p have an irreducible polynomial of the form $f(x) = x^2 + c_0$. When $p = 2$, we used the polynomial $f(x) = x^2 + x + 1$ to make generalizations about the internal direct product.

4.2 Algorithm for Internal/External Direct Product for $U\left(\frac{\mathbb{Z}_p[x]}{\langle (f(x)^k \rangle}\right)$ for $2 \leq k$ and $f(x)$ is an irreducible polynomial over $\mathbb{Z}_p$

Case 1:

1. If $k \leq p$, then $G_{p,2k} \approx \mathbb{Z}_{p^2-1} \oplus \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{2k-2}$

Case 2:

1. For $p < k$, let m_p be the smallest integer such that $k \leq m_p p$. Then $rk(Syl(G_{p,2k})) = 2k - 2m_p$ and there are a total of $2k - 2m_p + 1$ terms in the factorization of the external direct product.

2. To find the internal direct product of $G_{p,2k}$, fill the first position of the internal direct product with the element of order $p^2 - 1$ in $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k \rangle}\right)$.

3. Fill the remaining $2k - 2m_p$ slots with $\langle f(x)^j + 1 \rangle$ and $\langle f(x)^j x + 1 \rangle$ where $1 \leq j$ and j is not a multiple of p. Continue this process until all $2k - 2m_p$ slots are filled.

4. We now have the internal direct product of $G_{p,2k}$. To obtain the external direct product, replace every term of the internal direct product by the group of the form $\mathbb{Z}_r$, where r is the order of the generator.

In the next example, the generators for the term $\mathbb{Z}_8$ in the internal direct product were found by a computer.

Example 4.9.

$$
\begin{aligned}
U\Big(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^2\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\approx \langle x^3+1\rangle \times \langle (x^2+1)+1\rangle \times \langle (x^2+1)x+1\rangle \\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^2\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\approx \langle x^3+1\rangle \times \langle (x^2+1)+1\rangle \times \langle (x^2+1)x+1\rangle \\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^3\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\approx \langle x^3+1\rangle \times \langle (x^2+1)+1\rangle \times \langle (x^2+1)x+1\rangle \\
&\qquad \times \langle (x^2+1)^2+1\rangle \times \langle (x^2+1)^2x+1\rangle \\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\approx \langle x^7+x^3+x+1\rangle \times \langle (x^2+1)+1\rangle \times \langle (x^2+1)x+1\rangle \\
&\qquad \times \langle (x^2+1)^2+1\rangle \times \langle (x^2+1)^2x+1\rangle \\
U\Big(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^5\rangle}\Big) &\approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\approx \langle x^9+1\rangle \times \langle (x^2+1)+1\rangle \times \langle (x^2+1)x+1\rangle \times \langle (x^2+1)^2+1\rangle \\
&\qquad \times \langle (x^2+1)^2x+1\rangle \times \langle (x^2+1)^4+1\rangle \times \langle (x^2+1)^4x+1\rangle \quad \square
\end{aligned}
$$

Here is the verification for $U\Big(\frac{\mathbb{Z}_p[x]}{\langle (x^2+1)^4\rangle}\Big)$. Let $H_1 = \langle x^7+x^3+x+1\rangle, H_2 = \langle (x^2+1)+1\rangle, \ldots, H_5 = \langle (x^2+1)^4x+1\rangle$. Since $U\Big(\frac{\mathbb{Z}_p[x]}{\langle (x^2+1)^4\rangle}\Big)$ is Abelian and $\Big|U\Big(\frac{\mathbb{Z}_p[x]}{\langle (x^2+1)^4\rangle}\Big)\Big| = |H_1||H_2||H_3||H_4||H_5|$, all we need to do is show that $H_1H_2\cdots H_n \cap H_{n+1} = \{1\}$ for $i = 1, 2, 3, 4$. We can ignore the H_1 term because it has order 8 and all the other terms have order a power of 3. We first show that $H_2 \cap H_3 = \{1\}$. If the intersection was not just the identity, then they would have an element of order 3 in common. So $((x^2+1)+1)^3 = ((x^2+1)x+1)^s$ where $s = 3$ or 6. But evaluating $x = 0$ gives 2 on the left and 1 on the right, which confirms that $H_2 \cap H_3 = \{1\}$. Next, we show that $H_2H_3 \cap H_4 = \{1\}$. If $H_2H_3 \cap H_4 \neq \{1\}$, then they have an element of order 3 in common. So we have

$((x^2+1)+1)^{s_1}((x^2+1)x+1)^{s_2} = ((x^2+1)^2+1)^3$. But evaluating on the left at $x=1$ gives 0 and on the right gives 2. Thus $H_2H_3 \cap H_4 = \{1\}$. Next, we want to show $H_2H_3H_4 \cap H_5 = \{1\}$. If $H_2H_3H_4 \cap H_5 \neq \{1\}$, then they would have an element of order 3 in common. So we have $((x^2+1)+1)^{s_1}((x^2+1)x+1)^{s_2}((x^2+1)^2+1)^{s_3} = ((x^2+1)^2x+1)$. Evaluating at $x=1$ on the left side, each factor gives us 0 and on the right side we get 2. Thus $H_2H_3H_4 \cap H_5 = \{1\}$. Therefore, $U\left(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4\rangle}\right) \approx \langle x^7+x^3+x+1\rangle \times \langle (x^2+1)+1\rangle \times \langle (x^2+1)x+1\rangle \times \langle (x^2+1)^2+1\rangle \times \langle (x^2+1)^2x+1\rangle$. We have the full classification for reducible and irreducible polynomials over $\mathbb{Z}_p$. Next, we will study the structure of subgroups of $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ for various $f(x)$.

5 Subgroups of the form $U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ where $f(x)$ is reducible over $\mathbb{Z}_p$

In [1] Gallian uses the set $U_k(n) = \{x \in U(n) \mid x = kt+1, t \in \mathbb{Z}\}$ to create subgroups of $U(n)$.

Example 5.1.

One subgroup of $U(105)$ is $U_7(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}$. To see that this is a subgroup, note that $a = 1 \bmod 7$ and $b = 1 \bmod 7$, then $ab \bmod 7 = (a \bmod 7)(b \bmod 7) = 1 \cdot 1 = 1$. □

In this section we investigate the analog to the subgroups of $U(n)$. We define a subgroup of $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ as $U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right) = \{h(x) \in U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right) \mid h(x) = g(x)t(x)+1\}$ where deg $g(x) \leq$ deg $h(x) <$ deg $f(x)$ and $t(x) \in \mathbb{Z}_p[x]$. We will give a few examples to illustrate this idea.

Example 5.2.

Let $g(x) = x,\ f(x) = x^2$ and $p = 3$. Then, $U_x\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) = \left\{h(x) \in U\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) \,\middle|\, h(x) =\right.$

$xt(x)+1\Big\}$ and $t(x) \in \mathbb{Z}_3[x]$. For $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) = \{1, 2, x+1, x+2, 2x+1, 2x+2\} = \langle x+2\rangle$, which means $U_x\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) = \{1, x+1, 2x+1\} = \langle x+1\rangle$. □

Example 5.3.

Suppose $g(x) = x^2$, $f(x) = x^3$ and $p = 3$. Then, $U_{x^2}\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right) = \left\{h(x) \in U\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right) \middle| h(x) = x^2\, t(x) + 1\right\}$ and $t(x) \in \mathbb{Z}_3[x]$. If we list the elements of $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right)$, we see that $U_{x^2}\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right) = \{1, x^2+1, 2x^2+1\}$. □

Example 5.4.

Suppose $g(x) = x + 1$, $f(x) = x^2$, and $p = 3$. Then, $U_{x+1}\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) = \left\{h(x) \in U\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) \middle| h(x) = (x+1)\, t(x)+1\,,\ t(x) \in \mathbb{Z}_3[x]\right\}$. We know $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) = \{1, 2, x+1, x+2, 2x+1, 2x+2\}$, which means $U_{x+1}\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) = \{1, 2, x+1, x+2, 2x+1, 2x+2\} = U\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right)$. We get the entire group back, which is in agreement with Theorem 5.8.

Example 5.5.

The group $U\left(\frac{\mathbb{Z}_2[x]}{\langle x^4\rangle}\right) = \{1, x^2+1, x+1, x^2+x+1, x^3+x^2+x+1, x^3+x^2+1, x^3+x+1, x^3+1\}$. The subgroup $U_{x^2}\left(\frac{\mathbb{Z}_2[x]}{\langle x^4\rangle}\right) = \{1, x^2+1, xx^2+1, (x+1)x^2+1\} = \{1, x^2+1, x^3+1, x^3+x^2+1\}$. □

Example 5.6.

The group elements of $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^2(x+1)\rangle}\right) = \{1, 2, x^2+1, 2x^2+2, x^2+x+1, 2x^2+2x+1, x+2, 2x+1, x^2+x+2, 2x^2+x+1, 2x^2+2x+2\}$. One of the subgroups is $U_{x^2}\left(\frac{\mathbb{Z}_3[x]}{\langle x^2(x+1)\rangle}\right) = \{1, x^2+1\}$. To verify closure, note that $(x^2+1)^2 = x^4+2x^2+1 = x^2+2x^2+1 = 1$. □

Recall from [1], if $n = st$ where $\gcd(s,t) = 1$, then $U(st) \approx U(s) \oplus U(t)$ and $U_s(st) \approx U(t)$. Theorem 5.7 is an analog of the result for $U(st)$ where the first statement in Theorem 5.7 follows from Theorem 3.2.

Theorem 5.7. *Let $s(x)$ and $t(x)$ be relatively prime elements of $\mathbb{Z}_p[x]$. Then $U\left(\frac{\mathbb{Z}_p[x]}{\langle s(x)t(x)\rangle}\right) \approx U\left(\frac{\mathbb{Z}_p[x]}{\langle s(x)\rangle}\right) \oplus U\left(\frac{\mathbb{Z}_p[x]}{\langle t(x)\rangle}\right)$. Moreover, $U_{s(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle s(x)t(x)\rangle}\right)$ is isomorphic to $U\left(\frac{\mathbb{Z}_p[x]}{\langle t(x)\rangle}\right)$.*

Proof. Let $s(x)$ and $t(x)$ be relatively prime polynomials in $Z_p[x]$ where the mapping ϕ from $U_{s(x)}(Z_p[x]/\langle s(x)t(x)\rangle)$ to $U(Z_p[x]/\langle t(x)\rangle)$ is defined by $\phi(h(x) + \langle s(x)t(x)\rangle) = h(x) + \langle t(x)\rangle$.

To simplify the notation let $I = \langle s(x)t(x)\rangle$ and $J = \langle t(x)\rangle$. To prove that the mapping is onto it suffices to show that it is one-to-one and $|U_{s(x)}(Z_p[x]/I)| = |U(Z_p[x]/J)|$. It follows from properties of modular arithmetic that the mapping $\phi(h(x)+I) = h(x)+J$ from the ring $Z_p[x]/I$ to $Z_p[x]/J$ is a ring homomorphism. Let the distinct coset representatives of $Z_p[x]/J$ be $t_0(x) = 0, t_1(x), \ldots, t_{n-1}(x)$. In $Z_p[x]/I$ let $S = \{1 + I, s(x)t_1(x) + 1 + I, s(x)t_2(x)+1+I, \ldots, s(x)t_{n-1}(x)+1+I\}$. We claim that restriction of ϕ to S is a one-to-one mapping from the set S to the ring $Z_p[x]/J$. If $s(x)t_i(x) + 1 + J = s(x)t_j(x) + 1 + J$ with deg $t(x) >$ deg $(t_i(x) \geq$ deg $t_j(x) \geq 1$ then $(t_i(x) - t_j(x))s(x) = 0 \bmod t(x)$. This means that $t(x)$ divides $t_i(x) - t_j(x)$ and therefore $t_i(x) = t_j(x)$ (because deg $t(x) >$ deg $(t_i(x) - t_j(x))$). Next observe that every element in S is a unit in $Z_p[x]/I$ or a zero-divisor in $Z_p[x]/I$. Because all elements in S are relatively prime to $s(x)$, if $s(x)t_k(x) + 1 + I$ is a unit in $Z_p[x]/I$ then gcd$(s(x)t_k(x) + 1, t(x)) = 1$ and therefore there is no nonconstant divisor of $t(x)$ that divides $s(x)t_k(x) + 1$. But this means that $s(x)t_k(x)+1$ is relatively prime to $t(x)$ and therefore $s(x)t_k(x)+1+J$ is a unit in $Z_p[x]/J$. Conversely, if $s(x)t_k(x)+1+I$ is a zero-divisor in $Z_p[x]/I$ then the there is some nonconstant divisor $t^{'}(x)$ of $t(x)$ that divides $s(x)t_k(x) + 1$. Then $\phi(\frac{t(x)}{t^{'}(x)}(s(x)t_k(x) + 1 + I)) = t(x)(\frac{s(x)t_k(x)+1}{t^{'}(x)}) + J = 0$ in $Z_p[x]/J$. So, $s(x)t_k(x) + 1 + J$ is a zero-divisor in $Z_p[x]/J$. Thus, because S and $Z_p[x]/J$ both have exactly n elements, we have proved that ϕ maps the units in S onto the units in $Z_p[x]/J$ and the zero-divisors in S onto the zero-divisors in $Z_p[x]/J$ Since the units in $S = U_{s(x)}(Z_p[x]/I)$ and the units in $Z_p[x]/J = U(Z_p[x]/J)$, we have $|Us(x)(Z_p[x]/I)| = |U(Z_p[x]/J|$, as desired.

□

The next theorem shows that without loss of generality, we may assume that for subgroups of the form $U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. We may assume that $g(x)$ is a divisor of $f(x)$.

Theorem 5.8. *If* $g(x), f(x) \in \mathbb{Z}_p[x]$, *then* $U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right) = U_{gcd(g(x),f(x))}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$.

Proof. Following the proof from [2], let $\gcd(g(x), f(x)) = d(x)$, where $g(x) = d(x)h(x)$, and $b(x) \in U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. We want to show $b(x) \in U_{d(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. We know $b(x) = g(x)t(x) + 1 \pmod{f(x)}$, which implies $b(x) = d(x)h(x)t(x) + 1 \bmod f(x)$ and $b(x) \in U_{d(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. Thus $U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right) \subseteq U_{d(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. For $b(x) \in U_{d(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ we have $b(x) = d(x)t_1(x)+1 \pmod{f(x)}$ for some $t[x]$ in $\mathbb{Z}_p[x]$. We know there exists polynomials $s(x)$ and $t_1(x)$ in $\mathbb{Z}_p[x]$ such that $s(x)g(x)+t_1(x)f(x) = d(x)$ since $d(x) = \gcd(f(x), g(x))$. Therefore $b(x) = (s(x)g(x) + t(x)f(x))t_1(x) + 1 = g(x)(s(x)t_1(x)) + 1 \pmod{f(x)}$. So $b(x) \in U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ implying $U_{d(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right) \subseteq U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$. □

The patterns of the examples allows us to determine the order of the subgroups of the form $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$, which we will denote $H_{p,k,t}$. We use $Syl(H_{p,k,t})$ to denote the Sylow p-subgroup of $H_{p,k,t}$ and the rank of $H_{p,k,t}$ by $rk(Syl(H_{p,k,t}))$.

Theorem 5.9. *For prime* p *and* $1 \leq t \leq k$, *we have* $|U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)| = |H_{p,k,t}| = p^{k-t}$.

Proof. Every element in the subgroup $H_{p,k,t}$ has the form $x^t h(x)+1$ such that $h(x) \in \mathbb{Z}_p[x]$ and deg $(x^t h(x) + 1) \leq k - 1$. We know $\deg(x^t h(x) + 1) = \deg(h(x))+ \deg(x^t) \leq k - 1$. So deg $h(x) + t \leq k - 1$ giving deg $h(x) \leq k - t - 1$. Thus $h(x) = c_{k-t-1}x^{k-t-1} + \cdots + c_{m_p}x^{m_p} + \cdots + c_1x + c_0$ implying $\left|U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)\right| = |H_{p,k,t}| = p^{k-t}$. □

Corollary 5.10. *Let* p *be a prime and* $1 \leq t \leq k$. *If* $k \leq p$, *then* $rk(Syl(H_{p,k,t})) = k - t$.

Proof. Suppose $k \leq p$. Every element in $H_{p,k,t}$ has the form $x^t h(x) + 1$ for $h(x) \in \mathbb{Z}_p[x]$. To find the rank, we will determine the number elements of order p. Since $(x^t h(x) + 1)^p = x^{tp}h(x)^p + 1$ and $k \leq p \leq tp$, we have $x^{tp}h(x)^p + 1 = 1$. So every element has order 1 or p in $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$. We know from Theorem 5.9, that $H_{p,k,t}$ has order p^{k-t}, so it follows that $rk(Syl(H_{p,k,t})) = k - t$ and we have $k - t$ copies of $\mathbb{Z}_p$. □

As before, we let m_p be the smallest integer such that $k \leq m_p p$ for $G_{p,k}$.

Corollary 5.11. *If $p < k$ and $t < m_p$, then $rk(Syl(H_{p,k,t})) = k - m_p$. If $p < k$ and $m_p \leq t$, then $rk(Syl(H_{p,k,t})) = k - t$.*

Proof. Suppose $p < k$ and $t < m_p$. So $(x^t h(x)+1)^p = (x^t(c_{k-t-1}x^{k-t-1}+\cdots+c_{m_p}x^{m_p}+\cdots+c_{m_p-t}x^{m_p-t}+\cdots+c_0)+1)^p = ((c_{k-t-1}x^{k-1}+\cdots+c_{m_p}x^{m_p+t}+\cdots+c_{m_p-t}x^{m_p}+\cdots+c_0x^t)+1)^p = ((c_{k-t-1}x^{(k-1)p}+\cdots+c_{m_p}x^{(m_p+t)p}+\cdots+c_{m_p-t}x^{m_pp}+\cdots+c_0x^{tp})+1)$. The last term to be killed off is $c_{m_p-t}x^{m_pp}$. For elements of order p, the coefficients $c_{m_p-t-1} = \cdots = c_0 = 0$. Therefore there are $p^{k-t-1-(m_p-t-1)} - 1 = p^{k-m_p} - 1$ elements of order p and $rk(Syl(H_{p,k,t})) = k - m_p$.

If $p < k$ and $m_p \leq t$, then $(h(x)x^t + 1)^p = 1$ as $k \leq m_pp \leq tp$. So every element in $H_{p,k,t}$ has order 1 or p. Again, $rk(Syl(H_{p,k,t})) = k - t$. □

Corollary 5.12. *If $k \leq p$ or $p < k$ and $m_p \leq t$, then $H_{p,k,t} \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k-t}$*

The rank tells us the number of terms in the isomorphism class for $H_{p,k,t}$. So to determine the structure of $H_{p,k,t}$, it suffices to find the exponent of $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$. As before, let i be the smallest positive integer such that $k \leq p^i$ for $G_{p,k}$.

Theorem 5.13. *For a prime p and integers k and t with $1 \leq t \leq k$, let j be the smallest positive integer such that $k \leq tp^j$. Then p^j is the exponent of $H_{p,k,t}$ where $j = \lceil \log_p k - \log_p t \rceil$.*

Proof. Recall that every element in $H_{p,k,t}$ has the form $x^t h(x) + 1$. Then $(x^t h(x) + 1)^{p^j} = x^{tp^j} h(x)^{p^j} + 1 = x^{tp^j}(c_{k-t-1}x^{(k-t-1)p^j} + \cdots + c_t x^{tp} + \cdots + c_1 x^{p^j} + c_0) + 1 = 1$ and, by definition, j is the smallest such integer. Since $k \leq tp^j$, this means $\frac{k}{t} \leq p^j$ and $\lceil \log_p \frac{k}{t} \rceil \leq \lceil \log_p p^j \rceil = j$. Thus $\lceil \log_p \frac{k}{t} \rceil = \lceil \log_p k - \log_p t \rceil = j$. □

Let's find the isomorphism class for the subgroup $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$ for $p = 3, k = 4$, and $1 \leq t \leq 4$.

Example 5.14.

We will determine isomorphism classes using the cancellation property for $U_{x^t}\left(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\right)$ for $1 \leq t \leq 4$ where $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\right) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$.

$$
\begin{aligned}
t = 1 \qquad & U_x\Big(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\Big) \approx \langle x+1\rangle \times \langle x^2+1\rangle \approx \mathbb{Z}_9 \oplus \mathbb{Z}_3 \approx Syl\Big(U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\Big)\Big) \\
t = 2 \qquad & U_{x^2}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\Big) \approx \langle x^2+1\rangle \times \langle x^3+1\rangle \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx Syl\Big(U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\Big)\Big) \\
t = 3 \qquad & U_{x^3}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\Big) \approx \langle x^3+1\rangle \approx \mathbb{Z}_3 \approx Syl\Big(U\Big(\frac{\mathbb{Z}_3[x]}{\langle x\rangle}\Big)\Big) \\
t = 4 \qquad & U_{x^4}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^4\rangle}\Big) \approx \mathbb{Z}_1 \qquad \square
\end{aligned}
$$

Example 5.15.

$$U\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

$$
\begin{aligned}
t = 1 \qquad & U_x\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \langle x+1\rangle \times \langle x^2+1\rangle \times \langle x^3+1\rangle \times \langle x^4+1\rangle \approx \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 2 \qquad & U_{x^2}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \langle x^2+1\rangle \times \langle x^3+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle \approx \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 3 \qquad & U_{x^3}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \langle x^3+1\rangle \times \langle x^4+1\rangle \times \langle x^5+1\rangle \times \langle x^4+x^3+1\rangle \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 4 \qquad & U_{x^4}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \langle x^4+1\rangle \times \langle x^5+1\rangle \times \langle x^5+x^4+1\rangle \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 5 \qquad & U_{x^5}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \langle x^5+1\rangle \times \langle x^6+1\rangle \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 6 \qquad & U_{x^6}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \langle x^6+1\rangle \approx \mathbb{Z}_3 \\
t = 7 \qquad & U_{x^7}\Big(\frac{\mathbb{Z}_3[x]}{\langle x^7\rangle}\Big) \approx \mathbb{Z}_1
\end{aligned}
$$

Note, when $t = 3$, the rank is $k - t$ since $m_3 = t$ and $|H_{3,7,3}| = 3^{7-3} = 81$. Similarly, when $t = 4$, the rank is $k - t$ since $m_3 < t$ and $|H_{3,7,4}| = 3^{7-4} = 27$. Once the deg $g(x) = t \geq m_p$ for a given p, k, then every element in $H_{p,k,t}$ has order 1 or p. So the order of $H_{p,k,t}$ tells us the rank, which in turn, gives the structure of $H_{p,k,t}$. $\square$

5.1 Algorithm for Internal/External Direct Product for Subgroups of the form $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$

Case 1:

1. If $k \leq p$, then $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right) \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k-t}$.

2. For the internal direct product, fill the first slot of the internal direct product with $\langle x^t+1\rangle$.

3. Fill the remaining slots with $x^i + 1$ for each $i \geq t + 1$. We will allow the first i value such that $p \mid i$, but skip values of i such that $i > p$ and $p \mid i$ for the remainder of the internal direct product.

4. Next, find the order of each term.

5. These orders tell us the isomorphism class.

Case 2 (a)

Let m_p be the smallest positive integer such that $k \leq m_p\, p$.

1. If $p < k$ and $t \geq m_p$, then $H_{p,k,t} \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k\,-\,t}$

2. To find the internal direct product, fill the first slot of the internal direct product with $\langle x^t + 1\rangle$.

3. If $t \mid p$, fill the remaining slots with $x^i + 1$ for each $i \geq t + 1$, skipping values of i such that $i > p$ and $p \mid i$. Continue this process until all slots in the internal direct product are filled.

4. If $t \nmid p$, fill the remaining slots with $x^i + 1$ for each $i \geq t + 1$, including the first i that's a multiple of p and skipping values of i such that $i > p$ and $p \mid i$ for the remainder of the internal direct product.

4. Next, find the order of each term.

5. These orders tell us the isomorphism class.

Case 2 (b)

1. If $p < k$ and $t < m_p$, then the rank is $k - m_p$ where m_p is the smallest positive integer such that $k \leq m_p p$. There are $k - m_p$ terms in the factorization of the external direct prod-

uct.

2. To find the internal direct product, fill the first slot of the internal direct product with $\langle x^t + 1\rangle$. If there are leftover slots, then fill those slots with $\langle x^{i+1} + x^t + 1\rangle$.

3. Follow the same steps as **Case 2 (a)**.

4. Next, find the order of each term.

5. These orders tell us the isomorphism class. □

Theorem 5.16. *For $t \leq k$, we have* $\dfrac{U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)}{U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)} \approx U\left(\frac{\mathbb{Z}_p[x]}{\langle x^t\rangle}\right)$.

Proof. Let ϕ be the group homomorphism from $G = U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$ to $\overline{G} = U\left(\frac{\mathbb{Z}_p[x]}{\langle x^t\rangle}\right)$ defined by $gKer(\phi) \rightarrow \phi(g)$, in the First Isomorphism Theorem in [1]. Since $U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$ is an Abelian group and $U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)$ is a subgroup from Definition **??**, we have $\left|\dfrac{U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)}{U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)}\right| = \dfrac{\left|U\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)\right|}{\left|U_{x^t}\left(\frac{\mathbb{Z}_p[x]}{\langle x^k\rangle}\right)\right|} = \frac{p^{k-1}(p-1)}{p^{k-t}} = p^{t-1}(p-1)$. Note that $\left|U\left(\frac{\mathbb{Z}_p[x]}{\langle x^t\rangle}\right)\right| = p^{t-1}(p-1)$. □

We will give an example to illustrate Theorem 5.16.

Example 5.17.

Suppose $p = 3$, $k = 10$, and $t = 3$. Then the mapping from $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right)$ to $U\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right)$ given by the mapping $\phi : g(x) + \langle x^{10}\rangle \rightarrow g(x) + \langle x^3\rangle$ is a homomorphism. Consider the subgroup $U_{x^3}\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right) = \{g(x) \in U\left(\frac{\mathbb{Z}_p[x]}{\langle x^{10}\rangle}\right) \mid g(x) = h(x)x^3 + 1\}$. Using the First Isomorphism Theorem, we have $\dfrac{U\left(\frac{\mathbb{Z}_p[x]}{\langle x^{10}\rangle}\right)}{U_{x^3}\left(\frac{\mathbb{Z}_p[x]}{\langle x^{10}\rangle}\right)} \approx U\left(\frac{\mathbb{Z}_p[x]}{\langle x^{10}\rangle}\right)$. The reason why the factor group is all of $U\left(\frac{\mathbb{Z}_p[x]}{\langle x^{10}\rangle}\right)$ is $\left|\dfrac{U\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right)}{U_{x^3}\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right)}\right| = \dfrac{\left|U\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right)\right|}{\left|U_{x^3}\left(\frac{\mathbb{Z}_3[x]}{\langle x^{10}\rangle}\right)\right|} = \frac{3^9(3-1)}{3^{10-3}} = 3^2(3-1) = 18$ and $\left|U\left(\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}\right)\right| = 3^2(3-1) = 18$.

Finally, we consider $U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ when $f(x)$ is an irreducible quadratic polynomial over $\mathbb{Z}_p$.

6 $U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ where $f(x)$ is a degree 2 irreducible polynomial

Theorem 6.1. *For prime p and $1 \leq t \leq k$, we have $|U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)| = p^{2k-2t}$*

Proof. We know $U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right) = \{h(x) \in U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right) \mid h(x) = f(x)^t g(x) + 1\}$ where $g(x) \in \mathbb{Z}_p[x]$ and $1 \leq t \leq k$. Similar to the proof for Theorem 5.9, we know deg $h(x) =$ deg $(f(x)^t g(x) + 1) < 2k$. This means deg $g(x) < 2k - 2t$ resulting in p choices for each of the $2k - 2t$ coefficients. Therefore, $|U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)| = p^{2k-2t}$. □

As was with the reducible case, we will simplify the notation by using $H_{p,2k,2t}$ for $U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$ for the subgroup of $G_{p,2k}$. To determine the isomorphism class of $H_{p,2k,2t}$, it's helpful to know the rank.

Corollary 6.2. *Let p be a prime and $1 \leq t \leq k$. If $k \leq p$, then $rk(Syl(H_{p,2k,2t})) = 2k - 2t = 2(k - t)$.*

Proof. Every element in $H_{p,2k,2t}$ has the form $f(x)^t g(x) + 1$ for $g(x) \in \mathbb{Z}_p[x]$. To find the rank, we will determine the number elements of order p. Since $(f(x)^t h(x) + 1)^p = f(x)^{tp} h(x)^p + 1$ and $k \leq p \leq tp$, we have $f(x)^{tp} h(x)^p + 1 = 1$. So every element has order 1 or p in $H_{p,2k,2t}$. We know from Theorem 6.1, that $H_{p,2k,2t}$ has order p^{2k-2t}, so it follows that $rk(Syl(H_{p,2k,2t})) = 2k - 2t$ and we have $2k - 2t$ copies of $\mathbb{Z}_p$. □

As before, we let m_p be the smallest integer such that $k \leq m_p p$ for $G_{p,k}$.

Corollary 6.3. *If $p < k$ and $t < m_p$, then $rk(Syl(H_{p,2k,2t})) = 2k - 2t - m_p$. If $p < k$ and $m_p \leq t$, then $rk(Syl(H_{p,2k,2t})) = 2k - 2t$.*

Proof. Suppose $p < k$ and $t < m_p$. Then $(f(x)^t h(x)+1)^p = f(x)^{tp}h(x)^p+1$ and $f(x)^{tp} \neq 0$ since $tp < m_p p$. But $(f(x)^t h(x)+1)^p = f(x)^{tp}h(x)^p+1 = f(x)^{tp}(c_{2k-2t-1}x^{2k-2t-1} + \cdots + c_{m_p}x^{m_p} + c_{m_p-1}x^{m_p-1} + \cdots + c_1 x + c_0)^p + 1 = f(x)^{tp}(c_{2k-2t-1}x^{(2k-2t-1)p} + \cdots + c_{m_p}x^{m_p p} + c_{m_p-1}x^{(m_p-1)p} + \cdots + c_1 x^p + c_0) + 1$. The last term to be killed off is $c_{m_p}x^{m_p p}$. So, for elements of order p, we have the coefficients $c_{m_p-1} = \cdots = c_0 = 0$. Therefore there are $p^{2k-2t-1-(m_p-1)} - 1 = p^{2k-2t-m_p} - 1$ elements of order p and $rk(Syl(H_{p,k,t})) = 2k - 2t - m_p$.

If $p < k$ and $m_p \leq t$, then $(x^t h(x)+1)^p = 1$ as $k \leq m_p p < tp$. So every element in $H_{p,2k,2t}$ has order 1 or p. Again, $rk(Syl(H_{p,2k,2t})) = 2k - 2t$. □

Corollary 6.4. *If $k \leq p$ or $p < k$ and $m_p \leq t$, then $H_{p,2k,2t} \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{2k-2t}$*

The rank tells us the number of terms in the isomorphism class for $H_{p,2k,2t}$.

Example 6.5.

Let $p = 3$ and $f(x) = x^2 + 1$ where $k = 2$ and $t = 1$. Then every element in $H_{p,2k,2t}$ has the form $(x^2+1)g(x)+1$ for $g(x) \in \mathbb{Z}_p[x]$. Note that $|H_{p,2k,2t}| = p^{2k-2t} = 3^2 = 9$ and $rk(Syl(H_{p,2k,2t})) = 2k-2t = 4-2 = 2$ as $m_3 \leq t$. So $H_{3,8,2} \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3$. □

Example 6.6.

Let $p = 3$ and $f(x) = x^2 + 1$ where $k = 4$ and $1 \leq t \leq 4$. The isomorphism class for $U\left(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4 \rangle}\right) \approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

$$
\begin{aligned}
t = 1 \qquad & U_{x^2+1}\left(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4 \rangle}\right) \approx \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 2 \qquad & U_{(x^2+1)^2}\left(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4 \rangle}\right) \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 3 \qquad & U_{(x^2+1)^3}\left(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4 \rangle}\right) \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
t = 4 \qquad & U_{(x^2+1)^4}\left(\frac{\mathbb{Z}_3[x]}{\langle (x^2+1)^4 \rangle}\right) \approx \mathbb{Z}_1
\end{aligned}
$$
□

Next, we show the algorithm for finding the structure of the subgroups of $H_{p,2k,2t}$.

Algorithm for Internal/External Direct Product of Subgroups of the form $U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right)$

Case 1:

1. If $k \leq p$, then $U_{f(x)^t}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)^k\rangle}\right) \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{2k-2t}$.

2. For the internal direct product, fill the first and second slot of the internal direct product with $\langle f(x)^t + 1\rangle$ and $\langle f(x)^t x + 1\rangle$.

3. Fill the remaining pair of slots with $\langle f(x)^i + 1\rangle$ and $\langle f(x)^i x + 1\rangle$ for each $i \geq t+1$. We will allow the first i value such that $p \mid i$, but skip values of i such that $i > p$ and $p \mid i$ for the remainder of the internal direct product. If there are leftover slots, then fill those slots with $\langle f(x)^i + f(x)^t + 1\rangle$ and $\langle f(x)^i x + f(x)^t x + 1\rangle$.

4. Next, find the order of each term.

5. These orders tell us the isomorphism class.

Case 2 (a)

Let m_p be the smallest positive integer such that $k \leq m_p\, p$.

1. If $p < k$ and $t \geq m_p$, then $H_{p,2k,2t} \approx \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k-t}$

2. To find the internal direct product, follow the steps from **Case 1**.

Case 2 (b)

1. If $p < k$ and $t < m_p$, then the rank is $2k - 2t - m_p$ where m_p is the smallest positive integer such that $k \leq m_p p$. There are $2k-2t-m_p$ terms in the factorization of the external direct product.

2. To find the internal direct product, fill the first and second slot of the internal direct product with $\langle f(x)^t + 1\rangle$ and $\langle f(x)^t x + 1\rangle$.

3. Fill the remaining pair of slots with $\langle f(x)^i + 1\rangle$ and $\langle f(x)^i x + 1\rangle$ for each $i \geq t+1$. We will allow the first i value such that $p \mid i$, but skip values of i such that $i > p$ and $p \mid i$ for the remainder of the internal direct product. If there are leftover slots, then fill those slots

with $\langle f(x)^i + f(x)^t + 1\rangle$ and $\langle f(x)^i x + f(x)^t x + 1\rangle$.

4. Next, find the order of each term.

5. These orders tell us the isomorphism class. □

7 Summary

We have focused on the groups $U\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$ for the cases that $f(x)$ has small degree so could compute the internal direct products as well as the external direct products. In fact our methods for the external direct product apply to $U\left(\frac{\mathbb{Z}_q[x]}{\langle f(x)\rangle}\right)$, where q is any power of a prime and $f(x)$ is any polynomial in $\mathbb{Z}_q[x]$.

We have also determined the structure for the subgroups $U_{g(x)}\left(\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}\right)$.

8 References

[1] Joseph A. Gallian, "Contemporary Abstract Algebra," Ninth Edition, Cengage Learning Boston, 2017.

[2] Joseph A. Gallian and Shahriyar Roshan Zamir, Subgroups of groups of units modulo n, *Mathematics Magazine* (2020), to appear.

[3] Joseph A. Gallian and D. Rusin, Factoring groups of integers modulo n, *Mathematics Magazine* 53 (1980), 33-36.

[4] https://en.wikipedia.org/wiki/Chinese_remainder_theorem