Abstract Algebra Project

1 Background

For our project we, Noah Wong and Hongru Zhao, created a Mathematica code for Professor Joe Gallian and Karlee Westrem's research on factor groups of polynomials. Karlee Westrem is a fellow master's graduate student at University of Minnesota Duluth working on her master's thesis with Professor Gallian in the field of abstract algebra. Gallian had hired another student, Jiangyi Qui, to create a calculator to assist with their research in the summer of 2019. That program had two versions and was written in javascript. The versions can be found (http://www.d.umn.edu/~jgallian/polycalcNew/poly.html) and (http://www.d.umn.edu/~jgallian/polycalc/poly.html). These work on any internet browser, test them out if they are still up. However the online calculators had problems scaling when the polynomials that were tested became too big. So Joe and Karlee asked us to recreate the calculator but with the capability to solve bigger problems.

2 Code

The program was written in Wolfram Mathematica 11.0. We used mathematica because of the functions that came with mathematica dealing with division and modulo of polynomials. There are instructions written above each part of the calculator with clear indications of what inputs you can change. You must run the first section of 'Input', 'Functions' and 'Code' before you can use the two preceding sections. Depending on the size of k, p and the degree of $p_0(x)$ the program may have to run for hours to compute the first section.

3 Mathematics

Knowledge of factor rings, polynomial rings and elementary abstract algebra is needed to understand the mathematics. The research is on finite polynomials groups. I would recommend reading Chapters 12-14, 16 and 17 in Joe Gallian's book "Contemporary Abstract Algebra" for more on the mathematics involved. All definitions and notation used below are pulled from that book.

A polynomial ring contains a set of functions, in particular polynomials along with two operations addition and multiplication. The research deals with a particular ring of polynomials that is finite. However the generic polynomial rings are infinite, so we must construct the structure of this particular finite ring. We start with the generic infinite polynomial ring defined as

$$Z_p[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 | a_i \in Z_p\}$$

where p is a prime number and Z_p is the cyclic group of order p. Z_p contains the elements $\{0, 1, \ldots p-1\}$, so the coefficients of polynomials in $Z_p[x]$ can only

be $\{0, 1, \ldots p-1\}$. Chapter 17 of Joe's book goes into more detail as to why p is chosen to be prime. Pulling the coefficients from Z_p reduces how many polynomials in our ring, still $Z_p[x]$ is an infinite ring since the polynomials can have any degree, so there are an infinite number of possible polynomials available. To create a finite ring we first need to define a principal ideal for a polynomial $p_0(x)$ in our ring $Z_p[x]$,

$$\langle p_0(x)\rangle = \{f(x)p_0(x)|f(x) \in Z_p[x]\}.$$

A principal ideal for any $p_0(x)$ is a infinite subring $Z_p[x]$. The finite group Karlee and Joe are exploring is a finite ring based off the infinite ring $Z_p[x]$, called factor ring. For a given $p_0(x) \in Z_p[x]$ the factor ring is defined as

$$Z_p[x]/\langle p_0(x)\rangle = \{g(x) + \langle p_0(x)\rangle|g(x) \in Z_p[x]\}.$$

Let m denote the degree of $p_0(x)$, then for a polynomial $g(x) \in Z_p[x]/\langle p_0(x)\rangle$, the division algorithm says we can rewrite $g(x) = q(x)p_0(x) + r(x)$, with the degree of $r(x)$ to be less than m. The ideal $\langle p_0(x)\rangle$ will 'absorb' the term $q(x)p_0(x)$, since by definition $q(x)p_0(x) \in \langle p_0(x)\rangle$ so

$$g(x) + \langle p_0(x)\rangle = q(x)p_0(x) + r(x) + \langle p_0(x)\rangle = r(x) + \langle p_0(x)\rangle$$

Thus all nonzero elements in $Z_p[x]/\langle p_0(x)\rangle$ have degree less than m. This restriction on degree results in a finite ring. So this factor ring has finite order. The next step is finding a group inside this subring. The operation addition with $Z_p[x]/\langle p_0(x)\rangle$ is a group. The project involves the operation multiplication with $Z_p[x]/\langle p_0(x)\rangle$, however for most choices of $p_0(x)$ the factor ring is not a field, so multiplication with $Z_p[x]/\langle p_0(x)\rangle$ is not a group. This is because there are polynomials with no multiplicative inverse. These elements are called zero-divisors. An element $g(x) \in Z_p[x]/\langle p_0(x)\rangle$ is a zero-divisor if there exists a $h(x) \in Z_p[x]/\langle p_0(x)\rangle$ such that $g(x)h(x) = 0 + \langle p_0(x)\rangle$. If we remove this zero-divisors than $Z_p[x]/\langle p_0(x)\rangle$ will be a group under multiplication. We call this the 'U-group' and define it as

$$U\left(\frac{Z_p[x]}{\langle p_0(x)\rangle}\right) = \{g(x) \in Z_p[x]/\langle p_0(x)\rangle \mid g(x) \text{ is not a zero-divisor of } Z_p[x]/\langle p_0(x)\rangle\}.$$

These are the groups that are being investigated. Part of this research involves determining the structure of these groups given a particular prime p and polynomial $p_0(x)$. The calculator I helped create takes a p and $p_0(x)$ and an exponent k and calculates the orders of the elements of $U\left(\frac{Z_p[x]}{\langle p_0(x)^k\rangle}\right)$. It first finds all possible polynomials in the group by finding and throwing out any zero-divisors, then it finds the order of each remaining one. It then returns a list of all possible orders and how many polynomials have each order. Also you can type in a particular polynomial you wish to find it's order and it will return it. Lastly, given a particular order, say 12, you can type 12 into the calculator and it will return the first 50 polynomials that have order 12. The number of polynomials

returned can be changed as well if you wanted the first 100 polynomials with order 12.

The calculator scales well. The modest choice of $p_0(x) = x^2 + 1$, $p = 3$ and $k = 4$ has $6,561$ polynomials to test, the calculator has to calculate a lot. We were able to test large groups including $p = 13$, $p_0 = (x^2 + 2x + 3)^4$ which tests $13^8 = 815,730,721$ polynomials and return correct results.

4 Contact

If you have any questions on the program or the mathematics behind it you can contact us,
Noah Wong, wongx565@d.umn.edu
Hongru Zhao, zhao1118@d.umn.edu
When Karlee finishes her paper on the research it will be attached below as well.