Abstract Algebra Project

1 Background

Created a mathematica code with Hongru Zhao for Joe Gallian and Karlee Westrem's research on factor groups of polynomials. Karlee Westrem is a fellow masters graduate student at Duluth working on her master's thesis with Professor Gallian in the field of abstract algebra. Gallian had hired another student 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 programs were written by Jiangyi Qui and work on any internet browser. However the online calculators had problems scaling when the polynomials that were tested became too big. So Joe and Karlee asked Hongru Zhao, another masters grad student, and I 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 groups, polynomial rings and elementary abstract algebra is need to understand the mathematics. The research is on finite polynomials groups. I would reccomend reading Chapters 12-14, 16 and 17 in Joe Gallian's book "Contemporary Abstract Algebra".

A polynomial ring contains a set of functions, in particular polynomials. The two operations on these polynomials is addition and multiplication. The research deals with a particular ring of polynomials that is finite. We define

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

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 $Z_p[x]$ come 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. However $Z_p[x]$ is an infinite ring since 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 $Z_p[x]$,

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

Now the finite group Karlee and Joe are exploring are finite subring of 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 $q(x)p_0(x)$ 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 elements in $Z_p[x]/\langle p_0(x)\rangle$ have degree less than m. So this subring has finite order. Next we want to reduce this ring to a group by just looking at the operation multiplication, however for most choices of $p_0(x)$ the factor ring is not a field, so there are elements without inverses. These elements are called zero divisors, $g(x) \in Z_p[x]/\langle p_0(x)\rangle$ is a zero-divisor if there exists a $h(x) \in Z_p[x]/\langle p_0(x)\rangle$ such that $g(x)h(x) \equiv 0 + Z_p[x]/\langle p_0(x)\rangle$. 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 researched. Part of this research involves determining the structure of these groups given a particular p and $p_0(x)$. 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 throwing out any zero-divisors, then it tests individual polynomials and finds the order of each 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 the order and it will return it. Lastly, given a certain order, say 12, you can type 12 into the calculator and it will return the first 50 polynomials that have order 12.

The calculator scales well. Given a 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 me, Noah Wong, at wongx565@d.umn.edu! When Karlee finishes her paper on the research I'll attach it below as well.