1. Introduction

This semester I was continuing my work on the matrix group $GL(N, Z/p)$ and applied what I'd learned to the tribonnaci series.

At the end of spring semester, I'd read up in detail on the Crystallographic Restriction and modular arithmetic. I used this to find all the possible non-infinite orders of matrices with positive integer entries, before moving on to $GL(N, Z/p)$. (Recall that $GL(N, Z/p)$ is the group (for prime p) of all $N \times N$ matrices with entries in Z mod p.) I thought I could find a way to describe all the orders of $GL(N, Z/p)$ by connecting it to the set of matrices with positive integer entries by using the symmetric group S_n, but this approach didn't yield very impressive results.

There's a more pragmatic way to think of the problem, however. I observed that, for some N and p, there might be hundreds of different orders, but that most of these orders could be deduced from a few core orders. An order r is a core order if, for all $n \in N$ and $n > 1$, nr is not an order of $GL(N, Z/p)$.

To find all the orders of $GL(N, Z/p)$ from just the core orders, define the set R with $r \in R$ if r is a core order. Then, for every r, define a set D with $d \in D$ iff r/d is an integer. Then all integers of the form r/d are also orders of matrices in $GL(N, Z/p)$

The reasoning behind this is very simple. If A has order r, then A^2 has order $r/2$, A^3 has order $r/3$, and so on. This simplifies the problem of finding orders of elements of $GL(N, Z/p)$ significantly.

I also began working with the tribonnaci series this semester. The tribonnaci series is, like the name suggests, similar to the fibonnaci series. Instead of adding up the last two elements of a series to get the next, however, you add up the last three. In particular, I was interested in orders of the tribonnaci series under modular arithmetic.

2. GL(N,Z/p)

I made some progress on finding a theoretical description of orders of elements $GL(N, Z/p)$ this summer. The first thing I did was to simplify my table of known orders to include only core orders.

N	P	Orders
3	2	7, 4, 3
3	3	26, 8, 6
3	5	124, 24, 20
3	7	342, 48, 42, 28
4	2	15, 7, 6, 4
4	3	80, 26, 24, 18
4	5	624, 124, 20
4	7	2400, 342, 336
5	2	31, 21, 15, 14, 12, 8
5	3	242, 104, 80, 78, 24, 18
5	5	3124, 744, 624, 620

From here I could make a few observations. The highest possible order of an element of $GL(N, Z/p)$ seemed to be $p^N - 1$. (Note that, by definition, the highest order of $GL(N, Z/p)$ has to be a core order.) The order $p^{N-1} - 1$ was also always present.

I set about trying to prove that $p^N - 1$ was the highest possible order. My first idea was that there was some matrix with order $p^N - 1$ for a small N, and that as N increased, new matrices with order $p^N - 1$ could be formed from the old one by simply adding a new first row and column. This idea quickly fell through, however, when I thought about what it would mean for companion matrices.

If you wanted to construct an $N + 1 \times N + 1$ companion matrix from an $N \times N$ companion matrix by adding a new row and column, the old companion matrix would have to fit into the bottom right corner of your new companion matrix. This would mean that the top row of the $N+1 \times N+1$ companion matrix would have to have a non-zero entry in its top right corner. This in turn meant that if you could construct matrices of order $p^N - 1$ by adding a row and a column to a different matrix, then the right column of every companion matrix of order $p^N - 1$ would have no zeroes, only non-zero entries. I knew that companion matrices of order $p^N - 1$ did *not* have no non-zero entries in their rightmost column, so this idea couldn't be correct.

After that, I thought that maybe there would only be one, or at least not very many, matrices with order $p^N - 1$, and that the form these matrices or their characteristic polynomials would take would make it clear why their order was $p^N - 1$, or at least why these matrices had higher order than others. This made me think that one possibility was that matrices with order $p^N - 1$ would have the rightmost column of their associated companion matrix filled with large numbers, or would have evenly spaced zeroes, or some other relatively simple visual cue. (Recall that any matrix has an analagous companion matrix with the same order.)

With this in mind, I wrote a simple program that, for any N and p, would return all matrices that had order $p^N - 1$. It seemed that my hopes for a simple visual cue were unfounded, however, as there were many matrices that had order $p^N - 1$, and they didn't seem similar to each other.

Still, I wasn't exactly expecting an answer to appear as easily as that. I wrote another program that would take the matrices my first program found and multiply them by themselves, and would check to see if the matrices diagonalized before they became the identity, but this idea also fell through.

At this point I wasn't getting anywhere, so I went back and re-read some of the papers I'd researched in the spring. The approaches used in finding the Crystallographic Restriction made me think that perhaps the solution didn't lie in fiddling with matrices but in finding an algebraic solution using characteristic polynomials.

I wrote a program that would take any polynomial $P(x)$ and find the smallest d such that $P(x)$ divided $x^d - 1$. If there was such a d, the program would also return a second polynomial, $P'(x)$, with $P(x)P'(x) = x^d - 1$. (Recall that if a companion matrix has finite order r, then its characteristic equation will divide $x^d - 1$ if $d = r$ and for no smaller d.)

This led to some interesting results when I plugged in characteristic polynomials of matrices with order $p^N - 1$ as $P(x)$. The resulting $P'(x)$ had an pattern: $P'(x)$ would be divided into $p - 1$ subpolynomials of equal length, separated by $N - 1$ zeroes.

A few definitions are needed. When I refer to the 'length' of a polynomial, I mean the difference between the highest and the lowest power of x contained in said polynomial. Also, I will denote each subpolynomial $S_i(x)$, with $S_1(x)$ having the highest degree.

The length L of these subpolynomials can be found by solving a simple algebraic equation. Since $P(x)P'(x) = x^d - 1 = p^N - 1$ and there are $p-1$ subpolynomials separated by $N-1$ zeroes, you can write $(N-1)(p-2)+(p-1)L+(N-1) = p^N - 1$ and solve for $L = p^{N-1} + p^{N-2} + ... + p^2 + p + 1 - (N-1)$.

Another interesting aspect was that the coefficients of each subpolynomial $S_i(x)$ could be found recursively from the subpolynomial preceding it. If we denote $C_i(j)$ as the jth coefficient of the $S_i(X)$ polynomial, we can write $C_i(j) = 2 * C_{i-1}(j)$.

This reveals an interesting factorization of $P'(x)$. If we define $L(x)$ to be $S_1(x)$ divided by the smallest power of x so that $L(x)$ becomes a polynomial of degree $L-1$, then

$$P'(x) = L(x)(x^{d-[(L-1)+N]} + 2x^{d-2[(L-1)+N]} + 4x^{d-3[(L-1)+N]} + ...$$

This is an interesting result, but I haven't had time to properly understand it yet, and so have unfortunately not yet been able to prove why $p^N - 1$ is the largest order of $GL(N, Z/p)$. Still, I wasn't only working on $GL(N, Z/p)$ this semester but also on the tribonnaci series.

3. Tribonnaci Series

The reason I also worked on the tribonnaci series was because it was tied to my work with $GL(N, Z/p)$. The tribonnaci series can be modeled with matrices.

$\{a_i\}$ is a tribonacci series if $a_{i+3} = a_{i+2} + a_{i+1} + a_i$. If you take any three elements a_i, a_{i+1}, a_{i+2} and turn them into a 3×1 matrix, then you can write

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_i \\ a_{i+1} \\ a_{i+2} \end{bmatrix} = \begin{bmatrix} a_{i+1} \\ a_{i+2} \\ a_i + a_{i+1} + a_{i+2} \end{bmatrix} = \begin{bmatrix} a_{i+1} \\ a_{i+2} \\ a_{i+3} \end{bmatrix}$$

As you can see, this first matrix, which I will denote T', can recreate any tribonacci series. What makes T' particularly useful, however, is it's application in modular arithmetic. All integer tribonacci series have a finite order under modular arithmetic, but these orders can get difficult to compute. If you know a theoretical description of the orders of T' under modular arithmetic mod p, however, you will know at least some of the possible orders of tribonacci series mod p.

I didn't work with the T' matrix so much as I did its transpose, which I called the T matrix:

$$T = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

The reason I worked with T rather than T' is that T is a companion matrix, which I'd had experience with already, and the two matrices had the same order.

The first thing I did was write a program that computed the orders of the T matrix mod p. After making a list of orders, two things became apparent that simplified the problem of computing orders of T immensely.

Below, $ord(T_p)$ denotes the order of a tribonacci matrix under mod p, $T^{ord(T_p)} =$ Id mod p.

Theorem 1. *If $m = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$, then $ord(T_m) = LCM(ord(T_{p_1^{r_1}}), ..., ord(T_{p_k^{r_k}}))$.*

Proof. The identity mod m is a matrix

$$A = p_1^{r_1} p_2^{r_2} ... p_k^{r_k} * \begin{bmatrix} n_1 & n_2 & n_3 \\ n_4 & n_5 & n_6 \\ n_7 & n_8 & n_9 \end{bmatrix} + Id.$$

But we also know that, for $1 \leq q \leq k$,

$$T^{n*ord(T_{p_q^{r_q}})} = p_q^{r_q} \begin{bmatrix} n_1 & n_2 & n_3 \\ n_4 & n_5 & n_6 \\ n_7 & n_8 & n_9 \end{bmatrix} + Id.$$

Then, $T^{LCM(ord(T_{p_1^{r_1}}), ord(T_{p_2^{r_2}}))} = p_1^{r_1} p_2^{r_2} \begin{bmatrix} n_1 & n_2 & n_3 \\ n_4 & n_5 & n_6 \\ n_7 & n_8 & n_9 \end{bmatrix}$ + Id.

Furthermore, $T^{LCM(ord(T_{p_1^{r_1}}), ..., ord(T_{p_n^{r_n}}))} = p_1^{r_1} p_2^{r_2} ... p_n^{r_n} \begin{bmatrix} n_1 & n_2 & n_3 \\ n_4 & n_5 & n_6 \\ n_7 & n_8 & n_9 \end{bmatrix}$ + Id.

And $ord(T_m) = LCM(ord(T_{p_1^{r_1}}), ..., ord(T_{p_n^{r_n}}))$. This is what we needed to show.

Theorem 2. *$ord(T_{p^k}) = p^{k-1} ord(T_p)$.*

Proof. To prove this, we have to show that $ord(T_{p^k}) = p * ord(T_{p^{k-1}})$. Let

$$A = T^{ord(T_{p^{k-1}})} = \begin{bmatrix} n_1 p^{k-1} + 1 & n_2 p^{k-1} & n_3 p^{k-1} \\ n_4 p^{k-1} & n_5 p^{k-1} + 1 & n_6 p^{k-1} \\ n_7 p^{k-1} & n_8 p^{k-1} & n_9 p^{k-1} + 1 \end{bmatrix}$$

which is congruent to the identity mod p^{k-1} for $n_1, ..., n_9 < p$.
Then

$$T^{p*ord(T_{p^{k-1}})} = A^p$$

.

Define matrices

$$N = \begin{bmatrix} n_1 & n_2 & n_3 \\ n_4 & n_5 & n_6 \\ n_7 & n_8 & n_9 \end{bmatrix}$$

and

$$N^2 = \begin{bmatrix} n_1^2 + n_2 n_4 + n_3 n_7 & n_1 n_2 + n_2 n_5 + n_3 n_8 & n_1 n_3 + n_2 n_6 + n_3 n_9 \\ n_4 n_1 + n_5 n_4 + n_6 n_7 & n_2 n_4 + n_5^2 + n_6 n_8 & n_3 n_4 + n_6 n_5 + n_9 n_6 \\ n_1 n_7 + n_4 n_8 + n_7 n_9 & n_2 n_7 + n_5 n_8 + n_8 n_9 & n_3 n_7 + n_6 n_8 + n_9^2 \end{bmatrix}$$

letting N_{ij}^2 denote the element of N^2 that is on the ith row and jth column. Then

$$A^2 = \begin{bmatrix} N_{11}^2p^{2k-2} + 2n_1p^{k-1} + 1 & N_{12}^2p^{2k-2} + 2n_2p^{k-1} & N_{13}^2p^{2k-2} + 2n_3p^{k-1} \\ N_{21}^2p^{2k-2} + 2n_4p^{k-1} & N_{22}^2p^{2k-2} + 2n_5p^{k-1} + 1 & N_{23}^2p^{2k-2} + 2n_6p^{k-1} \\ N_{31}^2p^{2k-2} + 2n_7p^{k-1} & N_{32}^2p^{2k-2} + 2n_8p^{k-1} & N_{33}^2p^{2k-2} + 2n_9p^{k-1} + 1 \end{bmatrix}$$

Which is $2 * \begin{bmatrix} n_1p^{k-1} & n_2p^{k-1} & n_3p^{k-1} \\ n_4p^{k-1} & n_5p^{k-1} & n_6p^{k-1} \\ n_7p^{k-1} & n_8p^{k-1} & n_9p^{k-1} \end{bmatrix} + \text{Id}$, mod p^k (for $k > 2$).

In fact, $A^n = n * \begin{bmatrix} n_1p^{k-1} & n_2p^{k-1} & n_3p^{k-1} \\ n_4p^{k-1} & n_5p^{k-1} & n_6p^{k-1} \\ n_7p^{k-1} & n_8p^{k-1} & n_9p^{k-1} \end{bmatrix} + \text{Id}$, mod p^k.

This means that A^p is the identity mod p^k. This is what we needed to show.

Together, these two theorems simplify the problem of finding the orders of T mod p for any p to finding the orders of T mod p for only prime p. I modified my program to only show orders of T for prime p, with the results below:

P	Orders
2	4
3	13
5	31
7	48
11	110
13	168
17	96
19	360
23	553
29	140
31	331
37	467
41	560
43	308
47	46

These results seemed a bit confusing. In particular, I wasn't sure why the orders decreased, sometimes by a very large amount. Still, I had an idea on why this might be the case.

Because of the way that the T matrix is constructed, when you multiply T by itself each row acts as a tribonnaci series. So, for example, in T the first row is $\begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$, in T^2 the first row is $\begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$, in T^3 the first row is $\begin{bmatrix} 1 & 1 & 2 \end{bmatrix}$, and so on.

I thought that each row of the T matrix might have a sub-order different from the order of the T matrix. A definition is needed; if T_i^n denotes the ith row of the T^n matrix, and Id_i denotes the ith row of the identity matrix, then the sub-order of the T_i is the smallest k with $T_i^k = Id_i$. If the sub order of each row was different, then the order of T would be the LCM of the sub-orders of its rows, which I thought might result in the strange behavior I saw.

So I wrote another program that calculated the order of the T matrix in a new way; it would treat each row of the T matrix as a tribonnaci series and would display the sub-order of each row before taking their LCM and spitting out the order of T. I was surprised, however, to find that the order of the matrix was also the sub-order of every single row.

After some more thought, however, the reasoning for this became clear. Each row could be expressed as a combination of the other two. Using the same notation as before, we can write $T_3^n = T_1^{n+1}$ and $T_2^n = T_1^n + T_1^{n-1}$.

Now suppose

$$T_1^m = \left[\begin{array}{ccc} 1 & 0 & 0 \end{array} \right] = Id_1.$$

Then

$$T_3^m = T_1^{m+1} = \left[\begin{array}{ccc} 0 & 0 & 1 \end{array} \right] = Id_3,$$

and

$$T_2^m = T_1^m - T_1^{m-1} = \left[\begin{array}{ccc} 1 & 0 & 0 \end{array} \right] + \left[\begin{array}{ccc} (p-1) & 1 & 0 \end{array} \right] = \left[\begin{array}{ccc} 0 & 1 & 0 \end{array} \right] = Id_2.$$

As you can see, as soon as one row of T equals its counterpart in the identity matrix, so will the other two.

This approach may not have revealed how to compute the orders of T, but it did simplify the problem even further. Since I now knew that the sub-order of each row was identical to the order of T, and that each row acted as a tribonnaci series, my programs only had to compute the orders of the tribonnaci series 0 0 1 mod p instead of computing the order of the matrix T mod p.

Finally, I also applied the program I'd written in section 2. that found the smallest d such that a polynomial $P(x)$ divided $x^d - 1$ to the characteristic polynomial of the T matrix.

The result was interesting. If you write the polynomial $P'(x)$ returned by the program as $n_1 x^{d-3} + n_2 x^{d-4} + \ldots$, then $n_1 = 1$ and $n_m = n_{m-3} + n_{m-2} + n_{m-1}$ mod p. It was the tribonnaci series reappearing as coefficients in a polynomial. This polynomial with tribonnaci series coefficients would continue until the last three coefficients became 0, $p-1$, and 1. Unfortunately, this wasn't too useful, since if you wanted to find the order of the T matrix by finding how long this multiplied polynomial was, you'd still have to find the order of a tribonnaci series, which is what I'd already simplified the problem to.

4. Conclusion.

During the past semester, I've made progress and found interesting results on both my old problem of computing orders of $GL(N, Z/p)$ and the new one of computing orders of the T matrix and, eventually, tribonacci series. I've found that the maximum order of an element $GL(N, Z/p)$ is $p^N - 1$, as well as finding an interesting and, I believe, eventually useful factorization for the polynomial $P'(x)$. I've also reduced the problem of computing orders of T mod p to computing orders of T mod p for prime p, as well as simplifying the necessary computations in finding the order of T.