Introduction
Specific Examples
Linear Transformations
Counting Cycles
Extensions

Fractional Linear Functions

Anna Deng, Maggie Liang, Maggie Shen, Minerva You, Lisa Zheng

PROMYS

Summer 2024

Table of contents

1 Introduction

2 Specific Examples

3 Linear Transformations

4 Counting Cycles

5 Extensions

Fractional Linear Function

A **fractional linear function** (FLF) is a function f of the form

$$f(x) = \frac{ax+b}{cx+d}, \ (ad - bc \neq 0).$$

We will mostly focus on FLFs defined over $\mathbb{P}_p$.

Motivations for ∞

For example, we may try to define a fractional linear function f on $\mathbb{Z}_7$ by the expression

$$f(x) = \frac{2x+1}{x+1}.$$

But what happens when we try to evaluate $f(6) = f(-1)$? We can't divide by 0. So let's "invent" a new symbol, ∞, such that $f(-1) = \infty$.

Plugging in ∞ to f gives $\frac{2\infty+1}{\infty+1}$. If we treat ∞ as a very large value compared to 1, $f(\infty) = 2$.

Defining $\mathbb{P}_p$

Let p be a prime in $\mathbb{N}$. Then

$$\mathbb{P}_p := \mathbb{Z}_p \cup \{\infty\}.$$

what is so cool about P_p? Since p is prime, every element in the domain has an inverse, which is important for some properties we're using later.

Defining Usages of ∞

For an FLF in the form $f(x) = \frac{ax+b}{cx+d}$, if $cx + d = 0$, then $f(x) = \infty$. Meanwhile, $f(\infty) = \frac{a}{c}$.
Specifically for $\mathbb{P}_p$, $f(x) = \infty$ when $x \equiv dc^{-1} \pmod{p}$ and $f(\infty) = ac^{-1}$, where c^{-1} is the modular inverse of c in mod p. Note that because p is prime, if $c \neq 0$, $(c, p) = 1$, so the inverse of c exists.

Orbit Diagrams

For $f(x) = \frac{2x+1}{x+1}$ on $\mathbb{P}_7$, we can draw the following diagrams:

$$\begin{tikzcd} 0 \arrow[r] & 1 \arrow[d] & 2 \arrow[r] & 4 \arrow[d] \\ 5 \arrow[u] & 3 \arrow[l] & \infty \arrow[u] & 6 \arrow[l] \end{tikzcd}$$

Looping Functions

Definition 1: Looping Function and Order

A looping function f is a function such that there exists some $n \in \mathbb{N}$ such that $f^n(x) = x$. We will define n to be the order of such a looping function.

Theorem 1: Loop Lengths

If f has loop n then all possible loop lengths are divisors of n.

Looping Function: $\frac{x-1}{x+1}$

We claim that $\frac{x-1}{x+1}$ is a looping function. Let $f(x) = \frac{x-1}{x+1}$. Then $f(f(x)) = \frac{\frac{x-1}{x+1}-1}{\frac{x-1}{x+1}+1} = \frac{x-1-x-1}{x-1+x+1} = \frac{-2}{2x} = -x$. So $f(f(f(x))) = -\frac{x-1}{x+1}$. Then $f^4(x) = -\frac{\frac{x-1}{x+1}-1}{\frac{x-1}{x+1}+1} = x$. So f has an order of 4.

Thus f may "loop" back to itself after 4 times, 2 times, or 1 time. Note that if f looped back to itself in 2 times, then $x = f^2(x)$, meaning that $x = -x$. This may only happen if $x = 0$, but because $f(f(x)) = f(-1) = \infty \neq 0$, a loop of length 2 is not possible. Furthermore, if $x = \frac{x-1}{x+1}$, then $x^2 + x = x - 1$, so $x^2 + 1 = 0$ in $\mathbb{P}_p$.

Examining $f(x) = \frac{x-1}{x+1}$ in $\mathbb{P}_{11}$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 10 & & 2 & \longrightarrow & 4 & & 3 & \longrightarrow & 6 \\
\uparrow & & \downarrow & & \uparrow & & \downarrow & & \uparrow & & \downarrow \\
1 & \longleftarrow & \infty & & 8 & \longleftarrow & 5 & & 9 & \longleftarrow & 7
\end{array}$$

-1 is not a quadratic residue in $p = 4k + 3$, so there are no loops of length 1. So, all the loops have length 4 when $p = 4k + 3$, and there are $p + 1 = 4k + 4$ different elements of $\mathbb{P}_p$. So there are $\frac{4k+4}{4} = k + 1$ loops when $p = 4k + 3$.

Examining $f(x) = \frac{x-1}{x+1}$ in $\mathbb{P}_{13}$

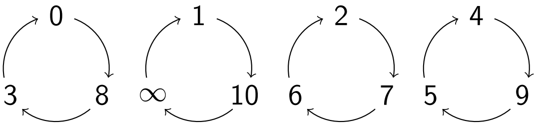
$$\begin{tikzcd}
0 \arrow[r] & 12 \arrow[d] & 2 \arrow[r] & 9 \arrow[d] & 3 \arrow[r] & 7 \arrow[d] & & \\
1 \arrow[u] & \infty \arrow[l] & 10 \arrow[u] & 6 \arrow[l] & 11 \arrow[u] & 4 \arrow[l] & 5 & 8
\end{tikzcd}$$

-1 is a quadratic residue in $p = 4k + 1$, so there are two loops of length 1 as there are two solutions to $x^2 + 1 = 0$ in $\mathbb{P}_p$. So, all the other loops have length 4 when $p = 4k + 1$, and there are $p + 1 = 4k + 2$ different elements of $\mathbb{P}_p$, so there are $\frac{4k+2-2}{4} = k$ loops of length 4.

Looping Function: $\frac{x-3}{x+1}$

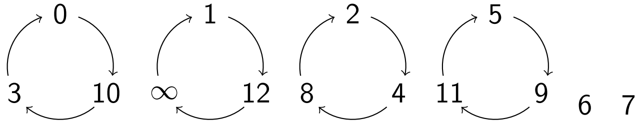
$\frac{x-3}{x+1}$ is also a looping function. Let $f(x) = \frac{x-3}{x+1}$. Then $f(f(x)) = \frac{\frac{x-3}{x+1}-3}{\frac{x-3}{x+1}+1} = \frac{x-3-3x-3}{x-3+x+1} = \frac{-2x-6}{2x-2} = \frac{-x-3}{x-1}$. So $f(f(f(x))) = \frac{-\frac{x-3}{x+1}-3}{\frac{x-3}{x+1}-1} = \frac{-x+3-3x-3}{x-3-x-1} = \frac{-4x}{-4} = x$.
So f has an order of 3, and f may “loop” back to itself after 3 times or 1 time. If $x = \frac{x-3}{x+1}$, then $x^2 + x = x - 3$, so $x^2 + 3 = 0$. x has an orbit of length 1 if -3 is a quadratic residue in mod p. This happens when $p \equiv 1 \pmod 3$.

Examining $f(x) = \frac{x-3}{x+1}$ in $\mathbb{P}_{11}$



Here $p = 3k - 1$, so -3 is not a QR and there are no loops of length 1. Thus all $p + 1 = 3k$ elements in $\mathbb{P}_p$ will be part of loops with length 3 for a total of $2k$ loops.

Examining $f(x) = \frac{x-3}{x+1}$ in $\mathbb{P}_{13}$



-3 is a quadratic residue in mod p when $p = 1 \pmod 3$, and $x^2 + 3 \equiv 0 \pmod{3k+1}$ would have 2 solutions. Thus, when $p = 3k + 1$, there are two loops of length 1. Because there are $p + 1 = 3k + 2$ elements in $\mathbb{P}_p$, $\frac{3k+2-2}{3} = k$ loops have length 2.

Matrices

We will introduce a relation between fractional linear functions and matrices.

Definition

Define the "matrix representation" of an FLF $\frac{ax+b}{cx+d}$ as $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Definition

Define the determinant of an FLF $\frac{ax+b}{cx+d}$ as $ad - bc$. We know the determinant cannot be zero.

FLF Composition

Claim 1: Composition of 2 FLFs is an FLF

$g = f_1 \circ f_2$ is an FLF.

Proof.

Say we have an FLF $f_1 = \frac{ax+b}{cx+d}$ and another FLF $f_2 = \frac{px+q}{rx+s}$.
Then, we have $g = f_1 \circ f_2 = \frac{a(\frac{px+q}{rx+s})+b}{c(\frac{px+q}{rx+s})+d} = \frac{(ap+br)x+(aq+bs)}{(cp+dr)x+(cq+ds)}$.
Also, because we have
$(ap+br)(cq+ds)-(aq+bs)(cp+dr) = (ad-bc)(ps-rq)$,

FLF Composition

This tells us that, given two matrices, $\underline{M}$ and $\underline{N}$, we have $|\underline{M}||\underline{N}| = |\underline{MN}|$, i.e. determinants of matrices/FLF's are multiplicative. Since neither $ad - bc$ nor $ps - rq$ can be zero, $(ad - bc)(ps - rq)$ also cannot be zero. Since $(ap + br), (aq + bs), (cp + dr), (cq + ds) \in \mathbb{P}_p$, and the determinant of g's matrix representation is also not zero, so we can conclude g is a fractional linear function in $\mathbb{P}_p$.

FLF Inverse

Claim 2: Inverse of an FLF is an FLF

$$f(x) = \frac{ax+b}{cx+d} \implies f^{-1}(x) = \frac{dx-b}{-cx+a}$$

Proof.

Let $f^{-1} = y$, so $y = \frac{ax+b}{cx+d}$ then since $f \circ f^{-1} = x$,
we have $\frac{ay+b}{cy+d} = x$
$\implies ay + b = cyx + dx$
$\implies y(a - cx) = dx - b$
so $y = f^{-1} = \frac{dx-b}{-cx+a}$.
This proves that f^{-1} is also a fractional linear function. □

Recursion

Consider the fractional linear function

$$\frac{ax+b}{cx+d}.$$

To begin our cycle, we can plug in 0 for x and obtain:

$$\frac{b}{d}.$$

Since we want to continue our cycle, we can plug this back into our original fractional linear function:

$$\frac{a\frac{b}{d}+b}{c\frac{b}{d}+d} = \frac{ab+bd}{db+d^2}.$$

In particular, we can define a recurrence relation!
We have:

$$P_0 = b \qquad P_k = aP_{k-1} + bQ_{k-1}$$
$$Q_0 = d \qquad Q_k = cP_{k-1} + dQ_{k-1}$$

Finding Cycles with Matrices

Consider again, our original value of $\frac{b}{d}$. We could plug that value into our FLF again, but note that the final answer we obtain is the same as multiplying the vector $\begin{bmatrix} b \\ d \end{bmatrix}$ by the matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

since

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} ab + bd \\ db + d^2 \end{bmatrix}.$$

In fact, we can continue this process: just multiply $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by $\begin{bmatrix} ab + bd \\ db + d^2 \end{bmatrix}$ to obtain the next fraction in our cycle.
We can think of "plugging in" any fractional value $\frac{p}{q}$ for x into the FLF $\frac{ax+b}{cx+d}$ as multiplying the FLF matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by the vector $\begin{bmatrix} p \\ q \end{bmatrix}$.

Matrices (Compositions)

We can use this matrix multiplication method to compose different fractional linear functions. Consider two FLF's, $f_1 = \frac{ax+b}{cx+d}$ and $f_2 = \frac{px+q}{rx+s}$. If we want to find the composition $f_1 \circ f_2$, we simply multiply the matrices:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} aq+pr & aq+bs \\ cp+dr & cq+ds. \end{bmatrix}$$

Note that this new matrix corresponds to the FLF $\frac{(aq+pr)x+(aq+bs)}{(cp+dr)x+(cq+ds)}$. We can use this method to compose different matrices to obtain a new matrix that corresponds to another FLF.

Matrices Exponentiation

In particular, we want to know what happens when we compose the FLF within itself, multiple times, which can provide a helpful description of the cycle lengths of the orbit diagrams. As described previously, this would correspond to multiplying the matrix representation multiple times, e.g. if we composed the FLF $\frac{ax+b}{cx+d}$ within itself n times, as a matrix we have:

$$\underbrace{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \cdots \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}}_{n \text{ times}}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix}^n.$$

However, multiplying matrices this way is very tedious and messy. Is there a better way?

Matrices (Inverses)

Now, recall that, given an FLF $\frac{ax+b}{cx+d}$, its inverse is $\frac{dx-b}{-cx+a}$. What if we did something similar with matrices?

Consider the corresponding matrix $\begin{bmatrix} a & b \\ c & d. \end{bmatrix}$

Therefore the inverse of a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is of the form $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We have $aa' + bc' = 1$, $ab' + bd' = 0$, $ca' + dc' = 0$, and $cb' + dd' = 1$. We claim that $a' = \frac{d}{ad-bc}$, $b' = \frac{-b}{ad-bc}$, $c' = \frac{-c}{ad-bc}$, and $d' = \frac{a}{ad-bc}$. Plugging in and verifying, we get:

$$
\begin{aligned}
a\frac{d}{ad-bc} + b\frac{-c}{ad-bc} &= 1 \\
a\frac{-b}{ad-bc} + b\frac{-a}{ad-bc} &= 0 \\
c\frac{d}{ad-bc} + d\frac{-c}{ad-bc} &= 0 \\
c\frac{-b}{ad-bc} + d\frac{a}{ad-bc} &= 1.
\end{aligned}
$$

Therefore, the inverse of a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a. \end{bmatrix}$

Note the similarity between the inverse of a matrix and the inverse formula we found in 2.1, $\frac{dx-b}{-cx+a}$; in fact, it's the exact same except without the $\frac{1}{ad-bc}$ in front of the matrix. In this case this isn't necessary because multiplying by a scalar will cancel out on top and bottom.

Cycle Lengths

Question 1

What are the possible cycle lengths?

To figure out the patterns of cycle lengths, let's try some examples in $\mathbb{P}_{13}$.

Cycle Lengths

Example 1

$\frac{x-2}{x+1}$

Cycle lengths: 7, 7

$1 \longrightarrow 6 \longrightarrow 8 \longrightarrow 5 \longrightarrow 7 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

$2 \longrightarrow 0 \longrightarrow 11 \longrightarrow 4 \longrightarrow 3 \longrightarrow 10 \longrightarrow 9 \longrightarrow 2$

Example 2

$\frac{x-3}{x+1}$

Cycle Lengths: 3, 3, 3, 1, 1

$1 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

$2 \longrightarrow 4 \longrightarrow 8 \longrightarrow 2$

$3 \longrightarrow 0 \longrightarrow 10 \longrightarrow 3$

6 (repeated)

7 (repeated)

Cycle Lengths

Example 3

$\frac{x-4}{x+1}$

Cycle Lengths: 12, 1, 1

$1 \longrightarrow 5 \longrightarrow 11 \longrightarrow 6 \longrightarrow 4 \longrightarrow 9 \longrightarrow 7 \longrightarrow 2 \longrightarrow 8 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

3 (repeated)

10 (repeated)

Example 4

$\frac{x-5}{x+1}$

Cycle length: 14

$1 \longrightarrow 11 \longrightarrow 7 \longrightarrow 10 \longrightarrow 4 \longrightarrow 5 \longrightarrow 0 \longrightarrow 8 \longrightarrow 9 \longrightarrow 3 \longrightarrow 6 \longrightarrow 2 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

Cycle Lengths

Example 5

$\frac{x-6}{x+1}$

Cycle length: 14

$1 \longrightarrow 4 \longrightarrow 10 \longrightarrow 11 \longrightarrow 8 \longrightarrow 6 \longrightarrow 0 \longrightarrow 7 \longrightarrow 5 \longrightarrow 2 \longrightarrow 3 \longrightarrow 9 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

Example 6

$\frac{x-7}{x+1}$

Cycle length: 14

$1 \longrightarrow 10 \longrightarrow 5 \longrightarrow 4 \longrightarrow 2 \longrightarrow 7 \longrightarrow 0 \longrightarrow 6 \longrightarrow 11 \longrightarrow 9 \longrightarrow 8 \longrightarrow 3 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

Cycle Lengths

Example 7

$\frac{x-8}{x+1}$

Cycle lengths: 7, 7

$1 \longrightarrow 3 \longrightarrow 2 \longrightarrow 11 \longrightarrow 10 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

$0 \longrightarrow 5 \longrightarrow 6 \longrightarrow 9 \longrightarrow 4 \longrightarrow 7 \longrightarrow 8 \longrightarrow 0$

Example 8

$\frac{x-9}{x+1}$

Cycle lengths: 6, 6, 1, 1

$1 \longrightarrow 9 \longrightarrow 0 \longrightarrow 4 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

$3 \longrightarrow 5 \longrightarrow 8 \longrightarrow 10 \longrightarrow 6 \longrightarrow 7 \longrightarrow 3$

2 (repeated)

11 (repeated)

Overlapping of Cycles

Claim 3: No Repeating Elements in Distinct Cycles

Distinct cycles formed by the same FLF in the same $\mathbb{P}_p$ can't have any repeating element in them. ($C_f(x)$ is the set of elements in the same cycle as x formed by FLF f).

Proof.

If $C_f(a) \cap C_f(b) \neq \varnothing$, then $\exists k_1, k_2 \in \mathbb{N}$ s.t. $f^{k_1}(a) = f^{k_2}(b)$
$\implies b = f^{k_1 - k_2}(a)$
But then we know that $\forall n \in C_f(b), n = f^{k_3}(b)$, so then
$n = f^{k_1 - k_2 + k_3}(a)$

Overlapping of cycles

Proof.

Since all elements in $C_f(b)$ can be written as some power of $f(a)$, then we know that $C_f(b) \subseteq C_f(a)$.
By symmetry, we could do the same for $C_f(b)$ to get $C_f(a) \subseteq C_f(b)$, which means that $C_f(b) = C_f(a)$.
Thus, if an element of two cycles overlaps, the two sets are equal, which proves our claim. $\square$

Lemma

For a given fractional linear function, there are either 0, 1, *or* 2 *inputs that cycle to themselves.*

Proof.

An input has a cycle length of 1 when a FLF $f(x) = \frac{ax+b}{cx+d}$ maps n to n for some $n \in \mathbb{Z}_p$. Thus, we have:

$$\frac{an+b}{cn+d} = n$$
$$an + b = cn^2 + dn$$
$$cn^2 + (d-a)n - b = 0$$

By Lagrange's Theorem, there are at most 2 solutions to a quadratic in $\mathbb{Z}_p$, so there are at most 2 one-cycles. $\square$

Claim 4

Every fractional linear function on $\mathbb{P}_p$ has a cycle length which divides $p^2 - 1$ or is exactly p.

Claim 5

For any given fractional linear function, there are at most 2 distinct possible cycle lengths, and if there are exactly 2, then one of the cycle lengths must be either 1 or 2.

Cycle Lengths

This requires some linear algebra background.

Diagonalizability

If an $n \times n$ matrix A is diagonalizable, then there exists a diagonal matrix D and $n \times n$ invertible matrix P such that $A = PDP^{-1}$.

Diagonal Matrix

A square matrix D where all the non-diagonal elements are 0.

D consists of the two eigenvalues of A. $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$

Cycle Lengths

The most important application of diagonalizable matrices is that you can easily exponentiate both sides. We can think of A^n as composing A with itself; or in FLF terms, applying the same fractional linear function n times.

$$A = PDP^{-1}$$

$$A^n = \underbrace{PDP^{-1} * PDP^{-1} * ... * PDP^{-1}}_{\text{n times}}$$

Due to the associative property of matrices,

$$A^n = \underbrace{PD(P^{-1} * P)DP^{-1} ... PD(P^{-1} * P)DP^{-1}}_{\text{n times}}$$

$$A^n = PD^nP^{-1}$$

Cycle Lengths

Anna Deng, Maggie Liang, Maggie Shen, Minerva You, Lisa Zheng

Introduction
Specific Examples
Linear Transformations
Counting Cycles
Extensions

Therefore, after finding D using eigenvalues, we can raise D to D^n. Since P and P^{-1} will remain the same, we can just view pre-multiplying by P and post-multiplying P^{-1} as a bijective function between A and D.

Cycle Lengths

Additionally, raising a diagonal matrix D to the nth power gives a diagonal matrix where each nonzero element in D to the nth power.

$$D = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$$

$$D^n = \begin{bmatrix} \lambda^n & 0 \\ 0 & \lambda^n \end{bmatrix}$$

Cycle Lengths

So we can use the diagonal matrix to determine the cycle length. If the cycle length is n, then D^n should give the same eigenvalues (mod p) as D. In terms of eigenvalues, that implies $\lambda_1^n = \lambda_1$ (mod p) and $\lambda_2^n = \lambda_2$. (mod p)
Thus, $\lambda_1^n - \lambda_1 = \lambda_2^n - \lambda_2 = 0$ (mod p)
In other words, λ_1 and λ_2 are the roots of the polynomial $x^n - x = 0$ or, dividing by x (assuming x is nonzero) $x^{n-1} - 1 = 0$.

Cycle Lengths

To calculate the eigenvalues, solve for λ in $|A - \lambda I| = 0$ where I is the identity matrix.

For example: Let's convert the cyclic FLF $\frac{x-6}{x+1}$ into a diagonal matrix.

$$A = \begin{bmatrix} 1 & -6 \\ 1 & 1 \end{bmatrix}$$

Solve for λ:

$$\left| \begin{bmatrix} 1 & -6 \\ 1 & 1 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right| = 0$$

$$\left| \begin{bmatrix} 1 & -6 \\ 1 & 1 \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \right| = 0$$

$$\left| \begin{bmatrix} 1-\lambda & -6 \\ 1 & 1-\lambda \end{bmatrix} \right| = 0$$

Cycle Lengths

$(1-\lambda)(1-\lambda)-(-6)(1)=0 \ \lambda^2-2\lambda+7$

Solving for λ gives a solution $\in \mathbb{C}$.

Namely, $\lambda = 1+\sqrt{6}i, 1-\sqrt{6}i$.

$$D = \begin{bmatrix} 1-\sqrt{6}i & 0 \\ 0 & 1+\sqrt{6}i \end{bmatrix}$$

Cycle Lengths

More generally,take an arbitrary FLF, $f(x) = \frac{ax+b}{cx+d}$. We diagonalize it by solving for λ:

$$\left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right| = 0$$

$$\left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \right| = 0$$

$$\left| \begin{bmatrix} a-\lambda & b \\ c & d-\lambda \end{bmatrix} \right| = 0$$

$$(a-\lambda)(d-\lambda) - bc = 0$$

$$\lambda^2 - (d+a)\lambda + ad - bc = 0$$

λ_1, λ_2 are the two roots of this quadratic.

Cycle Lengths

Here, we encounter an issue- these roots are not necessarily in $\mathbb{Z}_p$. Thus, we must move to a larger field in which the quadratic $\lambda^2 - (d+a)\lambda + ad - bc = 0$ has roots.

Definition 2: Splitting Fields

Let $K \subseteq L$ be fields. Let $f(x) = x^n + f_{n-1}x^{n-1} + \ldots + f_1x + f_0$ be a polynomial in $K[x]$. We say that L is a splitting field for f if

1. $f(x)$ *factors as* $\prod_{i=1} n(x - \theta_i)$ *in* $L[x]$
2. $L = K[\theta_1, \theta_2, \ldots, \theta_n]$

Cycle Lengths

Lemma

Let F be the set of solutions to $x^q = x$, taken $\pmod{p}$, where $q = p^n$ for some n. Then F is a field with characteristic p.

To prove, we show that there exists $0, 1$ in F, that F is closed under addition and multiplication, and that additive and multiplicative inverses exist in F. The most difficult step here is showing that F is closed under addition, we we do using binomial theorem.

Cycle Lengths

Lemma

Let $\mathbb{F}_q$ be the splitting field of the polynomial $x^q - x$. Then $\mathbb{F}_q$ has q elements, all of which are roots of $x^q - x$.

Proof.

By definition of a splitting field, $x^q - x$ factors into linear factors in $\mathbb{F}_q$. Thus, every root of $x^q - x$ must be in $\mathbb{F}_q$. By Lemma 1, these roots form a field, so this field must be the splitting field of $x^q - x$. Since the field contains all $(q-1)$th roots of unity and 0, there are exactly q elements in $\mathbb{F}_q$. $\square$

Cycle Lengths

$\forall x \in \mathbb{F}_q, x \neq 0$, where $q = p^2$ have the following:

$$\begin{aligned} x^q &= x \\ x^{q-1} &= 1 \\ x^{\frac{q-1}{2}^2} - 1 &= 0 \\ \left(x^{\frac{p^2-1}{2}} + 1\right)\left(x^{\frac{p^2-1}{2}} - 1\right) &= 0 \end{aligned}$$

Similar to in $\mathbb{Z}_p$, we know that x is a quadratic residue $\in \mathbb{F}_q$ $\iff x^{\frac{q-1}{2}} = 1$.

Cycle Lengths

Consider $a \in \mathbb{U}_p \subseteq \mathbb{F}_q$. We know that $a^{\frac{p-1}{2}} = \pm 1 \pmod{p}$. Thus, we have

$$\begin{aligned}
a^{\frac{p-1}{2}} &= \pm 1 \\
\left(a^{\frac{p-1}{2}}\right)^{p+1} &= \pm 1^{p+1} \\
p+1 \text{ is even} \implies \left(a^{\frac{p-1}{2}}\right)^{p+1} &= 1 \\
a^{\frac{(p-1)(p+1)}{2}} &= 1 \\
a^{\frac{p^2-1}{2}} &= 1 \\
\implies a \text{ is a QR} &\in \mathbb{F}_q
\end{aligned}$$

Cycle Lengths

Consider the quadratic $f(x) = ax^2 + bx + c$, $a, b, c \in U_p$. We have that the roots of this quadratic are given by the following:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

We know that $a, b, c \in U_p$. This implies that either $b^2 - 4ac \in U_p$ or $b^2 - 4ac = 0$. If the latter is true, then both roots of f are in U_p, which implies that they must also be in $\mathbb{F}_q$. Else, if $b^2 - 4ac \in U_p$, then it is a quadratic residue in $\mathbb{F}_q$, so there exists two elements in $\mathbb{F}_q$ that equal:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Thus, every root of a quadratic is in $\mathbb{F}_q$.

Cycle Lengths

For our proof, that means $\lambda_1, \lambda_2 \in \mathbb{F}_q$. Thus, for λ_1, λ_2 both we have the following:

$$\lambda^q = \lambda$$
$$\lambda^{q-1} = 1$$
$$\lambda^{(p^2-1)} = 1$$

Thus, if there exists $a \in N$ such that $\lambda_1^a = 1, \lambda_2^a = 1$, we have $a \mid (p^2 - 1)$.

Cycle Lengths

There is a special exception case here, what if the matrix is not diagonalizable? If our quadratic $\lambda^2 - (d+a)\lambda + ad - bc = 0$ has a double root, then the matrix is not necessarily diagonalizable. This happens when:

$$\begin{aligned} (d+a)^2 - 4ad + 4bc &= 0 \\ d^2 + 2ad + a^2 - 4ad + 4bc &= 0 \\ (d-a)^2 + 4bc &= 0 \end{aligned}$$

Recall our quadratic equation to find the one-cycles of an FLF. We had that the roots of $cn^2 + (d-a)n - b = 0$ are one-cycles. Notice how the determinant of this quadratic is the same as the determinant of our quadratic for λ. Thus, there is also a double root to this quadratic, so there is exactly one one-cycle. We conjecture that the remaining p elements of $\mathbb{P}_p$ form a single cycle of length p.

Number of functions on $\mathbb{P}_p$

How many fractional linear functions are on $\mathbb{P}_p$? There are two ways to consider this question: with simplification or without simplification. For example without simplification, we would consider

$$\frac{x+3}{2x+1}, \frac{2x+6}{4x+3}, \frac{5x+1}{3x+5}$$

as three different FLFs on $\mathbb{P}_7$. However, with simplification, we have

$$\begin{aligned}
\frac{x+3}{2x+1} \cdot \frac{2}{2} &= \frac{2x+6}{4x+2} \\
\implies \quad \frac{2x+6}{4x+2} &= \frac{x+3}{2x+1} \\
\frac{x+3}{2x+1} \cdot \frac{5}{5} &= \frac{5x+15}{10x+5} = \frac{5x+1}{3x+5} \\
\implies \quad \frac{5x+1}{3x+5} &= \frac{x+3}{2x+1}
\end{aligned}$$

Number of functions on $\mathbb{P}_p$

Definition 3: Simplified Fractional Linear Function

We say that a Fractional Linear Function $\frac{ax+b}{cx+d}$ *is in simplest form if and only if* $a = 1$ *or* $a = 0$ *and* $b = 1$.

Lemma

Let $f_1 = \frac{ax+b}{cx+d}$ *and* $f_2 = \frac{a'x+b'}{c'x+d'}$ *(where* $f_1, f_2 \in \mathbb{P}_p$*, then if we have* $u \in \mathbb{U}_p$ *such that:*

$$a = a'u,\ b = b'u,\ c = c'u,\ d = d'u$$

then $f_1 \sim f_2$ *in* $\mathbb{P}_p$*, where* $\sim$ *is defined as equivalent.*

Number of functions on $\mathbb{P}_p$

To prove that every FLF can be written as an equivalent simplified FLF, consider an arbitrary fractional linear function

$$f(x) = \frac{ax+b}{cx+d}$$

with $a, b, c, d \in \mathbb{Z}_p$. If $a = 0$ or $a = 1$, then we are done. Else, a has a multiplicative inverse a^{-1} in $\mathbb{U}_p$. We have:

$$\frac{ax+b}{cx+d} \cdot \frac{a^{-1}}{a^{-1}} = \frac{(a \cdot a^{-1})x + (b \cdot a^{-1})}{(c \cdot a^{-1})x + (d \cdot a^{-1})} = \frac{x + (b \cdot a^{-1})}{(c \cdot a^{-1})x + (d \cdot a^{-1})}.$$

Since a^{-1} is in $\mathbb{U}_p$, Thus by the Lemma,

$$\frac{x + (b \cdot a^{-1})}{(c \cdot a^{-1})x + (d \cdot a^{-1})} \sim f(x)$$

which is in simplest form.

Number of functions on $\mathbb{P}_p$

Claim 6

There are $(p-1)^2(p+1)(p)$ fractional linear functions without simplification.

To prove, we consider the set G of all fractional linear function on $\mathbb{P}_p$ Let

$$G = \left\{ \frac{ax+b}{cx+d} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc \neq 0 \text{ in } \mathbb{Z}_p \right\}$$

Number of functions on $\mathbb{P}_p$

Then, we claim G is a group under $\circ$. We can prove this by verifying that it satisfies the group axioms:

1. Associativity: The composition of functions is associative, so G is associative under $\circ$.
2. Identity: The FLF $\frac{x+0}{0x+1} = x$ is the identity, because if you compose any function with x and it will equal itself.
3. Inverses: By (b) there exists an unique inverse that is also a FLF to each FLF.
4. Closure: By (b) the composition of two FLFs is always another FLF, so G is closed under $\circ$.

Number of functions on $\mathbb{P}_p$

Definition 4: Stabilizer

Let X be a set with $x \in X$.Let G be a group that acts on X. Then, the stabilizer of x is

$$stab(x) = \{g \in G \mid g(x) = x\}.$$

Definition 5: Orbit

Let X be a set with $x \in X$. Let G be a group that acts on X. Then, the orbit of x is

$$orb(x) = \{g(x) \mid g \in G\}$$

.

Number of functions on $\mathbb{P}_p$

Theorem 2: Orbit-Stabilizer Theorem

For G a finite group which acts on X, $x \in X$, we have

$$|G| = |stab(x)| \cdot |orb(x)|$$

We can use the Orbit-Stabilizer Theorem to find the number of FLFs on $\mathbb{P}_p$. Since G is the group of all FLFs, $|G|$ is the number of FLFs on $\mathbb{P}_p$. G acts on the $\mathbb{Z}_p$, so $X = \mathbb{Z}_p$. To use Orbit-Stabilizer, we pick an element $x \in \mathbb{Z}_p$.

Number of functions on $\mathbb{P}_p$

Let $x = 0$. The orbit of 0 is the set of all elements that any FLF can map 0 to on $\mathbb{Z}_p$. Consider the following FLF for $a \in \mathbb{Z}_p$.

$$\frac{x+a}{x+1}$$

When $x = 0$, this FLF becomes $\frac{a}{1}$. Since a can take any value in $\mathbb{Z}_p$, there exists at least one FLF that maps a to every integer from 0 to $p-1$. Additionally, we have that the FLF

$$\frac{x+1}{x+0} = \frac{1}{0}$$

when $x = 0$, which means this FLF maps 0 to ∞. Thus, for each $y \in \mathbb{P}_p$ there exists at least one FLF that maps 0 to y. The orbit of 0 is $\mathbb{P}_p$, and we have

$$|\mathrm{orb}(0)| = p + 1.$$

Number of functions on $\mathbb{P}_p$

Now, we consider the stabilizer of 0, which is the set of all FLFs which map 0 to 0. Take an arbitrary FLF $f(x) = \frac{ax+b}{cx+d}$ in the stabilizer of 0.

$f(0) = 0 \implies b = 0$. We know that $ad - bc \neq 0 \mod p$, and since $b = 0, bc = 0$, we have $ad \neq 0 \implies a \neq 0, d \neq 0$. Otherwise, there are no other restrictions on the coefficients of f, so a, d can equal any nonzero element of $\mathbb{Z}_p$, c can equal any element of $\mathbb{Z}_p$, and b must be zero. Hence, we have that there are p choices for c and $p-1$ choices for a, d, and 1 choice for b giving us

$$|\text{stab}(0)| = (p-1)^2 \cdot p$$

By Orbit-Stabilizer Theorem, we have

$$\begin{aligned} |G| &= |\text{stab}(0)| \cdot |\text{orb}(0)| \\ &= (p-1)^2(p)(p+1). \end{aligned}$$

Number of functions on $\mathbb{P}_p$

Claim 7

There are $(p-1)(p+1)(p)$ fractional linear functions in simplest form.

Once again, lets construct a set H of all fractional linear functions. Let

$$H = \left\{ f(x) = \frac{ax+b}{cx+d} \mid a, b, c, d \in \mathbb{Z}_p, ad - bc \neq 0, f(x) \text{is in simpl} \right.$$

Number of functions on $\mathbb{P}_p$

Since H is a group, we can once again apply Orbit-Stabilizer. We will again consider the orbit and stabilizer of 0. The orbit of 0 is still $x+1$ because $\frac{x+a}{x+1}$ still maps 0 to each element $a \in \mathbb{Z}_p$ and $\frac{x+1}{x+0}$ still maps 0 to ∞. The stabilizer of 0 is the set of all FLFs in the form $f(x) = \frac{ax+b}{cx+d}$ where $a = 0, 1$ such that $f(0) = 0$. We once again have that $b = 0$. We have $ad - bc \neq 0$ and $b = 0 \implies bc = 0 \implies ad \neq 0 \implies a \neq 0, b \neq 0$. Since $a = 0, 1, a \neq 0$ we have $a = 1$. Thus, we have 2 of our coefficients fixed.

Number of functions on $\mathbb{P}_p$

d can take any value in $\mathbb{Z}_p$ except 0, so we have $p-1$ choices for d. c can take any value in $\mathbb{Z}_p$, so we have $p-1$ choices for c. In total, this gives us:

$$1 \cdot 1 \cdot (p-1) \cdot (p) = p(p-1)$$

functions in the stabilizer of 0.
By the Orbit-Stabilizer Theorem, we have:

$$|H| = |\text{stab}(0)| \cdot |\text{orb}(0)|$$
$$|H| = (p-1)(p)(p+1)$$

Determining an FLF

Claim 8: $f(\infty)$, $f(0)$, and $f(1)$

The FLF f can be uniquely determined by 3 values $f(\infty)$, $f(0)$, $f(1)$

Proof.

First, we know that

$$f(\infty) = \frac{a}{c}$$
$$f(0) = \frac{b}{d}$$
$$f(1) = \frac{a+b}{c+d}$$

By the previous lemma, we also know that the fractional linear functions differ by multiplications of $u \in \mathbb{U}_p$,

Determining an FLF

Proof.

so assume that

$$\frac{a}{c} \sim \frac{e_1}{e_2}, \text{ where } a = e_1 \cdot u_1,\ c = e_2 \cdot u_1$$
$$\frac{b}{d} \sim \frac{e_3}{e_4}, \text{ where } b = e_3 \cdot u_2,\ d = e_4 \cdot u_2$$
$$\frac{a+b}{c+d} \sim \frac{e_5}{e_6}, \text{ where } a+b = e_5 \cdot u_3,\ c+d = e_6 \cdot u_3$$

$$\text{So, } e_5 \cdot u_3 = e_1 \cdot u_1 + e_3 \cdot u_2$$
$$e_6 \cdot u_3 = e_2 \cdot u_1 + e_4 \cdot u_2$$

Now, we know that fractional linear functions can be expressed as matrices, so from the relationship above we have:

$$u_3 \begin{bmatrix} e_5 \\ e_6 \end{bmatrix} = \begin{bmatrix} e_1 & e_3 \\ e_2 & e_4 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

Determining an FLF

Proof.

$$\text{so, } \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \frac{u_3}{e_1 e_4 - e_2 e_3} \begin{bmatrix} e_4 & -e_3 \\ -e_2 & e_1 \end{bmatrix} \begin{bmatrix} e_5 \\ e_6 \end{bmatrix}$$

$$\implies u_1 = \frac{u_3}{e_1 e_4 - e_2 e_3}(e_4 e_5 - e_3 e_6)$$

$$u_2 = \frac{u_3}{e_1 e_4 - e_2 e_3}(e_1 e_6 - e_2 e_5)$$

and we assume

$$u_3 = e_1 e_4 - e_2 e_3$$

for the sake of canceling fractions.

Then, since $e_1, e_2, e_3, e_4, e_5, e_6$ are determined by $f(0), f(1), f(\infty)$, we can know the values of u_1, u_2, u_3 based on $f(0), f(1), f(\infty)$. So, we know that the values of these three values can uniquely determine the values of a, b, c, d. $\square$

Determining an FLF

Claim 9: An FLF can be determined by any three points

The FLF f can be unique determined by 3 values $f(x), f(y), f(z)$, where $x, y, z \in \mathbb{P}_p$.

Proof.

By above, we know that K_1 will be uniquely determined if

$$K_1(0) = n_1,\ K_1(\infty) = n_2,\ K_1(1) = n_3$$

the same applies for K_2 if

$$K_2(0) = m_1,\ K_2(\infty) = m_2,\ K_2(1) = m_3$$

Determining an FLF

Proof.

Now, define a fractional linear function, K_3, where $K_3 = K_1^{-1} \circ K_2$, so we get

$$K_3(n_1) = m_1,\ K_3(n_2) = m_2,\ K_3(n_3) = m_3$$

Since K_1 and K_2 are already uniquely determined, then we know that K_3 must also be uniquely determined in domain $\mathbb{P}_p$, which proves our claim. $\square$

Continued Fractions

Definition 6: Continued Fraction

A finite continued fraction is a rational written in the form $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}$*.An infinite continued fraction is an irrational written in the form* $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots +}}$.

Definition 7: Convergents

A convergent of $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}$ *or* $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots +}}$ *equals* $\frac{P_k}{Q_k} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_k}}}$ *where* $k \leq n$.

Continued Fractions

Theorem 3: Magic Square Recurrence

$$P_k = a_k P_{k-1} + P_{k-2}, Q_k = a_k Q_{k-1} + Q_{k-2}.$$

Let $f(x) = \frac{1}{a+x}$. Let us examine different compositions of f.

$$f(x) = f^1(x) = \frac{1}{a+x}$$

$$f(f(x)) = f^2(x) = \frac{1}{a + \frac{1}{a+x}}$$

$$f(f(f(x))) = f^3(x) = \frac{1}{a + \frac{1}{a+\frac{1}{a+x}}}$$

$$\vdots$$

Continued Fractions

We have shown that function composition of FLF's generates more FLFs. Thus, all $f^n(x)$ are also FLFs.

$$f(x) = f^1(x) = \frac{1}{a+x}$$

$$f(f(x)) = f^2(x) = \frac{x+a}{ax+(a^2+1)}$$

$$f(f(f(x))) = f^3(x) = \frac{ax+(a^2+1)}{(a^2+1)x+(a^3+2a)} \cdots$$

If we set $x=0$, these results are continued fractions $f^1(0) = \frac{1}{a} = \frac{P_1}{P_2}$, $f^2(0) = \frac{a}{a^2+1} = \frac{P_2}{P_3}$, $f^3(0) = \frac{a^2+1}{a^3+2a} = \frac{P_3}{P_4}, \ldots$.
In fact, they are convergents of the infinite continued fraction

$$y = \cfrac{1}{a + \cfrac{1}{a + \cdots}}.$$

Continued Fractions

We can try to solve for y by "undoing" a layer of the continued fraction:

$$\frac{1}{y} - a = y$$

$$y^2 + ay - 1 = 0$$

$$y = \frac{-a + \sqrt{a^2 + 4}}{2}.$$

Note how the coefficients in the FLF's of each level of composition show up in the continued fraction convergents. We see that $f^1(x) = \frac{P_0 x + P_1}{P_1 x + P_2}$, $f^2(x) = \frac{P_1 x + P_2}{P_2 x + P_3}, \ldots$ such that in general $f^n(x) = \frac{P_{n-1} x + P_n}{P_n x + P_{n+1}}$. This can be shown with induction. Our base case is shown above in the examples. Now assume that $f^k(x) = \frac{P_{k-1} x + P_k}{P_k x + P_{k+1}}$. Then $f^{k+1}(x) = \frac{1}{1 + f^k(x)} =$

$$\frac{1}{a + \frac{P_{k-1} x + P_k}{P_k x + P_{k+1}}} = \frac{P_k x + P_{k+1}}{a P_k x + a P_{k+1} + P_{k-1} x + P_k} = \frac{P_k x + P_{k+1}}{P_{k+1} x + P_{k+2}}.$$

Continued Fraction

Now we will generalize our findings to a more generalized continued fraction.

Claim: $\begin{bmatrix} P_{n-1} & P_n \\ Q_{n-1} & Q_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_2 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & a_n \end{bmatrix}$

Proof: We want to show that $\begin{bmatrix} P_k & P_{k+1} \\ Q_k & Q_{k+1} \end{bmatrix} =$ $\begin{bmatrix} P_{k-1} & P_k \\ Q_{k-1} & Q_k \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & a_{k+1} \end{bmatrix}$. The RHS equals $\begin{bmatrix} P_k & P_{k-1} + a_{k+1} P_k \\ Q_k & Q_{k-1} + a_{k+1} Q_k \end{bmatrix}$ and by the magic square recurrence formulas, this matrix is precisely $\begin{bmatrix} P_k & P_{k+1} \\ Q_k & Q_{k+1} \end{bmatrix}$.

Continued Fraction

In fact, we can represent these matrices with FLFs. So

$$\begin{aligned}\frac{P_{n-1}x + P_n}{Q_{n-1}x + Q_n} &= \frac{1}{x+a_1} \circ \frac{1}{x+a_2} \circ \cdots \circ \frac{1}{x+a_n} \\ &= \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_n + x}}}}.\end{aligned}$$

Fin.

Anna Deng, Maggie Liang, Maggie Shen, Minerva You, Lisa Zheng

Introduction
Specific Examples
Linear Transformations
Counting Cycles
Extensions

THANK YOU FOR LISTENING!

Any questions?