PROMYS 2024

Exploration Lab

Fractional Linear Functions

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

Counselor:
Andrew Tung

August 2, 2024

Contents

1 Introduction

1.1 Introductory Definitions

Definition 1: FLF

We define a fractional linear function (FLF) as a function f in the form:

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

Here, we'll focus on the FLFs defined over $\mathbb{P}_p$.

Now, let's try some examples on $\mathbb{Z}_7$, where

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

But, when we try to evaluate $f(6)$, we get $\frac{13}{7} = \frac{6}{0}$, but we can't divide anything by 0. So, let's define a new symbol ∞ such that $f(-1) = f(6) = \infty$.

Note that if we try to evaluate $f(\infty) = \frac{2\infty+1}{\infty+1}$, and since we treat ∞ as a very large value compared to 1, we get that $f(\infty) = \frac{2\infty+1}{\infty+1} = \frac{2\infty}{\infty} = 2$.

Definition 2: ∞

$\forall a \in \mathbb{R}, a \neq 0$, we define ∞ as $\frac{a}{0} = \infty$. Then, $\forall a, b, c, d \in \mathbb{R}, a, c \neq 0$, we $\frac{a\cdot\infty+b}{c\cdot\infty+d} = \frac{a}{b}$.

Definition 3: $\mathbb{P}_p$

Let p be a prime and $p \in \mathbb{N}$, then

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

Now, we can analyze the properties of ∞. Given $f(x) = \frac{ax+b}{cx+d}$, then we have that $f(x) = \infty$ when $cx+d = 0$, and $f(\infty) = \frac{a}{c}$.

To define our fractional linear function better, in $\mathbb{P}_p$, we have $f(x) = \infty$ when $x \equiv dc^{-1} \pmod{p}$ and $f(\infty) = ac^{-1}$, where c^{-1} is the modular inverse of c in $\mathbb{Z}_p$. Furthermore, we know that c^{-1} exists $\forall c \in \mathbb{Z}_p$ because p is prime, and thus if $c \neq 0 \implies (c, p) = 1$.

1.2 Orbit Diagrams

We can represent a Fractional Linear Function using an orbit diagram. For example, $f(x) = \frac{2x+1}{x+1}$ on $\mathbb{P}_7$, we can draw the following diagrams:

$$\begin{array}{ccccc} 0 & \longrightarrow & 1 & \quad 2 & \longrightarrow & 4 \\ \uparrow & & \downarrow & \quad \uparrow & & \downarrow \\ 5 & \longleftarrow & 3 & \quad \infty & \longleftarrow & 6 \end{array}$$

As represented in these diagrams, we know that $f(x) = \frac{2x+1}{x+1}$ maps 0 to 1, 1 to 3, 3 to 5, and 5 to 0 on $\mathbb{P}_p$. Additionally, it tells us that $f(x)$ maps 2 to 4, 4 to 6, 6 to ∞ and ∞ to 2.

Definition 4: Cycle

We call a cycle of an FLF $f(x)$ on $\mathbb{P}_p$ a closed loop on the orbit diagram of $f(x)$ on $\mathbb{P}_p$. For example, we would say that $f(x) = \frac{2x+1}{x+1}$ on $\mathbb{P}_7$ has two cycles of length 4.

Claim: Given a fractional linear function with $ad - bc \neq 0 \pmod{p}$ such that $a \neq 0, c \neq 0$ and p prime, every value of $\mathbb{P}_p$ is included in at least one orbit diagram.

Proof. Let

$$f(x) = \frac{ax+b}{cx+d},$$
$$\text{where } a, b, c, d \in \mathbb{Z}_p$$
$$ad - bc \neq 0, a \neq 0, c \neq 0,$$

be an arbitrary fractional linear function on $\mathbb{P}_p$. Suppose for the sake of contradiction that there exists some element $n \in \mathbb{P}_p$ which is not in any orbit diagram. First, we consider when $n = \infty$ or $n = 0$
If $n = \infty$, then by the definition of ∞, we have

$$f(x) = n \iff cx + d = 0.$$

If $n = 0$, then

$$f(x) = n \iff ax + b = 0$$

We know both $ax + b = 0$ and $cx + d = 0$ cannot be true because

$$\begin{aligned} & ax + b = 0, cx + d = 0 \\ \implies & x = \frac{-b}{a} = \frac{-d}{c} \\ \implies & ad = bc \\ \implies & ad - bc = 0. \rightarrow\leftarrow \end{aligned}$$

If $n = \infty$, since $c \neq 0$, we have $c \in U_p \implies \exists c^{-1} \in U_p$.
Let $x = c^{-1}(-d)$. Since $-d, c^{-1} \in U_p$, $x \in \mathbb{Z}$ by closure of multiplication. Then,

$$\begin{aligned} \frac{ax+b}{cx+d} &= \frac{a \cdot c^{-1}(-d) + b}{(c \cdot c^{-1}(-d)) + d} \\ &= \frac{a \cdot c^{-1}(-d) + b}{1 \cdot -d + d} \\ &= \frac{a \cdot c^{-1}}{0} \\ &= \infty \\ &= n \end{aligned}$$

If $n = 0$, then $a \neq 0 \implies a \in U_p \implies \exists a^{-1} \in U_p$. Then, let $x = a^{-1}(-b)$

$$\begin{aligned} \frac{ax+b}{cx+d} &= \frac{a \cdot (a^{-1}(-b)) + b}{c \cdot a^{-1}(-b) + d} \\ &= \frac{1 \cdot (-b) + b}{c \cdot a^{-1}(-b) + d} \\ &= \frac{0}{c \cdot a^{-1}(-b) + d} \\ &= 0 \\ &= n \end{aligned}$$

Otherwise, $n \in \mathbb{P}_p, \neq \infty, n \neq \infty \implies n \in \mathbb{U}_p$. Then we have that there does not exist x such that

$$\begin{aligned} f(x) = \frac{ax+b}{cx+d} &= n \\ ax+b &= (cx+d)n \\ ax+b &= cnx+dn \\ (a-cn)x &= dn-b \end{aligned}$$

Solving for x gives $x = \frac{dn-b}{a-cn}$. By closure, $a - cn \in \mathbb{Z}_p$. If $a - cn = 0, x = \infty$. Otherwise, $a - cn \in U_p$, so $\frac{1}{a-cn} \in U_p$ which implies $\frac{dn-b}{a-cn} \in \mathbb{Z}_p$.

Thus, there always exists an x in $\mathbb{P}_p$ such that $f(x) = n$. □

Claim: Distinct cycles formed by the same FLF in the same $\mathbb{P}_p$ can't have any repeating element in them.

Proof. Let $C_f(x)$ be the set of elements in the same cycle as x formed by FLF f

$$\begin{aligned} & C_f(a) \cap C_f(b) \neq \varnothing \\ \implies & \exists k_1, k_2 \in \mathbb{N} \text{s.t.} f^{k_1}(a) = f^{k_2}(b) \\ \implies & b = f^{k_1-k_2}(a) \end{aligned}$$

But then we know that $\forall n \in C_f(b), n = f^{k_3}(b)$, so then $n = f^{k_1-k_2+k_3}(a)$

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. □

2 Matrices

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

Definition 5: Matrix Representation of an FLF

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

Definition 6: Determinant of an FLF

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

2.1 Composition and Inverses

Let us first show that the composition of two FLFs is an FLF. 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:

$$\begin{aligned}
&(ap+br)(cq+ds) - (aq+bs)(cp+dr) \\
&= -bcps + apds + bcrq + brds - aqdr - bsdr \\
&= -bcps + apds + bcrq - aqdr \\
&= -bc(ps-rq) + ad(ps-qr) \\
&= (ad-bc)(ps-rq)
\end{aligned}$$

This tells us two things: given two matrices, M and N, we have $|M||N| = |MN|$, i.e. determinants of matrices and 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, g is a fractional linear function in $\mathbb{P}_p$. Furthermore, the composition of fractional linear functions is associative by properties of function composition.

Let us now show that given $f = \frac{ax+b}{cx+d}$, we have $f^{-1} = \frac{dx-b}{-cx+a}$. Let $f^{-1} = y$, then since $f \circ f^{-1} = x$, we have

$$\begin{aligned}
&\frac{ay+b}{cy+d} = x \\
&\implies ay + b = cyx + dx \\
&\implies y(a-cx) = dx - b \\
&\implies y = f^{-1} = \frac{dx-b}{-cx+a}.
\end{aligned}$$

This proves that f^{-1} is also a fractional linear function.

Furthermore, we can verify that, when we compose these two FLFs, we obtain

$$\begin{aligned}
&\frac{a\left(\frac{dx-b}{-cx+a}\right)+b}{c\left(\frac{dx-b}{-cx+a}\right)+d} \\
&= \frac{a(dx-b)+b(-cx+a)}{c(dx-b)+d(-cx+a)} \\
&= \frac{(ad-bc)x}{ab-bc} \\
&= x.
\end{aligned}$$

2.2 Matrices/Recursion

Consider the fractional linear function

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

First, we plug in 0 for x and obtain:

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

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:

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

This, on its own, isn't particularly useful. Another more useful discovery is the relation of these fractional linear functions to matrices. Consider again, our original value of $\frac{b}{d}$. We could plug that value in again, but note that the final answer we obtain is the same as multiplying $\frac{b}{d}$ 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 value in our cycle.

That's not all we can do, either! 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 continue composing matrices within itself.

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 $\begin{bmatrix} a & b \\ c & d. \end{bmatrix}$ We want to find an "identity" matrix, just like the identity FLF, which is x. Thus we wish to find matrix $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ such that

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

for all a, b, c, d. Therefore we want:

$$\begin{aligned} aq+pr &= a \\ aq+bs &= b \\ cp+dr &= c \\ cq+ds &= d \end{aligned}$$

Quickly we note that, $q = 1, s = 1, q = 0, r = 0$. Therefore the identity matrix is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1. \end{bmatrix}$$

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.

3 Fractional Linear Functions on $\mathbb{P}_p$

3.1 Cycle Lengths on $\mathbb{P}_p$

We examined different FLFs in the same modulus. Here is a series of examples in $\mathbb{P}_1 3$.

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)

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 (this FLF is cyclic!)
$1 \longrightarrow 11 \longrightarrow 7 \longrightarrow 10 \longrightarrow 4 \longrightarrow 5 \longrightarrow 0 \longrightarrow 8 \longrightarrow 9 \longrightarrow 3 \longrightarrow 6 \longrightarrow 2 \longrightarrow 12 \longrightarrow \infty \longrightarrow 1$

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

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)

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

Conjecture: 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.

3.2 Matrix Diagonalization

We will use Matrix Diagonalization to prove our first claim. This requires some linear algebra background.

Definition 7: Diagonal Matrix

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

Definition 8: 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 $A = PDP^{-1}$.

Diagonalizing a matrix makes it extremely easy to exponentiate, which is convenient for us. Suppose we have an $n \times n$ matrix A which is diagonalizable. Then, we have the following:

$$D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$
$$A = PDP^{-1}$$
$$A^n = \underbrace{PDP^{-1} * PDP^{-1} * \cdots * PDP^{-1}}_{\text{n times}}$$

Due to the associative property of matrices,

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

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.

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

$$D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$
$$D^n = \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix}$$

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 $\lambda_1^n = \lambda_1 \pmod p$ and $\lambda_2^n = \lambda_2 \pmod p$.

Thus, $\lambda_1^n - \lambda_1 = \lambda_2^n - \lambda_2 = 0 \pmod{\text{p}}$

In other words, λ_1 and λ_2 are the roots of the polynomial

$$\begin{aligned} x^n - x &= 0 \\ \implies x^{n-1} - 1 &= 0. \\ \implies x^{n-1} &= 1 \end{aligned}$$

To calculate the eigenvalues, we solve for λ:

$$|A - \lambda I| = 0$$

where I is the identity matrix.

For example, let's convert the cyclic FLF $\frac{x-6}{x+1}$ into a matrix. Solve for λ:

$$\begin{aligned} A &= \begin{bmatrix} 1 & -6 \\ 1 & 1 \end{bmatrix} \\ \left| \begin{bmatrix} 1 & -6 \\ 1 & 1 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right| &= 0 \\ \left| \begin{bmatrix} 1 & -6 \\ 1 & 1 \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \right| &= 0 \\ \left| \begin{bmatrix} 1-\lambda & -6 \\ 1 & 1-\lambda \end{bmatrix} \right| &= 0 \\ (1-\lambda)(1-\lambda) - (-6)(1) &= 0 \\ \lambda^2 - 2\lambda + 7 &= 0 \end{aligned}$$

Solving for λ gives a solution $\in \mathbb{C}$. Namely, $\lambda = 1 + \sqrt{6}i, 1 - \sqrt{6}i$.

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

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

$$\begin{aligned} \left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right| &= 0 \\ \left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \right| &= 0 \\ \left| \begin{bmatrix} a-\lambda & b \\ c & d-\lambda \end{bmatrix} \right| &= 0 \\ (a-\lambda)(d-\lambda) - bc &= 0 \\ \lambda^2 - (d+a)\lambda + ad - bc &= 0 \end{aligned}$$

λ_1, λ_2 are the two roots of this quadratic.

Notice how we are working in $\mathbb{Z}_p$, but in our example, we had $\lambda = 1 + \sqrt{6}i, 1 - \sqrt{6}i$, which is not in $\mathbb{Z}_p$. Thus, we need to move to another field L where the roots of $\lambda^2 - (d+a)\lambda + ad - bc = 0$ are in L.

Definition 9: Splitting Fields

Let $K \subseteq L$ be fields. Let $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ 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. *$L = K[\theta_1, \theta_2, \ldots, \theta_n]$*

Definition 10: Characteristic

Let F be a field with finitely many elements. Let p be the least positive integer which is 0 in F. Then, we say p is called the characteristic of F.

Lemma 1

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.

Proof. We know 0 is a root of $x^q - x$. We also have $\forall x \in F, x \neq 0$

$$x^q = x \implies x^{q-1} = 1$$

Thus, x is either 0 or a $(q-1)$th root of unity. Let ζ be a primitive $(q-1)$th root of unity. Then, we have

$$F = 0, \zeta, \zeta^2, \ldots \zeta^{q-1}$$

We need to show that F is field, which means it must follow the field axioms:

- Additive Identity: 0 is in F
- Multiplicative Identity: $\zeta^{q-} = 1 \implies 1 \in F$
- Closure under Multiplication: Take $x, y \in F$. We have the following:

$$\begin{aligned} x^q &= x \\ y^q &= y \\ \implies x^q y^q &= xy \\ \implies (xy)^q &= xy \\ \implies xy &\in F \end{aligned}$$

- Multiplicative Inverses: Take $x \in F$. We have the following:

$$\begin{aligned} x \cdot x^{-1} &= 1 \\ x^q \cdot (x^{-1})^q = (x \cdot x^{-1})^q &= 1^q = 1 \\ x &= x^q \\ \implies x \cdot (x^{-1})^q &= 1 \\ \implies (x^{-1})^q &= x^{-1} \\ \implies x^{-1} &\in F \end{aligned}$$

- Closure under Addition: Take $x, y \in F$. We prove closure of addition by Binomial Theorem.

$$(x+y)^q = x^q + \binom{q}{1}x^{q-1}y + \binom{q}{2}x^{q-2}y^2 + \cdots + \binom{q}{q-1}xy^{q-1} + y^q$$

We claim that $\forall k \in \mathbb{N}, k \leq p^n = q, \binom{p^n}{k}$ is a multiple of p. We can prove this by counting the power of p in the prime factorization of $(p^n)!$, $(k!)$, and $(p^n - k)!$, which we call $v_p(n)$ for some n. We have the following:

$$\begin{aligned}
v_p((p^n)!) &= \frac{p^n}{p} + \frac{p^n}{p^2} + \cdots + \frac{p^n}{p^n} \\
&= p^{n-1} + p^{n-2} + \cdots + 1 \\
v_p(k!) &= \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{k}{p^n} \right\rfloor \\
v_p((p^n-k)!) &= \left\lfloor \frac{p^n-k}{p} \right\rfloor + \left\lfloor \frac{p^n-k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{p^n-k}{p^n} \right\rfloor \\
v_p(k!) + v_p((p^n-k)!) &= \left\lfloor \frac{p^n-k}{p} \right\rfloor + \left\lfloor \frac{p^n-k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{p^n-k}{p^n} \right\rfloor + \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{k}{p^n} \right\rfloor \\
&= \left(\left\lfloor \frac{p^n-k}{p} \right\rfloor + \left\lfloor \frac{k}{p} \right\rfloor \right) + \left(\left\lfloor \frac{p^n-k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor \right) + \cdots + \left(\left\lfloor \frac{p^n-k}{p^n} \right\rfloor + \left\lfloor \frac{k}{p^n} \right\rfloor \right) \\
&= \left(\left\lfloor \frac{p^n-k}{p} \right\rfloor + \left\lfloor \frac{k}{p} \right\rfloor \right) + \left(\left\lfloor \frac{p^n-k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor \right) + \cdots + \left(\left\lfloor \frac{p^n-k}{p^{n-1}} \right\rfloor + \left\lfloor \frac{k}{p^{n-1}k} \right\rfloor \right) + (0+0) \\
&\leq \frac{p^n}{p} + \frac{p^n}{p^2} + \cdots + \frac{p^n}{p^{n-1}} + 0 \\
&= v_p(p!) - 1 \implies v_p(k!) + v_p((p^n-k)!) < v_p(p!)
\end{aligned}$$

Thus, we have that there are more powers of p in the numerator than the denominator, so $\binom{p^n}{k}$ is a multiple of p.

Our original equation, then becomes the following:

$$\begin{aligned}
(x+y)^q &= x^q + \binom{q}{1}x^{q-1}y + \binom{q}{2}x^{q-2}y^2 + \cdots + \binom{q}{q-1}xy^{q-1} + y^q \\
&= x^q + y^q && \pmod{p} \\
&= x + y \\
&\implies (x+y) \in F
\end{aligned}$$

- Additive Inverse: Let $x \in F$. Then, we have the following:

$$\begin{aligned}
0 &= 0^q \\
&= (x + (-x))^q \\
&= x^q + (-x)^q && \text{(By the same method shown above)} \\
&= x + (-x)^q \\
&\implies (-x)^q = (-x) \\
&\implies (-x) \in F
\end{aligned}$$

Thus, F is a field. □

Lemma 2

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 4, 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 $\mathbb{F}_q$. □

Let's consider the field $\mathbb{F}_q$ when $q = p^2$. We know that every element in $\mathbb{F}_q$ is a root of the polynomial $x^q - x$. We claim that the roots of every quadratic in $\mathbb{Z}_p[x]$ is in $\mathbb{F}_q$.
To prove this, we $\forall x \in \mathbb{F}_q, x \neq 0$ have the following:

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

Similar to in $\mathbb{Z}_p$, we know that if x is a quadratic residue $\in \mathbb{F}_q$, then $x^{\frac{q-1}{2}} = 1$. Thus, we have $x^{\frac{p^2-1}{2}} - 1 \iff x$ is a quadratic residue. Consider $a \in \mathbb{U}_p \subseteq \mathbb{F}_p$. We know that $a^{\frac{p-1}{2}} = \pm 1 \pmod p$. Thus, we have

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

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 $\mathbb{F}_p$. Else, if $b^2 - 4ac \in U_p$, then it is a quadratic residue in $\mathbb{F}_p$, so there exists two element in $\mathbb{F}_p$ that equal:

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

Thus, every root of a quadratic is in $\mathbb{F}_p$.
For our proof, that means $\lambda_1, \lambda_2 \in \mathbb{F}_p$. Thus, for λ_1, λ_2 both we have the following:

$$\begin{aligned} \lambda^q &= \lambda \\ \lambda^{q-1} &= 1 \\ \lambda^{(p^2-1)} &= 1 \end{aligned}$$

Thus, if there is an FLF has for some $a+1 \in N$, $\lambda_1^{a+1} = \lambda_1, \lambda_2^{a+1} = \lambda_2$, then we that there are a elements in the cycle of that FLF on $\mathbb{P}_p$ because the $a+1$th element is equivalent the the 1st element. We have $\lambda_1^a = 1$ and $\lambda_2^a = 1 \implies a \mid (p^2 - 1)$.

3.3 Non-Diagonalizable Matrices

Lemma 3

Claim: *For a given fractional linear functions, then one of two possibilities holds:*

1. *There are either* 0, 1, *or* 2 *inputs that cycle to themselves in any given fractional linear function.*

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

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

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. □

Previously, we assumed that $f(x) = \frac{ax+b}{cx+d}$ could be written as a diagonalizable matrix. However, this isn't always the case. If a matrix has two distinct eigenvalues, then it is always diagonalizable. However, if it has a repeated eigenvalue (i.e. the quadratic used to generate λ_1 and λ_2 has a double root), then the matrix is not necessarily diagonalizable.

Thus, if we have $f(x) = \frac{ax+b}{cx+d}$, which is represented by the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is non-diagonalizable, then we have that the discriminant of $\lambda^2-(d+a)\lambda+ad-bc$ is 0.

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

Consider the quadratic from Lemma 3, $cn^2+(d-a)n-b=0$. The discriminant of that quadratic is the following:

$$(d-a)^2+4bc$$

which is the same as the discriminant of the quadratic for λ. Thus, if $\lambda^2-(d+a)\lambda+ad-bc$ has a double root, $cn^2+(d-a)n-b$ also has a double root. It follows that if the matrix representation of $f(x)$ is non-diagonalizable, then there exists exactly one one-cycle on $f(x)$.

By our conjecture, the remaining p elements must all have the same cycle length because there can only be 2 distinct cycle lengths for any given FLF. Since p is prime, the only possibility is that these p elements are all in the same cycle with cycle length p.

3.4 Counting Fractional Linear Functions on $\mathbb{P}_p$

There are two ways to consider this question: with simplification or without simplification. Without simplification, we would consider each fractional linear function with different coefficients as distinct functions. With simplification, we would reduce each fraction linear function so that there are no common factors between the coefficients a, b, c, d.

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

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

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

Proof. Let

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

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 $\circ$.

Definition 11: 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 12: 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

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

.

Theorem 1: 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 $x \in \mathbb{Z}_p$.

WLOG, 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

$$|\text{orb}(x)| = p + 1.$$

Now, we consider the stabilizer of 0, which is the set of all FLFs which map 0 to 0. Take an arbitrary FLF $f(x)$ in the stabilizer of 0,

$$\begin{aligned} f(x) &= \frac{ax+b}{cx+d} \\ f(0) &= \frac{a \cdot 0 + b}{c \cdot 0 + d} = 0 \\ f(0) &= \frac{b}{d} = 0 \\ \implies b &= 0 \end{aligned}$$

We know that $ad - bc \neq 0 \mod p$. Since $b = 0$, we have $ab \neq 0 \implies a \neq 0, b \neq 0$. 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. Since there are p elements in $\mathbb{Z}_p$, we have that there are p choices for c and $p-1$ choices for a, d, and 1 choice for b giving us

$$(p-1)^2 \cdot p \cdot 1$$

total functions in the stabilizer of 0. In other words,

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

By Orbit-Stabilizer Theorem, we have

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

□

This raises the question, if we simplify all FLFs to their simplest form, how many Fractional Linear Functions would there be on $\mathbb{P}_p$?
To answer this, we first need to provide a formal definition of a "simplified" FLF.

Definition 13: 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* $b = 1$.

We can show that every fractional linear function on $\mathbb{P}_p$ can be written in simplest form without altering the inputs or outputs of the function. 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, since $a \in \mathbb{Z}_p, a \neq 0$, a has a multiplicative inverse a^{-1} in $\mathbb{Z}_p$. We have:

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

Since a^{-1} is in $\mathbb{Z}_p$, $b \cdot a^{-1}, c \cdot a^{-1}, d \cdot a^{-1} \in \mathbb{Z}_p$. Thus

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

is a fractional linear function equivalent to $f(x)$ which is in simplest form.
By the process above, we can formalize a lemma.

Lemma 4: Equivalent FLFs

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.*

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

Proof. Let

$$H = \left\{ \frac{ax+b}{cx+d} \mid a,b,c,d \in \mathbb{Z}_p, a = 0,1, ad-bc \neq 0 \right\}.$$

Then, we claim H is a group under $\circ$. We can verify this by checking that H satisfies the group axioms:

1. Associativity: The composition of functions is associative, so H is associative under $\circ$
2. Identity: The FLF $\frac{x+0}{0x+1} = x$, which is in H because $a = 1$, is the identity, because if you compose any function with x and it will equal itself
3. Inverses: By 2.2 there exists an unique inverse f^{-1} to every FLF f. We can simplify f^{-1} (if it is not already in simplest form) by multiplying the numerator and denominator by a^{-1} to get an inverse in H.
4. Closure: By 2.1, given two FLFs g, f, we know $g \circ f$ is always another FLF. We can reduce $g \circ f$ to simplest form (if it is not already in simplest form) by multiplying the numerator and denominator by a^{-1} to get a FLF in H thus, H is closed under $\circ$.

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 $f(x) = x$. We have:

$$\begin{aligned} f(x) &= \frac{ax+b}{cx+d} \\ &= \frac{0x+b}{0c+d} \\ \implies b &= 0 \end{aligned}$$

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. 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:

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

□

4 Looping Functions

Definition 14: Looping Function and Order

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

Theorem 2: Cycle Lengths

If f has order n then the possible cycle lengths of elements in $\mathbb{P}_p$ are divisors of n.

Proof: For the sake of contradiction, assume that for element b, f has a cycle length c that is not a divisor of n. Thus $n = cq + r$ where $r < c$. Then $f^k(b) \neq b$ for all $k \leq c$, but $f^n(b) = f^{cq}(f^r(b)) = f^r(b) = b$, but this contradicts our previous statement. Therefore, c must divide n.

Orbit diagram for $f(x) = \frac{x-1}{x+1}$ in $\mathbb{P}_{11}$:

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

Orbit diagram for $f(x) = \frac{x-1}{x+1}$ in $\mathbb{P}_{13}$:

$$\begin{array}{cccccccc} 0 & \longrightarrow & 12 & 2 \longrightarrow 9 & 3 & \longrightarrow 7 & & \\ \uparrow & & \downarrow & \uparrow \quad \downarrow & \uparrow & \quad \downarrow & & \\ 1 & \longleftarrow & \infty & 10 \longleftarrow 6 & 11 & \longleftarrow 4 & 5 & 8 \end{array}$$

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

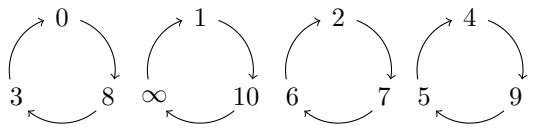
$$f^4(x) = -\frac{\frac{x-1}{x+1} - 1}{\frac{x-1}{x+1} + 1} = x.$$

So f has an order of 4.

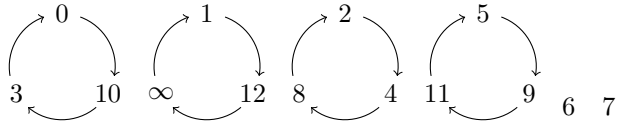
Thus f may "loop" back to itself after 4 times, 2 times, or 1 time. Note that if f looped back to itself in 2 times, then $x = f^2(x)$, meaning that $x = -x$. This may only happen if $x = 0$, but because $f(f(x)) = f(-1) = \infty \neq 0$, a loop of length 2 is not possible.
Furthermore, if $x = \frac{x-1}{x+1}$, then $x^2 + x = x - 1$, so $x^2 + 1 = 0$ which has no solutions in $\mathbb{P}_p$ when $p = 4k + 3$ as -1 is not a quadratic residue in p. Thus, there exist no loops of length 1 either. 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 $p = 4k + 3$.

Meanwhile, if $p = 4k + 1$, there exists two solutions to $x^2 \equiv -1 \pmod 4$, so there are 2 loops of length 1. 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.

Orbit diagram for $f(x) = \frac{x-3}{x+1}$ in $\mathbb{P}_{11}$:



Orbit diagram for $f(x) = \frac{x-3}{x+1}$ in $\mathbb{P}_{13}$:



$\frac{x-3}{x+1}$ 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 $p = 1 \pmod 3$, 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. Now if $p = 3k-1$, then all $p+1 = 3k$ elements in $\mathbb{P}_p$ will be part of loops with length 3 for a total of $2k$ loops.

4.1 Observations of $\frac{x-a}{x+1}$

Let $f(x) = \frac{x-a}{x+1}$. Then we can compose f multiple times to see some patterns:

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

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

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

$$f^4(x) = \frac{(1+(-6+a)a)x + a(-4+4a)}{(4-4a)x + (1+(-6+a)a}$$

$$f^5(x) = \frac{(a(5a-10)+1)x + a((10-a)a-5)}{((a-10)a+5)x + a(5a-10)+1}$$

$$f^6(x) = \frac{(a((a-15)a+15)-1)x + a(a(6a-20)+6)}{((20-6a)a-6)x + a((a-15)a+15)-1}$$

The clearest pattern is in how each $f^n(x)$ is in the form $\frac{cx-da}{dx+c}$. This can be proven with induction. Our base case is $c = 1, d = 1$ gives $f^1(x)$. Now assume that $f^k(x) = \frac{cx-da}{dx+c}$ for some c, d. Then $f^{k+1}(x) = \frac{f^k(x)-a}{f^k(x)+1} = \frac{\frac{cx-da}{dx+c}-a}{\frac{cx-da}{dx+c}+1}$ which equals

$$\frac{cx-da-adx-ac}{cx-da+dx+c} = \frac{(c-ad)x - a(c+d)}{(c+d)x + (c-ad)}.$$

This also fits the form, so our induction is complete.

f is a looping function when d becomes 0. For instance, the d in $f^4(x)$ is $4(-1+a)$, and $4(-1+a) = 0$ when $a = 1$, which is why $\frac{x-1}{x+1}$ has a loop of length 4.

5 Extensions

5.1 Determining an FLF

Claim: 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 Lemma 1, we also know that the fractional linear functions differ by multiplications of $u \in \mathbb{U}_p$, 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:

$$u_3 \begin{bmatrix} e_5 \\ e_6 \end{bmatrix} = \begin{bmatrix} e_1 & e_3 \\ e_2 & e_4 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$
$$\text{so, } \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \frac{u_3}{e_1 e_4 - e_2 e_3} \begin{bmatrix} e_4 & -e_3 \\ -e_2 & e_1 \end{bmatrix} \begin{bmatrix} e_5 \\ e_6 \end{bmatrix}$$
$$\implies u_1 = \frac{u_3}{e_1 e_4 - e_2 e_3}(e_4 e_5 - e_3 e_6)$$
$$u_2 = \frac{u_3}{e_1 e_4 - e_2 e_3}(e_1 e_6 - e_2 e_5)$$
$$\text{and we assume}$$
$$u_3 = e_1 e_4 - e_2 e_3$$
$$\text{for the sake of canceling fractions.}$$

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. □

Claim: 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

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

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.

□

5.2 Continued Fractions

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

$$\begin{aligned} f(x) = f^1(x) &= \frac{1}{a+x} \\ f(f(x)) = f^2(x) &= \frac{1}{a+\frac{1}{a+x}} \\ f(f(f(x))) = f^3(x) &= \frac{1}{a+\frac{1}{a+\frac{1}{a+x}}} \\ &\vdots \end{aligned}$$

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

$$\begin{aligned} f(x) = f^1(x) &= \frac{1}{a+x} \\ f(f(x)) = f^2(x) &= \frac{x+a}{ax+(a^2+1)} \\ f(f(f(x))) = f^3(x) &= \frac{ax+(a^2+1)}{(a^2+1)x+(a^3+2a)} \\ &\vdots \end{aligned}$$

If we set $x = 0$, these results are continued fractions.

$$\begin{aligned} f^1(0) &= \frac{1}{a} = \frac{P_1}{Q_1} \\ f^2(0) &= \frac{a}{a^2+1} = \frac{P_2}{Q_2} \\ f^3(0) &= \frac{a^2+1}{a^3+2a} = \frac{P_3}{Q_3} \\ &\vdots \end{aligned}$$

In fact, they are convergents of the infinite continued fraction $y = \cfrac{1}{a+\cfrac{1}{a+\cfrac{1}{a+\cdots}}}$. Note that $Q_n = P_{n+1}$.

We can prove this statement with strong induction. Our base case is done in the first few examples above. Now assume that $Q_k = P_{k+1}$ for all $k \leq n-1$. By the "magic box" recursive formula, $Q_n = a \cdot Q_{n-1} + P_{n-1} = a \cdot P_n + P_{n-1} = P_{n+1}$. So our induction is complete.

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

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

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

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

We disregard the negative solution of the quadratic as the continued fractions is evidently positive. Note how the coefficients in the FLF's of each level of composition show up in the continued fraction convergents. We see that

$$f^1(x) = \frac{P_0 x + P_1}{P_1 x + P_2},$$

$$f^2(x) = \frac{P_1 x + P_2}{P_2 x + P_3}, \dots$$

such that in general

$$f^n(x) = \frac{P_{n-1} x + P_n}{P_n x + P_{n+1}}.$$

This can once again 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

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

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 will proceed with induction. Our base case is satisfied because

$$\begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix}$$

has consists of $\frac{0}{1}$ and $\frac{1}{a_0}$ which are convergents. Now assume

$$\begin{bmatrix} P_{k-1} & P_k \\ Q_{k-1} & Q_k \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & a_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_2 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & a_k \end{bmatrix}.$$

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 $\begin{bmatrix} P_k & P_{k+1} \\ Q_k & Q_{k+1} \end{bmatrix}$.

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

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

□

6 Conclusion

In this paper, we have investigated fractional linear functions taken over $\mathbb{P}_p$ and how they correspond to 2×2 matrices. We've noted how this matrix representation of fractional linear functions can provide a helpful way of understanding compositions/inverses. Using matrix diagonalization and splitting fields, we've proved that every FLF on $\mathbb{P}_p$ has cycle lengths that either divide $p^2 - 1$ or are exactly p. We've also proved that there are exactly $p(p-1)^2(p+1)$ FLFs on $\mathbb{P}_p$ without simplification and exactly $p(p-1)(p+1)$ FLFs on $\mathbb{P}_p$ with simplification. Along with other lemmas from our observations, we proved that a fractional linear function can be uniquely determined by three values. We also explored the similarities and applications of fractional linear functions to continued fractions and observed a relationship with quadratic residues through looping functions.

There is still a lot to be discovered about Fractional Linear Functions. For instance, some conjectures we were not able to prove in this paper are:

- 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.
- A stronger version of our cycle length conjecture: the cycle length of an FLF on $\mathbb{P}_p$ divides $p-1$ or $p+1$
- How to effectively find cycle lengths

Additionally, in this paper, we only investigated fractional linear functions defined over $\mathbb{P}_p$. However, fractional linear functions $f(x) = \frac{ax+b}{cx+d}$ with coefficients $a, b, c, d \in \mathbb{R}$ also pose an interesting question. They define a function $f : \mathbb{P}_{\mathbb{R}} \mapsto \mathbb{P}_{\mathbb{R}}$ and also a function $f : \mathbb{P}_{\mathbb{C}} \mapsto \mathbb{P}_{\mathbb{C}}$, where $\mathbb{P}_{\mathbb{R}}$ denotes $\mathbb{R} \cup \{\infty\}$ and $\mathbb{P}_{\mathbb{C}}$ denotes $\mathbb{C} \cup \{\infty\}$.

If we consider these fractional linear functions as linear transformations, we can find some very interesting applications to hyperbolic geometry. In particular, we have that if the determinant of the fractional linear function is positive, in other words, if $ad - bc > 0$, then the linear transformation f preserves the upper half of the complex plane. In the upper half-plane, we could consider fractional linear transformations with positive discriminant as orientation-preserving isometries. An investigation of this topic could lead to some very interesting geometric tools and results.