Hahn THE Lheem's (fluffy) Fractional Linear Functions
PROMYS 2022 Exploration Lab

Hahn Lheem (Counselor), Andrew Tung, Ivan Wong, Reese Long, and Michael Yang

(Dated: July & August 2022)

In this exploration lab, we investigated the cycle structure of fractional linear functions with coefficients in $\mathbb{Z}_p$ acting on $\mathbb{P}_p$. It has previously been suggested that the action of a fractional linear function creates cycles on the elements of $\mathbb{P}_p$. In this paper, a number of important properties of these cycle structures are established, such as the fact that every cycle of length at least 2 has the same length for $p \geq 5$. We also introduce the notion of a determinant of a fractional linear f unction and demonstrate its connection to properties of the cycle structure, as well as using group theory to use and classify results of combinatorial nature. We also state a conjecture about the full characterization of all cycle structures of fractional linear functions modulo p and prove it for certain classes of primes.

I. BEGINNINGS OF THE HAHN ERA

We begin with a few basic facts which have been suggested in the description of the topic. For the remainder of this paper, we consider fractional linear functions $f(x) = \frac{ax+b}{cx+d}$ where $ad - bc \neq 0$.

Theorem I.1 (cycles exist)**.** *Every function $f(x) = \frac{ax+b}{cx+d}$ with $ad-bc \neq 0$ induces a permutation on $\mathbb{P}_p$. This permutation can be partitioned into disjoint cycles.*

Proof. Every function of this form is invertible with inverse $\frac{-dx+b}{cx-a}$. Therefore, it maps $\mathbb{P}_p$ to itself bijectively, so it creates a permutation. Cycles exist because every permutation can be partitioned into disjoint cycles. □

Proposition I.2 (number of functions)**.** *The number of distinct fractional linear functions mod p with $ad - bc \neq 0$ is $p^3 - p$. (Here we consider the action of the function rather than the tuple (a, b, c, d).)*

Proof. Observe that every function corresponds to $p - 1$ distinct tuples (a, b, c, d), since multiplying all the coefficients by any constant $1, 2, \ldots, p - 1$ results in the same function. So it suffices to count tuples (a, b, c, d) with $ad - bc \neq 0$ and then divide by $p - 1$.

To do this, we use complementary counting. There are p^4 tuples total. We then count all functions with determinant 0. If all of a, b, c, d are nonzero, then there are $(p - 1)^3$ functions, since three of the entries determine the fourth one. If exactly three of a, b, c, d are nonzero, then this is impossible because two remaining entries must multiply to 0. If exactly two of a, b, c, d are nonzero, then there are 4 possible configurations for the 0's, after which the nonzero elements can be chosen arbitrarily, giving $4(p-1)^2$. If one of a, b, c, d are nonzero, then there are again 4 configurations of the 0 entries and the nonzero element can be chose arbitrarily, giving $4(p-1)$. Finally if none of a, b, c, d are nonzero, we have 1 possibility. This gives

$$\frac{p^4 - (p-1)^3 - 4(p-1)^2 - 4(p-1) - 1}{p-1} = p^3 - p$$

□

Proposition I.3 (0, 1, ∞ determine a FLF)**.** *A FLF $f(x)$ over a $\mathbb{P}_p$ for a fixed p is uniquely determined by $f(0)$, $f(1)$, and $f(\infty)$.*

Proof. Let $f(0) = \frac{b}{d} = r$, $f(1) = \frac{a+b}{c+d} = s$, and $f(\infty) = \frac{a}{c} = t$. r, s, t are fixed.

Since we consider FLFs to be equivalent under scaling, we can write any FLF to be $c = 0$ or $c = 1$.

Case 1: $t = \infty$
This means that $c = 0$. The FLF is $\frac{ax+b}{d}$. Then by scaling we can just multiply everything by d^{-1} to get some equivalent FLF with $d = 1$. Also $d \neq 0$ because then $ad - bc = 0$, which is not allowed. So let $d = 1$

$s = a + b$, and $r = b$. This uniquely determines b and a, so the FLF is determined.

Case 2: $t \neq \infty$
Here we can just count for when $c = 1$. This gives $a = t$.

Now we do casework on the values of r and s.

Case 2a: $r, s \neq \infty$
$b = dr$, and $a + b = s(1 + d)$. So $t + dr = s(1 + d)$, meaning $\frac{t-s}{s-r} = d$. $s \neq r$, so this is allowed. So d is uniquely determined, meaning that now b is also uniquely determined.

Case 2b: $r = \infty$
This means $d = 0$, $a + b = s$. This uniquely determines $b = s - t$.

Case 2c: $s = \infty$
This means $1 + d = 0$ and $b = dr$. This fixes $d = -1$, and then b is also determined.

These are all the cases on r, s, t, meaning these are all the possible FLFs. Therefore, a FLF can be uniquely determined by $f(0), f(1)$ and $f(\infty)$. □

This gives another way to count the number of FLFs on $\mathbb{P}_p$. We have $p + 1$ choices for what $f(0)$ can be, p choices for what $f(1)$ can be, and $p - 1$ choices for what $f(\infty)$ can be, so this gives $(p + 1)(p)(p - 1) = p^3 - p$ FLFs in total.

II. HAHN'S ISOMORPHISM

Lheemma II.1. *The set of fractional linear functions with coefficients in $\mathbb{F}_p$ forms a group under composition, denoted $FL(\mathbb{F}_p)$.*

Proof. We must prove that the operation of composition is associative and that fractional linear functions are both closed under the operation and have an inverse.

It is well known that function composition is an associative operation. Additionally, we have already shown that the composition of any two fractional linear functions gives another fractional linear function as well as the existence of a unique inverse function for every element. Hence, the set of all fractional linear functions with coefficients in $\mathbb{F}_p$ forms a group under composition. □

Theorem II.2. *We have*

$$FL(\mathbb{F}_p) \cong GL_2(\mathbb{F}_p)/\sim$$

where the equivalence relation $\sim$ is defined by $A \sim B$ if and only if $A = \lambda B$ for some nonzero λ.

Proof. We first need to prove that the relation in the problem is reflexive an equivalence relation. It is symmetric since $A = 1 \cdot A$. It is symmetric since $A = \lambda B$ means $B = \lambda^{-1} A$ (and inverses always exist mod p). It is transitive since $A = \lambda_1 B$ and $B = \lambda_2 C$ means $A = (\lambda_1 \lambda_2) C$.

We also have to prove that the operation on $GL_2(\mathbb{F}_p)/\sim$ is well defined. Let A, A' be from the same equivalence class, and let B be another arbitrary matrix. We must prove $AB \sim A'B$. Since $A \sim A'$, $A = \lambda A'$, so $AB = \lambda A'B$, as desired.

Now we must construct an isomorphism. Define the isomorphism $\phi : FL(\mathbb{F}_p) \to GL_2(\mathbb{F}_p)/\sim$ by

$$\phi\left(\frac{ax+b}{cx+d}\right) := \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]$$

where the brackets denote the equivalence class in $GL_2(\mathbb{F}_p)$ containing $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

We first prove that this is a homomorphism. We have

$$\phi\left(\frac{ax+b}{cx+d} \circ \frac{ex+f}{gx+h}\right) = \phi\left(\frac{(ae+bg)x + (af+bh)}{(ce+dg)x + (cf+dh)}\right) = \left[\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\right] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]\left[\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right]$$

To prove this is bijective, suppose $f(x) = \frac{ax+b}{cx+d}$ and $g(x) = \frac{ex+f}{gx+h}$ are such that $\phi(f) = \phi(g)$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ for some λ, since they must belong to the same equivalence class. This means that f and g are the same function, since $\frac{ax+b}{cx+d} = \frac{\lambda ex + \lambda f}{\lambda gx + \lambda h} = \frac{ex+f}{gx+h}$. □

From now on, we will consider the case of FLFs with $c = 0$ or $c = 1$. This covers the entirety of unique FLFs up to scaling, so the only condition we have to worry about is nonzero determinant once we stipulate that c must equal one of these two values.

Corollary II.3. *The order of any fractional linear function (i.e. the smallest $n \geq 1$ such that $f^n(x) = x$ for all x) divides $p^3 - p$.*

Proof. This follows from Lagrange's Theorem and the count of the total number of FLFs. □

Now that we've established the idea of scaling, we will define a notion of determinant that is consistent of this idea.

Definition II.4. When considering fractional linear functions up to scaling in $\mathbb{P}_p$, we will consider the following collection of functions $\frac{ax+b}{cx+d}$:

- The functions for which $c = 0$ and $a = 1$;
- The functions for which $c = 1$ and for which a, b, and d are allowed to take any values from 0 to $p - 1$ (inclusive) with the constraint that $ad \not\equiv b \pmod{p}$.

Now, we define the ***determinant*** of a fractional linear function $\frac{ax+b}{cx+d}$ for $a, b, c, d \in \mathbb{P}_p$ as $ad - bc$, where $\frac{ax+b}{cx+d}$ is in this form.

The choice that we made to consider this particular class of functions is not unique; however, we will be talking about the determinant in this sense moving forward.

III. ANALYZING THE FIBONACCI USING FLFS AND CONTINUED FRACTIONS

We notice that special FLFs, notably those of the form $f(x) = \frac{1}{x+d}$, give ways to represent the Fibonacci numbers and other recursive sequences.

We particularly examine $f(x) = \frac{1}{x+1}$ and its relation to F_n, which denotes the nth Fibonacci number where $F_1 = F_2 = 1$.

Theorem III.1. *Given k is the smallest natural number satisfying $p \mid F_k$, then the cycle length of $f(x) = \frac{1}{x+1}$ in $\mathbb{P}_p$ divides k.*

Proof. We consider what happens when we compose f with itself, in which we get $f^2(x) = \frac{1}{1+\frac{1}{x+1}}$. Each time we compose f with itself, it adds another layer to the continued fraction, so we can observe that

$$f^n(x) = [0; \overbrace{1, 1, 1, ..., 1}^{n-1}, x+1]$$

Then, using properties of continued fractions, we can calculate the convergents of $f^n(x)$ to be
$\{\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{3}{5}, ..., \frac{F_{n-1}}{F_n}, \frac{F_{n-1}(x+1)+F_{n-2}}{F_n(x+1)+F_{n-2}}\}$, where we find that

$$\begin{aligned} f^n(x) &= \frac{F_{n-1}(x+1) + F_{n-2}}{F_n(x+1) + F_{n-2}} \\ &= \frac{F_{n-1}x + F_n}{F_n x + F_{n+1}} \end{aligned}$$

Clearly, when $p \mid F_k$, then $f^k(x) = \frac{F_{k-1}x+F_k}{F_k x+F_{n+1}} \equiv \frac{F_{k-1}x}{F_{k+1}} \pmod{p}$. Since we know $F_{k-1} + F_k = F_{k+1}$, we have that $F_{k-1} \equiv F_k \pmod{p}$. Hence, $f^k(x) \equiv \frac{F_{k-1}x}{F_{k+1}} \equiv x \pmod{p}$, so $f^k(x) = x$ in $\mathbb{P}_1$. It follows that all cycle lengths in $f(x)$ must divide k.

□

Corollary III.2. *Given k is the smallest natural number satisfying that rational prime $p \mid F_k$, then $k \leq p + 1$.*

We note that this approach to the Fibonacci numbers can also be applied to other similar recursive sequences, such as those defined by $S_n = mS_{n-1} + S_{n-2}$ which we can model using the convergents of the continued fraction generated by $f^n(x)$ where $f(x) = \frac{1}{x+m}$.

It follows from the same reasoning as the proof above that

Theorem III.3. *Given k is the smallest natural number satisfying that rational prime $p \mid S_k$, then $k \leq p + 1$.*

It is also not unreasonable to generalize even further and lift restrictions on a, b, c in order to analyze more general recursive sequences using FLFs. This opens several new avenues of exploration and relationships with other areas of mathematics.

IV. HAHN'S LITTLE THEOREM

Theorem IV.1 (Hahn's Little Theorem)**.** *Every cycle of length at least* 3 *has the same length.*

Proof. Consider the number of solutions to $f^n(x) = x$. Let n be the smallest such value where $f^n(x) = x$ for 3 or more values of x. Then, we know that $f^2(x)$ is also a fractional linear function, and if it is non-trivial, then $f^2(x) = x$ gives a quadratic polynomial that has at most 2 solutions mod p. Hence, since $f^n(x) = x$ for at least 3 values of x, $f^n(x)$ must in fact be the trivial fractional linear function $f^n(x) = \frac{x+0}{0+1}$, meaning that $f^n(x) = x$ holds for all values of x.

As such, the length of every cycle must divide n. Since n is the smallest cycle length greater than 3, then any cycle length greater than 3 must be both greater than or equal to n and divide n, implying that an cycle of length at least 3 must have exactly the same length: n. □

Proposition IV.2 (Small cycles)**.** *For $p \geq 5$, the only possible cycle lengths less than* 3 *are either: no cycles, one fixed point, two fixed points, one two-cycle, all fixed points, or all two-cycles.*

Proof. First, notice that the function $f(x) = x$ has all fixed points. Henceforth, assume that our function is not x.

We know that the cycle length of all cycles outside of two fixed points or a two-cycle, denoted k, must divide $p^3 - p = p(p-1)(p+1)$. Additionally, since the cycle lengths are each the same length, the k must similarly divide one of $\{p+1, p, p-1, p-2, p-3\}$, corresponding to the number of elements contained in the one or two-cycles.

Clearly, $k \mid p+1$, $k \mid p$, and $k \mid p-1$ is consistent with $k \mid p^3 - p$. However, $\gcd(p-2, p^3-p) = \gcd(p-2, 6) = 1$ for all prime p except $p = 5$; however, to discount 3 elements from when $p = 5$ to have $k \mid 3$, then there must be a 2-cycle and $k = 3$. This is impossible since $2 \nmid 3$. Similarly, $\gcd(p-3, p^3-p) = \gcd(p-3, 24) = 1$ for all prime p except, again, $p = 5$. However, we cannot find two fixed points and two different 2-cycles for much the same reason.

As such, for all p, there can be no small cycles, one fixed point, two fixed points, one two-cycle, all fixed points, or all two-cycles. □

V. ADDITIVE AND MULTIPLICATIVE HAHN LHEEMMAS

Lheemma V.1 (Additive Hahn Lheemma)**.** *The permutations induced by $f(x)$ and $g(x) = f(x) + 1$ have the same parity of the number of cycles.*

Proof. Suppose f has permutation σ_f and g has permutation σ_g. Since the parity of a permutation on $p+1$ elements is $(-1)^{(p+1)-c}$, where c is the number of cycles, it suffices to show that σ_f and σ_g have the same parity.

Observe that $g(x) = f(x)+1$ is equivalent to multiplying on the left by the p-cycle $(0\ 1\ \ldots\ p-1)$. This cycle has parity $p-1$, which is even, so σ_f and $\sigma_g = (0\ 1\ \ldots\ p-1)\sigma_f$ must have the same parity. □

Lheemma V.2 (Multiplicative Hahn Lheemma)**.** *If p is $1 \mod 4$, then f and $1/f$ have the same parity of the number of cycles. Otherwise, they have opposite parity.*

Proof. The proof is exactly the same as that of the Additive Hahn Lemma, except that the transformation $f \to 1/f$ now corresponds to multiplying on the left by the permutation that switches x and x^{-1}. This permutation is $(0\ \infty)(2\ 2^{-1})\ldots$, which is composed of $\frac{p-1}{2}$ transpositions. This is even if p is 1 mod 4, in which case it does not change the parity. Otherwise it is odd, so it switches the parity of the number of cycles. □

Lheemma V.3. *The permutations induced by $f(x)$ and $g(x) = \frac{f(x)}{f(x)+1}$ have the same parity of the number of cycles.*

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

If p is 1 (mod 4), then $\frac{1}{1+\frac{1}{f(x)}}$ has the same parity as $1 + \frac{1}{f(x)}$ which has the same parity as $\frac{1}{f(x)}$ which has the same parity as $f(x)$.

If p is not, then $\frac{1}{1+\frac{1}{f(x)}}$ has different parity as $1 + \frac{1}{f(x)}$, which has the same parity as $\frac{1}{f(x)}$, which is the opposite parity as $f(x)$, but the opposite of the opposite parity is the same, so $f(x)$ has the same parity as $\frac{1}{1+\frac{1}{f(x)}}$. □

VI. THE HAHN TREES

In this section, consider the determinant of some expression to be determined by its tuple of coefficients (a, b, c, d). Let the determinant of $\frac{ax+b}{cx+d}$ be $ad - bc$.

Starting from a root of $\frac{1x+0}{0x+1}$, construct a binary tree so that the left child of $\frac{ax+b}{cx+d}$ is $\frac{(a+c)x+(b+d)}{cx+d}$, and the right child is $\frac{ax+b}{(a+c)x+(b+d)}$.

The determinant of $\frac{1x+0}{0x+1}$ is 1.

For any function $\frac{ax+b}{cx+d}$ with $ad - bc = 1$, $\frac{(a+c)x+(b+d)}{cx+d}$ has determinant $d(a + c) - c(b + d) = ad - bc = 1$. $\frac{ax+b}{(a+c)x+(b+d)}$ also has determinant $a(b + d) - b(a + c) = ad - bc = 1$. In matrix terms, this is because adding one row to another does not change the determinant.

Notice that these are the transformations $f(x) + 1$ and $\frac{f(x)}{f(x)+1}$.

Also, even though we are using the integers without modding anything, if we can get all the fractions with determinant 1 in the tree, all fractions with determinant 1 with coefficients in $\mathbb{Z}_p$ will also be in the tree.

Lheemma VI.1. *All fractional linear functions in the tree have determinant one.*

Proof. Any fractional linear function in Hahn's tree of determinant one is made up of composing transformations that preserve determinant, therefore all the fractional linear functions in the tree have determinant one. □

Lheemma VI.2. *All fractional linear functions of determinant one are in the tree.*

Proof. Any FLF of determinant 1 either has no parents, or is descended from something that has no parents.

If $a \geq c$ and $b \geq d$, then it would be a left child of $\frac{(a-c)x+(b-d)}{cx+d}$. Also, if $a \leq c$ and $b \leq d$, then it would be a right child of $\frac{ax+b}{(c-a)x+(d-b)}$.

Assume $\frac{ax+b}{cx+d}$ with determinant 1 is not in the tree.

Case 1: We want $a \geq c$ or $d \geq b$, but not $a = c$ or $b = d$. So we want $a \geq c+1$ or $d \geq b+1$ (since a, b, c, d are integers, so $ad - bc \geq (c+1)(b+1) - bc = b + c + 1$. So $1 \geq b + c + 1$, which means $(a, b, c, d) = (1, 0, 0, 1)$.

Case 2: $c \geq a + 1$ and $b \geq d + 1$, so $ad - bc \leq (c-1)(b-1) - bc = 1 - b - c$. This means $b + c + 1 \leq 1$ again.

This means that any fraction with determinant 1 is descended from the only FLF with determinant 1 without a parent, which is just $\frac{1x+0}{0x+1}$. □

Proposition VI.3. *A FLF is in Hahn's Tree if and only if it has determinant 1.*

Proof. This follows directly from the two previous Lheemmas. □

So all linear fractional functions of determinant 1 can be composed of $x + 1$ and $\frac{x}{x+1}$'s, so by the Hahn Lemmas, since x, $x + 1$, and $\frac{x}{x+1}$ have even number of cycles, all linear fractional functions of determinant 1 have an even number of cycles.

Take a fractional linear function $\frac{ax+b}{cx+d}$. Now multiply numerator and denominator by λ. We get that the fraction stays the same because we multiplied by 1, so there are still the same number of cycles. But the determinant goes to λ^2, a QR.

Definition VI.4. A QRDFLF is a fractional linear function that has a determinant that is a quadratic residue.

There will be more on QRDFLFs and cycle lengths in the next section.

A. Hahn Trees of Other Determinants

We can use the same ideas as in determinant 1 to construct trees of other determinant FLFs.

Using the same method as in the Hahn Tree of determinant 1, we can generalize for any function with determinant D. The fractions without a parent are the ones with b, c satisfy $D = ad - bc$, and $D \leq b + c + 1$.

We can ignore $D \geq 1 - b - c$ means $b + c \leq 1 - D$, which is negative when $D > 1$.

So the number of trees needed to contain all of the FLFs of determinant D is the number of tuples (a, b, c, d) that satisfy these inequalities and the determinant equation.

VII. HAHN'S PARITY THEOREM

Lheemma VII.1 (Hahn's Transformation Lemma)**.** *Given any $f = \frac{ax+b}{cx+d}$, with $ad - bc \neq 0$, let*

$$g(x) = \begin{cases} \frac{a^2}{ad-bc}x & \text{if } a \neq 0 \\ \frac{b}{cx} & \text{if } a = 0 \end{cases}$$

Then g has the same parity of the number of cycles as f.

Proof. We transform f into g using the operations from the Additive and Multiplicative Hahn Lemmas. Essentially this is just row-reduction of the corresponding matrix, so for this proof we speak in terms of matrices.

Observe that the operation $f \to \frac{1}{f}$ is equivalent to swapping the rows of the corresponding matrices, and $f \to f+1$ is equivalent to adding the second row to the first row. Adding the first row to the second row can be achieved by the transformation $f \to \frac{f}{f+1}$, which is just $\frac{1}{1+\frac{1}{f}}$. Observe that this does not change the parity of the number of cycles, since the reciprocal operation is performed an even number of times (twice).

If $a \neq 0$, we have the following steps:

$$\begin{aligned}
\begin{pmatrix} a & b \\ c & d \end{pmatrix} &\to \begin{pmatrix} a & b \\ 0 & d - bca^{-1} \end{pmatrix} && \text{(add } -a^{-1}c \text{ copies of row 1 to row 2)} \\
&\to \begin{pmatrix} a & 0 \\ 0 & d - bca^{-1} \end{pmatrix} && \text{(add } (-db^{-1} + ca^{-1})^{-1} \text{ copies of row 2 to row 1)} \\
&\to \begin{pmatrix} a^2 & 0 \\ 0 & ad - bc \end{pmatrix} && \text{(multiply by } a\text{)} \\
&\to \begin{pmatrix} \frac{a^2}{ad-bc} & 0 \\ 0 & 1 \end{pmatrix} && \text{(multiply by } (ad-bc)^{-1}\text{)}
\end{aligned}$$

Each of these operations does not change the parity of the number of cycles, by the above reasoning.

If $a = 0$, we have the following steps:

$$\begin{aligned}
\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} &\to \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} && \text{(add } -b^{-1}d \text{ copies of row 1 to row 2)} \\
&\to \begin{pmatrix} 0 & \frac{b}{c} \\ 1 & 0 \end{pmatrix} && \text{(multiply by } c^{-1}\text{)}
\end{aligned}$$

Again none of the operations change the parity of the number of cycles. □

Lheemma VII.2 (QR Lemma)**.** *Let $x \in U_p$. Then x is a quadratic residue if and only if $\frac{p-1}{\mathrm{ord}_p(x)}$ is even.*

Proof. Let g be a generator of U_p. Then for some a, $x = g^a$. If x is a quadratic residue, then a must be even. The order of x is $\frac{p-1}{\gcd(p-1,a)}$ (the proof of this is left as an exercise to the reader), so $\frac{p-1}{\mathrm{ord}_p(x)} = \gcd(p-1, a)$. Since $p-1$ and a are both even, $\gcd(p-1, a)$ is even too. If x is not a quadratic residue, then a is odd. So $\frac{p-1}{\mathrm{ord}_p(x)} = \gcd(p-1, a)$ is odd. □

Theorem VII.3 (Hahn's Parity Theorem)**.** *(formerly Hahn's Conjecture of the first kind). f is a QRDFLF if and only if the number of cycles of f is even.*

Proof. First suppose $a \neq 0$. We can use Hahn's Transformation Lemma to reduce f to $g(x) = \frac{a^2}{ad-bc}x$. Observe that $ad - bc$ is a QR if and only if $\frac{a^2}{ad-bc}$ is, so $\det(f)$ is a QR if and only if $\det(g)$ is too. Now note that the cycle structure of g is relatively simple: it consists of two

fixed points, 0 and ∞, and $\frac{p-1}{\operatorname{ord}_p\left(\frac{a^2}{ad-bc}\right)}$ cycles of length $\operatorname{ord}_p\left(\frac{a^2}{ad-bc}\right)$. Therefore the parity of the number of cycles is $\frac{p-1}{\operatorname{ord}_p\left(\frac{a^2}{ad-bc}\right)}$, which is even if and only if $\frac{a^2}{ad-bc}$ is a quadratic residue.

If $a = 0$, then we can use similar logic. We can use Hahn's Transformation Lemma to reduce f to $g(x) = \frac{b}{cx}$. Note $\det(f) = -\det(g)$, so if f is a QR, g is a QR if and only if $p \equiv 1 \bmod 4$. This means the determinant of $1/g = \frac{c}{b}x$, namely $\frac{c}{b}$, is a QR if and only if $\det(f)$ is a QR. Again the cycle structure of $\frac{c}{b}x$ is two fixed points and all other cycles with the same length, so the parity of the number of cycles is $\frac{p-1}{\operatorname{ord}_p(c/b)}$, which is even if and only if $\frac{c}{b}$ is a QR by the QR Lemma. □

Corollary VII.4. *Given the parities of the number of cycles of f and g, we can find the parity of the number of cycles of $f \circ g$. In particular, they behave like $\mathbb{Z}_2$: if f and g both have an even number of cycles, then $f \circ g$ does too; if f has an odd number of cycles and g has an even number, then $f \circ g$ has an odd number; and if f and g have an odd number of cycles then $f \circ g$ has an even number.*

f	g	$f \circ g$
even	*even*	*even*
even	*odd*	*odd*
odd	*even*	*odd*
odd	*odd*	*even*

Proof. Let the matrices corresponding to f and g, as described by Hahn's Isomorphism, be F and G respectively. We have four cases.

If f and g both have an even number of cycles, then $\det(F)$ and $\det(G)$ are both quadratic residues. Since the product of two quadratic residues is also a quadratic residue, $\det(FG) = \det(F)\det(G)$ is a quadratic residue. So $f \circ g$ is a QRDFLF, and it has an even number of cycles.

The cases where one of f and g has an even number of cycles are symmetric, so WLOG f has an even number of cycles and g has an odd number of cycles. Then $\det(F)$ is a QR and $\det(G)$ is a QNR, so $\det(FG) = \det(F)\det(G)$ is a QNR. Therefore $f \circ g$ has an odd number of cycles.

Finally, if f and g both have an odd number of cycles, then $\det(F)$ and $\det(G)$ are both QNRs. So $\det(FG) = \det(F)\det(G)$ is a QR, so $f \circ g$ has an even number of cycles. □

VIII. HAHN'S (UNHELPFUL) CHARACTERIZATION

Theorem VIII.1. *Let f be a fractional linear function. Define $\sigma_1 = (0\ 1 \dots p-1)$ be the permutation that adds 1 mod p and $\sigma_2 = (0\ \infty)(2\ 2^{-1})\dots$ be the permutation that swaps an element with its inverse. Let σ be the cycle structure of the function g from Hahn's Transformation Lemma. Then the permutation of f is:*

$$\begin{cases} \sigma_2\sigma_1^{ca^{-1}}\sigma_2\sigma_1^{-(ab)(ad-bc)^{-1}}\sigma & \text{if } a \neq 0 \\ \sigma_1^{b^{-1}d}\sigma & \text{if } a = 0 \end{cases}$$

Proof. The proof uses Hahn's Transformation Lemma and some of the insights from the proofs of Hahn's Additive and Multiplicative Lhemmas. The idea is that for every transformation of

the corresponding matrix, we know the precise effect it has on the permutation. These are summarized in the table below:

Matrix operation	Function transformation	Permutation
add 2nd row to 1st row	$f \to f + 1$	σ_1
add 1st row to 2nd row	$f \to \frac{1}{1+\frac{1}{f}}$	$\sigma_2\sigma_1\sigma_2$
swap rows	$f \to \frac{1}{f}$	σ_2

In each case, transforming the function multiplies the function's permutation on the left by the permutation indicated above. We can then follow the proof of Hahn's Transformation Lemma.

First we take the case where $f = \frac{ax+b}{cx+d}$ has $a \neq 0$. Note that σ is defined to be the permutation corresponding to $g(x)$. Following the steps from the proof of Hahn's Transformation Lemma, we have the following. The permutation for the function corresponding to

$$\begin{bmatrix} a & 0 \\ 0 & d - bca^{-1} \end{bmatrix}$$

is $\sigma_1^{-(ab)(ad-bc)^{-1}}\sigma$, as the matrix can be obtained from the matrix of g by adding the 2nd row to the 1st row $(-db^{-1} + ca^{-1})^{-1} = (ab)(ad - bc)^{-1}$ times. The permutation for the function corresponding to

$$\begin{bmatrix} a & b \\ 0 & d - bca^{-1} \end{bmatrix}$$

is

$$(\sigma_2\sigma_1\sigma_2)^{ca^{-1}}\,\sigma_1^{-(ab)(ad-bc)^{-1}}\sigma = \sigma_2\sigma_1^{ca^{-1}}\sigma_2\sigma_1^{-(ab)(ad-bc)^{-1}}\sigma$$

as this matrix can be obtained from the previous one by adding ca^{-1} copies of row 1 to row 2. The permutation simplifies in the manner shown above as σ_2 has order 2. This completes the proof of the first case.

For the second case, where $a = 0$, we use exactly the same logic, just following the second case in the proof of Hahn's Transformation Lemma. We start with the permutation σ, then multiply on the left by $\sigma_1^{b^{-1}d}$ due to the fact that we added $-b^{-1}d$ copies of row 1 to row 2. □

IX. CONCRETE HAHN CHARACTERIZATIONS

This section will describe some more concrete characterizations that hold true throughout all the fractional linear functions. In some ways, this section can be thought of as using the tools we've developed to prove new results that follow nicely.

Lheemma IX.1 (Hahn's Odd Lemma)**.** *The number of odd-length cycles is even for $p > 2$.*

Proof. There are $p + 1 \equiv 0 \pmod 2$ in total, so the number of odd-length cycles will be even for the same reason as posited in the Handshake Lemma. □

Lheemma IX.2 (Hahn's Even Lemma)**.** *In a QRDFLF, the number of cycles with even length is even.*

Proof. This follows directly from Hahn's Obvious Lemma and the Hahn Parity Theorem. □

The real power from these two lemmas comes from the fact we didn't even mention the modulus. Thus, we have the following results:

Corollary IX.3 (Singular Fixed Point Implies Complete Cycle Structure)**.** *For $p > 3$, a FLF with a singular fixed point has a cycle structure consisting of that fixed point and another cycle of length p.*

Proof. By Proposition 2, we know that there are no other cycles of length < 3. Now, by Hahn's Theorem, we know that every other cycle must have the same length. However, since there are $p + 1$ elements in total and one of them is the fixed point, there are p elements left. Since p is prime and the cycle has length greater than or equal to 3, we conclude that there must only be one cycle of length p, as desired. □

Actually, this tells us that every FLF with exactly one fixed point is in fact a QRDFLF!

X. TIDBITS OF GROUP THEORY

We remarked earlier that $FL(\mathbb{F}_p)$ is a group. In fact, we can say something even stronger: this group *acts* on the set of elements in $\mathbb{P}_p$ in the natural manner (where a function $f \in FL(\mathbb{F}_p)$ acts on an element $p \in \mathbb{P}_p$ by $(f, p) \to f(p)$). This is a group action because of Hahn's Isomorphism and because matrix multiplication is associative. Thus, we can apply some of the theory of group actions to get some nice results!

First, consider the orbits that $FL(\mathbb{F}_p)$ partitions $\mathbb{P}_p$ into. We can actually see that there is exactly one orbit; this is because from the element 0, we can get to all the other non-infinity elements by applying the function $x + k$ to 0 as k ranges from 1 to $p - 1$, inclusive. Then, to get ∞, we can consider the function $f(x) = \frac{1}{x}$ acting on 0. Hence, everything is in 0's orbit, so there is only one unique orbit.

Now, by Burnside's Lemma, we get that

$$1 = \frac{1}{|FL(\mathbb{F}_p)|} \sum_{f \in FL(\mathbb{F}_p)} |\text{Fix}(f)|,$$

so the sum of the total number of fixed points across all FLFs is $|FL(\mathbb{F}_p)| = p^3 - p$.

Next, we have the following combinatorial result.

Proposition X.1. *The number of FLFs with exactly one fixed point in $FL(\mathbb{F}_p)$ is $p^2 - 1$ for $p \geq 3$.*

Proof. We will use the same formulation of unique FLFs up to scaling as Definition II.4. Let our function be denoted $\frac{ax+b}{cx+d}$. Notice that solving $\frac{ax+b}{cx+d} = x$ is equivalent to solving the quadratic $cx^2 + (d - a)x - b \equiv 0 \pmod{p}$ (more on this in the next section!), with ∞ being defined as a root of this if and only if $c = 0$.

First, if $c = 0$, then ∞ is one fixed point; thus, it must be the only one. We can see that this happens if and only if $d = a$ and $b \not\equiv 0 \pmod{p}$; this has $p - 1$ solutions up to scaling.

Now, if $c = 1$, our polynomial becomes $x^2 + (d - a)x - b \equiv 0 \pmod{p}$. This polynomial must have a double-root (that isn't infinity) modulo p, so first pick that root in p ways. Now,

$d - a$ and b are both fixed because the polynomial is fixed (since it's monic). Now, all of these different functions are unique up to scaling, so there are p ways to choose d; after this, everything is fixed. This gives an initial count of p^2 solutions. We do have to be careful about when the determinant equals zero, however! In particular, we need

$$ad - b \not\equiv 0 \pmod{p}.$$

Let the double-root of our quadratic be r for some $r \in \mathbb{Z}_p$. Now, we have $d - a \equiv -2r \pmod{p}$ and $-b \equiv r^2 \pmod{p}$, so $ad - b \not\equiv 0 \pmod{p}$ is equivalent to

$$a(a - 2r) + r^2 \not\equiv 0 \pmod{p} \implies (a - r)^2 \not\equiv 0 \pmod{p}.$$

Thus, we also have the added restriction $a \not\equiv r \pmod{p}$, which removes p solutions from our original count due to the determinant being zero. Thus, there are a total of $p(p-1)$ solutions in this case.

In total, the number of solutions is $p(p-1) + p - 1 = p^2 - 1$. □

Now, notice that each function either has zero fixed points, one fixed point, two fixed points, or is the identity function (with $p+1$ fixed points). This means that with the information that there are exactly $p^2 - 1$ functions with one fixed point and $p^3 - p$ functions total, we can sum the number of fixed points remaining to get the following count!

Proposition X.2. *For any prime $p \geq 3$, the number of FLFs with no fixed points is equal to $\frac{p^2(p-1)}{2}$.*

We will see even more group theory in the next section!

XI. HAHN'S LAST THEOREM

Theorem XI.1 (Cycle Classification)**.** *Let $p > 3$ be a prime. Then, the cycle structure of every FLF is one of the following:*

- *All fixed points;*
- *All two-cycles;*
- *A single fixed point and a cycle of length p;*
- *Two fixed points and $\frac{p-1}{d}$ cycles of length d, where $1 < d < p - 1$;*
- *ℓ cycles of length $\frac{p+1}{\ell}$, where $\ell < p + 1$ is any proper divisor of ℓ.*

This is unproven. To prove this, it suffices to prove that there exists a function with one big cycle of length $p+1$ and that there exist no singular two-cycles as the only cycles of length less than 3 for $p > 3$. This suffices due to the fact that any cycle of length at least 3 must divide $p-1, p$, or $p+1$ following from Hahn's Little Theorem and Small cycles theorem. Then, if have FLFs that have a $p - 1$, p, and $p + 1$ cycle, then we can simply take powers of these FLFs to generate any cycle length that is a proper divisor of $p-1, p$, and $p+1$. Clearly, $f(x) = 2x$ and $f(x) = x + 1$ are a $p - 1$ and p cycle for for any p, respectively.

We'll address the lack of 2-cycles next. This section will make extensive use of the Hahn Isomorphism.

Lheemma XI.2 (Singular Two-Cycle in FLFs)**.** *No FLF, taken modulo $p > 3$, has a singular two-cycle as its only cycle of length less than 3.*

Proof. Assume for the sake of contradiction that there exists such a function $f(x) = \frac{ax+b}{cx+d}$ in $\mathbb{P}_p$ for some prime $p > 3$. Now, consider the solutions to the equation $f(x) = x$. Note that if some $q \in \mathbb{P}_p$ is a solution, then it must be a root of the quadratic $cx^2 + (d-a)x - b = 0$ (where ∞ is defined to be a root if and only if $c = 0$). Since the only small cycle of f is a 2-cycle, then we know that this quadratic has no solutions.

On the other hand, we know that $f(f(x)) = x$ has two distinct solutions. Computing (or using Hahn's Isomorphism), we can get that

$$f(f(x)) = x \iff \frac{(a^2+bc)x + b(a+d)}{c(a+d)x + (bc+d^2)} = x \iff (a+d)(cx^2 + (d-a)x - b) = 0,$$

where ∞ is again a root if and only if $c = 0$. But then, since $cx^2 + (d-a)x - b \neq 0$ by our first assumption, we know that $a + d = 0$; however, this means that $f(f(x)) = x$ identically, so f is all two-cycles. This contradicts the fact that there is only one two-cycle. □

Notice that this tells us something very nice—in particular, we have $f(f(x)) = x$ identically if and only if the *trace* of the matrix corresponding to f is zero! This gives us an important characterization for when a function is "all small cycles".

Corollary XI.3. *(of Hahn's Last Theorem) There exists a FLF f mod p with a cycle length of n if and only if $p \equiv \pm 1 \bmod n$.*

The above corollary implies, for example, that there always exists a function with a 4-cycle by taking $n = 4$.

In an effort to prove Hahn's Last Theorem, we take a detour to the apparently unrelated topic of counting the numbers of FLFs.

XII. COUNTING FLFS

We generalize our idea of trace to fractional linear functions.

Definition XII.1. Consider a fractional linear function $f(x) = \frac{ax+b}{cx+d}$ outlined in Definition II.4. Then, we define the ***trace*** of f as $a + d \pmod p$.

Next, we have a very important result.

Proposition XII.2 (FLFs Equally Distributed Among Determinants)**.** *For any determinant $u \in U_p$, the number of FLFs with determinant u (where we define "up to scaling" as having $c = 0$ or $c = 1$) is equal to $p(p+1)$.*

Proof. Let L denote the list of all the unique FLFs with determinant 1 with $c \in \{0, 1\}$, and let $u \in U_p$ denote an arbitrary nonzero residue. To create a bijection between functions with determinant 1 and determinant u, consider corresponding every function of the form $\frac{ax+b}{cx+d}$ where $a, b, c, d \in \mathbb{Z}_p$ of determinant 1 with the fraction $\frac{u(ax+b)}{cx+d}$. This has determinant u, and the collection of these FLFs is unique up to scaling (i.e. this is injective) because the original list is also unique up to scaling and we're multiplying by a constant; furthermore, this is invertible since the inverse map is multiplication by u^{-1}. This means that this is a bijection. □

Now, notice that for any prime p, the number of nonzero quadratic residues equals the number of nonzero quadratic nonresidues. This gives us the following:

Corollary XII.3 (QRDFLFs Form Half of FLFs)**.** *For all primes $p \geq 3$, there exist exactly $\frac{p^3-p}{2}$ QRDFLFs up to scaling.*

From this, we can discover something very interesting about the relationships between squares and QRDFLFs.

Proposition XII.4 (Squares Injective in 1 (mod 8) Primes)**.** *Take a prime $p \equiv 1 \pmod 8$. Furthermore, consider two FLFs $f(x)$ and $g(x)$ up to scaling (so the coefficient of the x term in the denominator of f and g is either 0 or 1) that satisfy the following properties:*

- *Both have nonzero trace;*
- *The determinant of $f(x)$ equals the determinant of $g(x)$ modulo p;*
- *Both f and g are not QRDFLFs;*
- *$f(f(x)) = g(g(x))$ for all $x \in \mathbb{P}_p$.*

Then, $f(x) = g(x)$ for all $x \in \mathbb{P}_p$.

Proof. First, we claim that $f(f(x))$ and $g(g(x))$ both have nonzero trace as well. To see why, we can consider the cycle decomposition of f and g. Notice that the only FLFs q who can square to get zero trace (i.e. maximum cycle length is 2) falls into one of three categories for any odd prime:

- The trace of q is already zero;
- q consists of all four-cycles;
- q consists of two fixed points and the remaining cycles are all four-cycles.

We stipulated already that f and g do not have zero trace; furthermore, since $p+1 \equiv 2 \pmod 8$, we cannot have all four-cycles. Lastly, the third condition is violated by the fact that we want f and g to not be QRDFLFs, which contradicts that condition and Hahn's Parity Theorem.

Now, we will use Hahn's Isomorphism. Let $f(x) = \frac{ax+b}{cx+d}$ and $g(x) = \frac{ex+f}{gx+h}$. Then, $f(f(x)) = g(g(x))$ is equivalent to

$$\begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{bmatrix} \equiv \begin{bmatrix} e^2+fg & f(e+h) \\ g(e+h) & h^2+fg \end{bmatrix},$$

where the entries are taken modulo p. First, it is straightforward to check that if $c = 0$, then $g = 0$ as well and the two functions are in fact identical. Thus, we henceforth assume that both f and g are not linear.

Now, comparing the off-diagonal entries give us the two equations

$$b(a+d) = f(e+h), c(a+d) = g(e+h),$$

so we thus conclude that $\frac{b}{c} = \frac{f}{g} \implies \frac{b}{f} = \frac{c}{g}$ since $c \neq 0$ (which is because we're defining our functions up to scaling and f, g are not linear. For what it's worth, we can also stipulate

$c = g = 1$ at this point, although we won't need this; we will prove that the two functions are unique up to scaling instead). Thus, let $\frac{b}{f} = \frac{c}{g} = r$ for some nonzero $r \in \mathbb{Z}_p$. Now, comparing the diagonal entries yields

$$a^2 + bc = e^2 + fg, d^2 + bc = h^2 + fg \implies (a-d)(a+d) = (e-h)(e+h).$$

Now, take our first equation $a^2 + bc \equiv e^2 + fg$ from the upper-left entry, and let the common determinant of both matrices be denoted k. Now, we get that $a^2 + bc = a^2 + k - ad$ and $e^2 + fg = e^2 + k - eh$, so in fact $a^2 + bc = e^2 + fg \implies a^2 - ad = e^2 - eh \implies a(a-d) = e(e-h)$. Now, if $a = d$, it is now straightforward to check that $e = h$ and thus $b = f$ from the equations, so the two functions are equal; on the other hand, if $a - d, e - h \neq 0$, then $\frac{a}{e} = \frac{e-h}{a+d} = \frac{a+d}{e+h}$, where the last equality is from the equation $(a-d)(a+d) = (e-h)(e+h)$. Thus, this implies that $\frac{a}{e} = \frac{d}{h}$, at which point it becomes easy to check that $\frac{a}{e} = \frac{d}{h} = r$. Thus, the two functions are the same up to scaling and must thus be identical, as desired. □

Now, notice that we didn't actually use the fact that both $f(f(x))$ and $g(g(x))$ have nonzero trace! Actually, the following (more general fact) holds:

Lheemma XII.5 (Constant-Determinant Squares Injective)**.** *Consider FLFs up to scaling. Now, squaring is a injective map between nonzero-trace elements of determinant b for any $b \in U_p$ and elements of determinant b^2.*

Now, we also have the following result:

Lheemma XII.6 (Zero-Trace Elements Distributed Almost Equally Among Determinants)**.** *Again define FLFs up to scaling where the x-coefficient in the denominator is either 0 or 1 and where everything is accounted for up to scaling, where $c = 0$ means $a = 1$. Then, every unique nonzero determinant modulo p except -1 has an equal number of zero-trace elements.*

Proof. Fix some value of a; then, $d \equiv -a \pmod{p}$. We will now do casework on c. If $c = 0$, then we can scale things further such that $a = 1$; thus, $d = -1$ and the determinant is -1.

On the other hand, if $c = 1$, then the determinant is $-a^2 - b$. We can easily see that this hits every nonzero determinant exactly once as b ranges over $\mathbb{Z}_p$. □

XIII. PROGRESS ON HAHN'S LAST THEOREM

Now, we actually have all the tools that we need to prove a specific case of Hahn's Last Theorem!

Theorem XIII.1 (Specific Case of Hahn's Last Theorem)**.** *For all primes p such that $p \equiv 1 \pmod{8}$ and $\frac{p+1}{2}$ is prime, there exists a FLF which has one big cycle of length $p + 1$.*

Proof. First, note that since $FL(\mathbb{F}_p)$ is a group, there exists an element $g \in FL(\mathbb{F}_p)$ such that g has order $\frac{p+1}{2}$ by Cauchy's Theorem (since $\frac{p+1}{2}$ is prime). Next, let n denote the determinant of g; we know that n is a QR by Hahn's Parity Theorems and the fact that g has exactly two distinct cycles in its cycle decomposition.

Lheemma XIII.2. *There exists such a FLF with determinant not a quartic residue modulo p.*

Proof of Lemma. To do this, let g' represent the FLF denoted by the matrix $g \in FL(\mathbb{F}_p)$. If the determinant of g' is not a quartic residue, we're done. Otherwise, consider an element $\lambda \in U_p$ such that λ is a quadratic residue but not a quartic residue (which can be seen to exist), and consider the function $h = \lambda \cdot g'$. It now follows from induction that

$$h^n(x) = \underbrace{h(h(\cdots h(x)))}_{n \text{ times}} \equiv \lambda^n \cdot g^n(x) \pmod{p},$$

so—in particular—the order of h divides $\frac{p+1}{2}$ since $\lambda^{\frac{p+1}{2}} \equiv 1 \pmod{p}$ by Euler's Criterion. However, we can also see that the order of h cannot be one (and hence $h(x) \neq x$ identically) since the determinant of h is not a quartic residue; hence, the order of h is $\frac{p+1}{2}$ and it has determinant a non-quartic residue, as desired. □

Now, let the determinant of h be denoted m, and let $u \in U_p$ be a number such that $u^2 \equiv m \pmod{p}$. By virtue of m not being a quartic residue modulo p, we have that u is not a quadratic residue modulo p.

Consider the injective map we established earlier between the nonzero-trace elements of $FL(\mathbb{F}_p)$ with determinant u and the elements of determinant $u^2 \equiv m \pmod{p}$. From our work before and the fact that $p \equiv 1 \pmod{8}$, we can actually strengthen this to a *bijective* map between nonzero-trace elements with determinant u and nonzero-trace elements of determinant m. This tells us that there exists a FLF $z(x)$ with determinant u such that $z(z(x)) = h(x)$ for all values of x. But since z is not a QRDFLF, it has an odd number of cycles; thus, since $p \equiv 1 \pmod{8}$, each cycle must be of even length. Hence, upon squaring z, each cycle must split into two smaller cycles of half the length. In particular, since $z^2(x) = h(x)$ has two cycles, z must have a single cycle. We're done! □

The first few primes for which this result applies are $p = 73, 193, 313$.

XIV. OTHER CONJECTURES OF NOTE

Using code that was displayed the cycles for every FLF in $\mathbb{P}_p$ for some small p, we have more conjectures:

- p always divides the number of functions (call it $\pi_1(p)$) with one big cycle of length $p+1$. Actually, it seems like $p(p-1)$ always divides it, with some suspicious linear patterns.
  - $7 \to 84 = 2 \cdot 6 \cdot 7$
  - $11 \to 220 = 2 \cdot 10 \cdot 11$
  - $13 \to 468 = 3 \cdot 12 \cdot 13$
  - $17 \to 816 = \binom{18}{3} = 3 \cdot 17 \cdot 18$
  - $19 \to 1368 = 4 \cdot 18 \cdot 19$
  - $23 \to 2024 = 4 \cdot 22 \cdot 23$
  - $29 \to 3248 = 4 \cdot 28 \cdot 29$
  - $31 \to 7440 = 8 \cdot 30 \cdot 31$
- Let $\pi_2(p)$ denote the number of functions with two fixed points and one cycle of length $p-1$. Then, it seems like $p(p+1)$ divides $\pi_2(p)$.

- $19 \to 1140 = 3 \cdot 19 \cdot 20$
- $23 \to 2760 = 5 \cdot 23 \cdot 24$
- $29 \to 5220 = 6 \cdot 29 \cdot 30$
- $31 \to 3968 = 4 \cdot 31 \cdot 32$

- The determinant of any function which has one large $p+1$-cycle is a primitive root modulo p, and its characteristic polynomial is irreducible modulo p.

XV. FLFS OVER THE REALS

We will talk about FLFs with integer coefficients over the real numbers. In some ways, this branches into a lot of topics beyond just number theory, such as calculus. We have many observations and conjectures, and leave most of them unproven.

Conjecture XV.1 (C&C)**.** If $f(x)$ is not strictly increasing or decreasing, then $f(x)$ either cycles or $f^n(x)$ converges as n approaches infinity.

Conjecture XV.2 (The Jung Theorem)**.** The nth roots of unity are the roots of a quadratic polynomial with integer coefficients if and only if $n = 1, 2, 3, 4, 6$.

Conjecture XV.3 (The Kook Corollary)**.** $f(x)$ cannot have a cycle length $n \geq 5$ except $n = 6$.

We note that the Kook Corollary should follow from the Jung Theorem.

Theorem XV.4 (Real Hahn Theorem)**.** *For any FLF, any cycles it has of length greater than or equal to 3 all have the same length.*

This follows from the same proof as Hahn's Little Theorem, although we note that there are cases where FLFs never cycle. However, if a FLF does cycle, then it can never diverge.