# Polynomials in $\mathbb{F}_p[x]$ Which Commute Under Composition

J. Hatley and M. Teplitskiy

**Abstract -** Let $\mathbb{F}$ be a finite field and let $f$ be a linear polynomial in $\mathbb{F}[x]$. We investigate the number of polynomials of degree $d$ which commute with $f$ under composition. In so doing, we rediscover a result of Park, but with a conceptually simpler proof.

**Keywords :** polynomials; finite fields; composition of functions; combinatorics

**Mathematics Subject Classification** (2020) **:** 11T06; 05E99

## 1 Introduction

In [6], Zimmerman studies the following question: given an algebraically closed field $\mathbb{F}$ of characteristic zero, a nonlinear polynomial $f \in \mathbb{F}[x]$, and a natural number $d$, how many polynomials in $\mathbb{F}[x]$ of degree $d$ commute with $f$ under composition? That is, how many polynomials $g \in \mathbb{F}[x]$ of degree $d$ satisfy $f \circ g = g \circ f$? This question was motivated by similar work by Julia [1] and Ritt [5] regarding complex *rational* functions.

The surprising main result of [6] is that, for every $d \geq 1$, the number of polynomials in $\mathbb{F}[x]$ of degree $d$ which commute with $f$ is constant. The arguments used to establish this theorem rely crucially on the fact that $\mathbb{F}$ is algebraically closed.

Motivated by the work of Zimmerman, we investigated a similar question in a slightly different setting. More specifically, let $p$ be a prime, and let $\mathbb{F}_p$ be the finite field with $p$ elements. Let $f \in \mathbb{F}_p[x]$ be a linear polynomial (other than the "identity" polynomial $I(x) = x$). Given $d \geq 1$, we sought to determine how many polynomials in $\mathbb{F}_p[x]$ of degree $d$ commute with $f$. Denote this number by $\#C_d(f)$. We offer proofs of the following results (but see § 1.1 for the history of such results).

**Theorem** 5.1. Let $p \geq 3$ be a prime, and let $f \in \mathbb{F}_p[x]$ be a linear polynomial with leading coefficient $a \neq 1$. Let $d \geq 0$ be an integer, and let $r = \mathrm{ord}_p(a)$. Then

$$\#C_d(f) = \begin{cases} (p-1)p^{\frac{d-1}{r}}, & \text{if } d \equiv 1 \mod r \\ 0, & \text{if } d \not\equiv 1 \mod r \end{cases}.$$

**Theorem** 6.1. Let $p \geq 3$ be a prime, let $f \in \mathbb{F}_p[x]$ be a monic linear polynomial, and let $d \geq 0$ be an integer. Then

$$\#C_d(f) = \begin{cases} (p-1)p^k, & \text{if } d = kp \text{ for some integer } 0 \leq k \leq p \\ 0, & \text{otherwise} \end{cases}.$$

**Remark 1.1** The careful reader will observe that our arguments go through verbatim upon replacing $\mathbb{F}_p$ with a finite field of order $q = p^m$ for any $m \geq 1$ and replacing each instance of $p$ with $q$ in the formulas given in Theorems 5.1 and 6.1.

In fact, the *constructive* portions of our arguments would remain valid over the algebraic closure of $\mathbb{F}_p$, although the counting formulas would of course cease to be relevant.

### 1.1 Relation to Previous Work

Over a decade earlier than [6], Park [4] studied the following problem: For a finite field $\mathbb{F}$ and fixed $a, c \in \mathbb{F}$, determine which polynomials $g \in \mathbb{F}_{p^k}[x]$ satisfy the relation $g(x+a) = g(x) + c$.

The authors were not aware of Park's work until after writing this paper. Clearly, taking $a = c$ in Park's work recovers the problem addressed by Theorem 6.1. We also note other similarities between our own work and Park's: the arguments in [4] exploit explicit binomial coefficient identities modulo $p$, and the main result requires the degree bound $d < p^2$.

Nevertheless, we believe that our approach contains some significant conceptual simplifications. In particular, the key insights of this paper are:

- the observations in Section 3, which allow us to focus our attention on particularly "nice" linear polynomials $f$, and
- the recognition of an orderly, "scaffolded" structure, described via the *orbit* sets $T_k$ defined in Section 6, which is amenable to the application of useful mod $p$ binomial identities as recalled in Section 4.

Thus, despite the many similarities between the present work and [4], we believe that our approach, discovered independently, gives a conceptually simpler and cleaner proof, while still remaining elementary and constructive.

**Remark 1.2** In fact, Zieve and Masuda published a stronger result than ours or Park's only a year after Zimmerman's paper was published. Both Theorem 5.1 and Theorem 6.1 (with no upper bound on the degree) can be obtained as special cases of [3, Theorem 1.1]. The authors were unaware of [3] or [4] until after the completion of this paper.

## 2 Hypotheses and Notation

Throughout this paper we let $p$ denote a fixed odd prime. Let $\mathbb{F}_p[x]$ denote the ring of polynomials with coefficients in $\mathbb{F}_p$. As all of our computations will take place over the base field $\mathbb{F}_p$, we will often write $=$ instead of $\equiv \bmod p$.

Let $f, g \in \mathbb{F}_p[x]$. If $(f \circ g) = (g \circ f)$, then we write $f \sim g$. It is easy to see that this is an equivalence relation on $\mathbb{F}_p[x]$.

Let $f \in \mathbb{F}_p[x]$ and let $d \geq 1$ be a natural number. We write

$$C_d(f) = \{g \in \mathbb{F}_p[x] \colon f \sim g \text{ and } \deg(g) = d\}.$$

# 3 Algebraic Structure of $C_d(f)$

In this section, we record some useful lemmas on the algebraic structure of the sets $C_d(f)$. In particular, we are able to reduce the problem of determining $C_d(f)$ for general $f \in \mathbb{F}_p[x]$ to just two cases: $f = x + 1$ and $f = ax$ for $a \neq 1$.

## 3.1 Similar Polynomials

Let $\lambda = \alpha x + \beta \in \mathbb{F}_p[x]$ be a linear polynomial, so in particular $\alpha \in \mathbb{F}_p^\times$. We denote its inverse by $\lambda^{-1} = \alpha^{-1}x - \alpha^{-1}\beta \in \mathbb{F}_p[x]$.

We will make use of the following useful notion which also plays a key role in [6].

**Definition 3.1** *Let $f, g \in \mathbb{F}_p[x]$. We say $f$ and $g$ are <u>similar</u> if there exists a linear polynomial $\lambda \in \mathbb{F}_p[x]$ such that*

$$g = \lambda^{-1} \circ f \circ \lambda.$$

One easily checks that if $f$ and $g$ are similar then they have the same degree. In fact, we have the following useful results.

**Lemma 3.2** *Let $f = ax + b \in \mathbb{F}_p[x]$ be a linear polynomial, so in particular $a \in \mathbb{F}_p^\times$. Furthermore, if $b = 0$, then assume $a \neq 1$.*

1. *If $a \neq 1$, then $f$ is similar to $ax + c$ for any $c \in \mathbb{F}_p$.*
2. *If $a = 1$, then $f$ is similar to $x + c$ for any $c \in \mathbb{F}_p^\times$.*

**Proof.** To prove (1) (resp. (2)), just take $\lambda$ to be $x + (c - b)(a - 1)^{-1}$ (resp. $bc^{-1}x$ ). ☐

**Proposition 3.3** *Let $f, g \in \mathbb{F}_p[x]$ and let $d \in \mathbb{N}$. Suppose $f$ is similar to $g$ by $\lambda$. Then $\lambda$ induces an isomorphism of sets*

$$C_d(f) \xrightarrow{\sim} C_d(g).$$

**Proof.** We define the map

$$\Lambda \colon C_d(f) \to C_d(g)$$

by

$$\Lambda(P) = \lambda^{-1} \circ P \circ \lambda.$$

Since this map is clearly invertible, it suffices to show that the map is well-defined. Thus, let $P \in C_d(f)$ and let $Q = \Lambda(P)$. We must show $Q \in C_d(g)$. Let $Q = \lambda^{-1} \circ P \circ \lambda$. Then

$$\begin{aligned} g \circ Q &= (\lambda^{-1} \circ f \circ \lambda) \circ (\lambda^{-1} \circ P \circ \lambda) \\ &= \lambda^{-1} \circ (f \circ P) \circ \lambda \\ &= \lambda^{-1} \circ (P \circ f) \circ \lambda && \text{since } P \in C_d(f) \\ &= (\lambda^{-1} \circ P \circ \lambda) \circ (\lambda^{-1} f \circ \lambda) \\ &= Q \circ g. \end{aligned}$$

Thus $Q \in C_d(g)$ as desired. □

**Remark 3.4** In particular, to prove our main theorems, it suffices to study $C_d(x+1)$ and $C_d(ax)$ for $a \notin \{0, 1\}$.

### 3.2 Group Structure of $C_d(x+1)$

In this section, we observe that $C_d(x+1)$ may be given the structure of a group. For the rest of this section, write $f = x + 1$.

**Definition 3.5** *Let $g, h \in \mathbb{F}_p[x]$. Define the polynomial $g \oplus h$ by*

$$(g \oplus h)(x) = g(x) + h(x) - x.$$

Note that this definition does not require $g$ and $h$ to have the same degree.

**Proposition 3.6** *Let $f = x+1$ and let $g, h \in \mathbb{F}_p[x]$. If $f \sim g$ and $f \sim h$, then $f \sim (g \oplus h)$.*

**Proof.** We compute

$$\begin{aligned} [(g \oplus h) \circ f](x) &= g(x+1) + h(x+1) - (x+1) \\ &= [g(x) + 1] + [h(x) + 1] - x - 1 \\ &= g(x) + h(x) - x + 1 \\ &= [f \circ (g \oplus h)](x). \end{aligned}$$

□

It is straightforward to check that this makes $(C_d(x+1), \oplus)$ into a group with identity element $x$. In particular, the linear term can be seen as a "correction factor" among polynomials of $C_d(x+1)$. In contrast, the constant term is totally free.

**Lemma 3.7** *Suppose $g \in \mathbb{F}_p[x]$, $f = x + 1$, and $f \sim g$. Then for any $c \in \mathbb{F}_p$, we also have $f \sim (g + c)$.*

**Proof.** We compute

$$\begin{aligned}[(g+c)\circ f](x) &= g(x+1)+c \\ &= [g(x)+1]+c \\ &= [g(x)+c]+1 \\ &= [f\circ(g+c)](x).\end{aligned}$$

□

## 4 Two Useful Binomial Coefficient Identities

Recall the binomial expansion

$$(ax+b)^n = \sum_{i=0}^{n} \binom{n}{i} (ax)^{n-i} b^i.$$

In this section, we collect some useful identities for the binomial coefficients $\binom{n}{i}$ modulo $p$. For instance, in an elementary number theory course, one encounters the so-called "Freshman's Dream"

$$(x+y)^p \equiv x^p + y^p \mod p,$$

which is equivalent to the statement that

$$\binom{p}{i} \equiv 0 \mod p, \quad 1 \le i \le p-1.$$

The following generalization of this fact is due to Lucas [2, Section XXI].

**Theorem 4.1 (Lucas)** *Let $p$ be a prime number, and let $m, n$ be nonnegative integers. Denote by*

$$m = \sum_{i=0}^{k} m_i p^i$$

*the base-$p$ expansion of $m$, and similarly for $n$. Then*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod p.$$

*In particular, $n_i > m_i$ for some $1 \le i \le k$ if and only if $\binom{m}{n} \equiv 0 \mod p$.*

At one crucial moment we will also need the following well-known identity.

**Theorem 4.2 (Chu-Vandermonde Identity)** *Let $m, n,$ and $k$ be non-negative integers. Then*

$$\sum_{j=0}^{k} \binom{m}{j}\binom{n-m}{k-j} = \binom{n}{k}.$$

## 5 Main Results for Non-monic Linear Polynomials

In this section we will prove the following theorem.

**Theorem 5.1** *Let $f \in \mathbb{F}_p[x]$ be a linear polynomial with leading coefficient $a \neq 1$. Let $d \geq 0$ be an integer, and let $r = \mathrm{ord}_p(a)$. Then*

$$\#C_d(f) = \begin{cases} (p-1)p^{\frac{d-1}{r}}, & \text{if } d \equiv 1 \mod r \\ 0, & \text{if } d \not\equiv 1 \mod r \end{cases}.$$

Recall that, by Remark 3.4, it suffices to consider the case $f = ax$ for $a \neq 1$.
**Proof.** Let $f = ax$ for $a \neq 1$, and let $g \in \mathbb{F}_p[x]$ be a polynomial of degree $d$. Then

$$f(g(x)) = a(c_d x^d + c_{d-1}x^{d-1} + ... + c_0), \quad \text{and}$$
$$g(f(x)) = c_d(ax)^d + c_{d-1}(ax)^{d-1} + ... + c_0.$$

Assume $f \sim g$. Then for every $0 \leq i \leq d$, we must have

$$ac_i \equiv a^i c_i \mod p. \tag{1}$$

In particular, since $g$ is degree $d$, we have $c_d \neq 0$, so (1) implies that

$$a \equiv a^d \mod p. \tag{2}$$

Thus, it is necessary that $r = \mathrm{ord}_p(a) \mid d-1$, in which case (2) is satisfied for any of the $p-1$ choices of $c_d \in \mathbb{F}_p^\times$.

Now, for any $0 \leq i \leq d$, the same argument shows that if $c_i \neq 0$, then $r \mid i-1$. Since we must have $r \mid d-1$, there are only $\frac{d-1}{r}$ such indices for which we may have $c_i \neq 0$, and in each such case we have $p$ choices for $c_i$. This completes the proof. □

## 6 Main Results for Monic Linear Polynomials

We now turn our attention to the case of monic linear polynomials, where we have the following result.

**Theorem 6.1** *Let $p \geq 3$ be a prime, let $f \in \mathbb{F}_p[x]$ be a monic linear polynomial, and let $d \geq 0$ be an integer. Then*

$$\#C_d(f) = \begin{cases} (p-1)p^k, & \text{if } d = kp \text{ for some integer } 0 \leq k \leq p \\ 0, & \text{otherwise} \end{cases}.$$

We begin by proving that $f$ can only commute with a polynomial of degree $kp$.

**Proposition 6.2** *Let $f$ be a monic linear polynomial and let $g$ be any polynomial of degree $d$ that is not the identity. If $f \sim g$, then $d = kp$ for some $k \in \mathbb{N}$.*

**Proof.** Recall that it suffices to consider the case where $f = x+1$. Assume $f \sim g$. Then comparing $(d-1)$st coefficients of $f(g(x))$ and $g(f(x))$, we see

$$c_{d-1} \equiv c_{d-1} + dc_d \mod p.$$

This will only hold if $d \equiv 0 \mod p$. Hence, $d = kp$ for some $k \in \mathbb{N}$. □

Define

$$T_0 = \{0\} \quad \text{and} \quad T_p = \{p^2\},$$

and for $0 < k < p$, inductively define

$$\begin{aligned} T_k &= \{i+1 \mid i \in T_{k-1}\} \cup \{kp\} \\ &= \{ip + j \mid i, j \geq 0,\ i + j = k\}. \end{aligned}$$

Then set

$$R_k = \bigcup_{i=0}^{k} T_k \quad \text{and} \quad S_k = \{0, 1, 2, \ldots, kp\} \setminus R_k.$$

Thus, when $0 \leq k \leq p$, any polynomial $g$ of degree $kp$ may be written in the form

$$g(x) = \sum_{I \in R_k} c_I x^I + \sum_{J \in S_k} c_J x^J.$$

**Remark 6.3** From the second description of $T_k$ above, we may identify each element of $T_k$ with an ordered pair $(i, j)$.

**Example 6.4** If $p = 5$, the sets obtained in this fashion are shown in the following table.

| $k$ | $T_k$ | $R_k$ | $S_k$ |
|---|---|---|---|
| 0 | {0} | {0} | |
| 1 | {1,5} | {0,1,5} | {2,3,4} |
| 2 | {2,6,10} | {0,1,2,5,6,10} | {3,4,7,8,9} |
| 3 | {3,7,11,15} | {0,1,2,3,5,6,7,10,11,15} | {4,8,9,12,13,14} |
| 4 | {4,8,12,16,20} | {0,1,2,3,4,5,6,7,8,10,11,12,15,16,20} | {9,13,14,17,18,19} |
| 5 | {25} | {0,1,2,3,4,5,6,7,8,10,11,12,15,16,20,25} | {9,13,14,17,18,19,21,22,23,24} |

For any integer $k \geq 0$, let $[kp]$ denote the set of integers between $(k-1)p$ and $kp$, inclusive. Set $\tilde{R}_k = R_k \cap [kp]$ and $\tilde{S}_k = S_k \cap [kp]$. Then we see that

$$\tilde{R}_k = \begin{cases} \{(k-1)p, (k-1)p+1, kp\} & \text{if } p \nmid k \\ \{(k-1)p, kp\} & \text{if } p \mid k \end{cases} \tag{3}$$

and

$$\tilde{S}_k = \begin{cases} \{(k-1)p + i \mid 2 \leq i \leq p-1\} & \text{if } p \nmid k \\ \{(k-1)p + i \mid 1 \leq i \leq p-1\} & \text{if } p \mid k \end{cases}. \tag{4}$$

The following lemma sheds light on the definitions above, and it is crucial to our approach.

**Lemma 6.5** *Let $k \geq 0$ be an integer. Let $r \in R_k$ and $s \in S_k$. Then*

$$\binom{r}{s-1} = 0.$$

**Proof.** We may assume without loss of generality that $s \in \tilde{S}_k$, i.e. that $(k-1)p \leq s-1 \leq kp-2$. Since the conclusion of the lemma is trivial if $r < s-1$, we may assume $r > s-1$, so by (3) we must have $r = kp$. The result now follows from Theorem 4.1. □

As a corollary, we obtain the following important description of polynomials in $C_{kp}(x+1)$.

**Lemma 6.6** *Let $g \in C_{kp}(x+1)$. Then $g$ is of the form*

$$g(x) = \sum_{I \in R_k} c_I x^I.$$

*That is, $c_J = 0$ for each $J \in S_k$.*

**Proof.** Write

$$g(x) = \sum_{I \in R_k} c_I x^I + \sum_{J \in S_k} c_J x^J$$

and suppose $n$ is the largest value in $S_k$ for which $c_n \neq 0$. Since $g \in C_{kp}(x+1)$, we have

$$g(x) + 1 = g(x+1). \tag{5}$$

The coefficient of $x^{n-1}$ on the left-hand side is clearly $c_{n-1}$. Let us also determine this coefficient on the right-hand side.

Only terms of index greater than or equal to $n-1$ will contribute to this coefficient. If $m > n$, then $c_m \neq 0$ implies $m \in R_k$, and so the coefficient of $x^{n-1}$ in the expansion of $c_m(x+1)^m$ vanishes by Lemma 6.5. Thus, the coefficient of $x^{n-1}$ on the right-hand side of (5) is

$$c_{n-1} + nc_n.$$

Since $n \in S_k$, we know by (4) that $n \not\equiv 0 \mod p$, so this implies that $c_n = 0$. This contradicts our choice of $n$, hence

$$g(x) = \sum_{i \in R_k} c_i x^i \tag{6}$$

as desired. □

We will prove Theorem 6.1 by determining the dependencies between the various coefficients of $g$. To begin with, we have the following very simple lemma.

**Lemma 6.7** *If $g \in C_d(x+1)$ then $g + c \in C_d(x+1)$ for any $c \in \mathbb{F}_p$.*

**Proof.** If $g(x)+1 = g(x+1)$, then

$$g(x+1)+c = [g(x)+1]+c = [g(x)+c]+1.$$

□

In the argument that follows, we say that coefficients (identified by their indices) occupy the same *orbit* if the choice of one determines the values of the others. So for instance, by Lemma 6.7 we always have the singleton orbit $\{0\}$, while Example 6.8 below will establish that in degree $p$ we have an additional orbit $\{1, p\}$. Every orbit gives rise to $p$ possible choices (or $p-1$ for the orbit of the top-degree term), so determining how to partition $R_k$ into orbits gives us the size of $C_{kp}(x+1)$: namely, if $R_k$ can be partitioned into $\ell+1$ orbits, then $\#C_{kp}(x_1) = (p-1)p^\ell$. We will show that the orbits at degree $kp$ are precisely the sets $T_0, \ldots, T_k$, from which Theorem 6.1 follows.

Since we have an addition operation on $C_{kp}$ as described in Section 3, it suffices to show that we may construct an element of $C_{kp}(x+1)$ whose only nonzero coefficients come from $T_k$ plus a linear term (which, in light of Section 3, can be viewed as a correction term), and that these coefficients are all determined by the choice of the leading coefficient.

Before proving this last claim, let us illustrate our argument in the cases $k=1$ and $k=2$.

**Example 6.8** Case $k=1$

By Lemma 6.6, if $g \in C_p(x+1)$, it may only have nonzero coefficients at the degrees in $R_1 = \{0, 1, p\}$. By Lemma 6.7, it suffices to consider

$$g(x) = c_p x^p + c_1 x.$$

Then

$$\begin{aligned} g(x+1) &= c_p x^p + c_1 x + (c_1 + c_p) \\ &= g(x) + (c_1 + c_p), \end{aligned}$$

which shows that we are free to pick any value for $c_p$, and then choosing $c_1 = 1 - c_p$ yields an element of $C_p(x+1)$. There are $p$ choices for $c_0$ and $p-1$ nonzero choices for $c_p$, giving $(p-1)p$ polynomials in $C_p(x+1)$.

**Example 6.9** Case $k=2$

By Lemma 6.6, if $g \in C_{2p}(x+1)$, it may only have nonzero coefficients at the degrees in $R_2 = \{0, 1, p, 2, p+1, 2p\}$. The degrees which were not present in the case $k=1$ are precisely those in $T_2 = \{2, p+1, 2p\}$. Any polynomial we can construct from just $T_2$ may be added (in the sense of Definition 3.5) to polynomials constructed from $T_0$ and $T_1$ to yield more polynomials in $C_{2p}$. So let us determine how many such polynomials we can build.

Suppose

$$g(x) = c_{2p} x^{2p} + c_{p+1} x^{p+1} + c_2 x^2 + x.$$

Then

$$g(x+1) = g(x) + (2c_{2p} + c_{p+1})x^p + (c_{p+1} + 2c_2)x + (c_{2p} + c_{p+1} + c_2 + 1).$$

Thus, upon choosing a value for $c_{2p}$, we must have $c_{p+1} = -2c_p$ and $c_2 = c_{2p}$, and then the constant term in the displayed equation is identically 1, as desired. Thus, the indices in $T_2$ form a new, distinct orbit.

Excluding zero, there are $(p-1)$ choices for $c_{2p}$, so there are $(p-1)$ choices of $g(x)$ as above. Under our addition law for $C_d(x+1)$ $[g_1 \oplus g_2 = g_1 + g_2 - x]$, we may combine these choices of $g(x)$ with those of degree $p$. Since we may now allow $c_p = 0$, there are $p^2$ polynomials in $C_{2p}(x+1)$ with which to combine, so these combinations give us $\#C_{2p}(x+1) = (p-1)p^2$ polynomials in $C_{2p}(x+1)$.

As our arguments above have explained, it suffices to show that for each $k$ we can construct a polynomial in $C_{kp}$ using only indices from $T_k$. We do this now.

Suppose

$$g(x) = x + \sum_{I \in T_k} c_I x^I.$$

Using Theorem 4.1, we find that $g(x+1) = g(x) + h(x)$ where

$$h(x) = (1 + \sum_{I \in T_k} c_I) + \sum_{t \in R_{k-1}} \left( \sum_{I \in T_k} \binom{I}{t} c_I \right) x^t. \tag{7}$$

We now make a sequence of observations about the coefficients appearing on the right-hand side of (7) in order to show that, for each choice of value for $c_{kp}$, there is a unique choice of value for each other $c_I$, $I \in T_k$ which makes $h(x)$ identically zero.

First note that the case $k = p$ is special, since one immediately checks that $x^{p^2}$ commutes with $x+1$. Thus, $[p^2]$ is its own orbit. We now consider $k < p$.

Since $k < p$, we have

$$T_k = \{ip + j \mid i, j \geq 0,\ i + j = k\}.$$

We identify the element $ip + j \in T_k$ with the ordered pair $(i, j)$.

Let $t \in T_{k-1}$, so that $t = i'p + j'$ where $i' + j' = k - 1$. Then from (7), the coefficient of $x^t$ is

$$\begin{aligned}\sum_{I=(i,j) \in T_k} \binom{I}{t} c_I &= \sum_{\substack{i,j \geq 0 \\ i+j=k}} \binom{ip+j}{i'p+j'} c_{(i,j)} \\ &= \sum_{\substack{i,j \geq 0 \\ i+j=k}} \binom{i}{i'} \binom{j}{j'} c_{(i,j)} \qquad \text{by Theorem 4.1.}\end{aligned}$$

Applying Theorem 4.1 again, we see that the only binomial coefficients in the sum above which are not zero in $\mathbb{F}_p$ are

$$\binom{i'+1}{i'}\binom{j'}{j'} = i'+1 \qquad \text{and} \qquad \binom{i'}{i'}\binom{j'+1}{j'} = j'+1.$$

Thus, the coefficient of $x^t$ is

$$(i'+1)c_{(i'+1,j')} + (j'+1)c_{(i',j'+1)},$$

and if $g \sim f$ then this coefficient must be zero. This produces a chain of dependencies between the $c_I$ for $I \in T_k$:

$$\begin{aligned} (k)c_{(k,0)} &= -c_{(k-1,1)} \\ (k-1)c_{(k-1,1)} &= -2c_{(k-2,2)} \\ (k-2)c_{(k-2,2)} &= -3c_{(k-3,3)} \\ &\vdots \\ c_{(1,k-1)} &= -kc_{(0,k)}. \end{aligned}$$

In particular, choosing a value for $c_{(k,0)} = c_{kp}$ determines the values for the rest of the $c_I$ for $I \in T_k$, and these choices are consistent with the requirement from the constant term in (7) that $\sum_{I \in T_k} c_I = 0$.

The only thing left to check is that the conditions imposed by the coefficients of $x^t$ for $t \in R_{k-2}$ do not contradict the ones we just found. Let $1 \leq k' \leq k-2$. Using the same style of computation as above, the coefficient of $x^t$ for each $t \in T_{k'}$ yields a linear dependence equation between the $c_I$ for $I \in T_k$. Rather than write these individually, consider the sum of these linear dependence equations. In this sum, the coefficient of $c_{(i,j)}$ is

$$\begin{aligned} \sum_{\substack{i',j' \geq 0 \\ i'+j'=k'}} \binom{ip+j}{i'p+j'} &= \sum_{\substack{i',j' \geq 0 \\ i'+j'=k'}} \binom{i}{i'}\binom{j}{j'} \\ &= \binom{k}{k'} && \text{by Theorem 4.2.} \end{aligned}$$

Since this is true for every $I \in T_k$, we see that the linear dependence conditions imposed by $R_{k-2}$ are also consistent with the condition imposed by the linear term in (7). This completes the proof.

## 7 Some Numerical Examples

We now provide examples which illustrate the methods in Section 6.

Example #1:

Let $p = 3$ and $k = 2$. By Theorem 6.1, we calculate 18 polynomials that commute with $x + 1$. We will now show why this is the case in this particular example. By Lemma 6.3, we know that this polynomial will take the form $c_6x^6 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$. We also know that our orbits will be $[0], [1, 3], [2, 4, 6]$.

| determined degree | $c_6$ | $c_4$ | $c_3$ | $c_2$ | $c_1$ | $c_0$ |
|---|---|---|---|---|---|---|
| $c_6$=1 | $c_6$=1 | $c_4$=1 | | $c_2$=1 | | |
| $c_6$=2 | $c_6$=2 | $c_4$=2 | | $c_2$=2 | | |
| $c_3$=0 | | | $c_3$=0 | | $c_1$=1 | |
| $c_3$=1 | | | $c_3$=1 | | $c_1$=0 | |
| $c_3$=2 | | | $c_3$=2 | | $c_1$=2 | |
| $c_0 = 0$ | | | | | | $c_0 = 0$ |
| $c_0 = 1$ | | | | | | $c_0 = 1$ |
| $c_0 = 2$ | | | | | | $c_0 = 2$ |

We can see from the table that there are 18 possible polynomials of degree 6 that commute with $x + 1$. We can build these polynomials by selecting one choice for $c_6, c_3$ and $c_0$ and combining the three. Some examples of these polynomials are

- $x^6 + x^4 + x^2$
- $2x^6 + 2x^4 + x^3 + 2x^2 + 1$
- $x^6 + x^4 + 2x^3 + x^2 + 2x + 2$

Example #2:

Let $p = 5$ and $k = 5$. By using our method for finding degrees that can show up in $g$, we see that degrees 0,1,2,3,4,5,6,7,8,10,11,12,15,16,20,25 can appear in $g$, while all other degrees $0 \leq d \leq 25$ cannot.

Then we can see that our orbits have the following structure:

| $k$ | new degrees | orbits |
|---|---|---|
| 1 | 0,1,5 | [0],[1,5] |
| 2 | 2,6,10 | [0],[1,5],[2,6,10] |
| 3 | 3,7,11,15 | [0],[1,5],[2,6,10],[3,7,11,15] |
| 4 | 4,8,12,16,20 | [0],[1,5],[2,6,10],[3,7,11,15],[4,8,12,16,20] |
| 5 | 25 | [0],[1,5],[2,6,10],[3,7,11,15],[4,8,12,16,20],[25] |

## Acknowledgments

The authors are thankful to Michael Zieve for bringing their attention to his work with Ariane Masuda, and also to the work of Hong Goo Park. The authors are especially grateful to the anonymous referee for their careful reading and helpful suggestions.

The authors thank Union College for providing an encouraging environment for undergraduate research.


## References


[1] J. Gaston, Mémoire sur la permutabilité des fractions rationnelles, *Ann. Sci. École Norm. Sup. (3)*, **39** (1922), 131–215.

[2] E. Lucas, Theorie des Fonctions Numeriques Simplement, *Amer. J. Math.*, **1** (1878), 197–240.

[3] A.M. Masuda, M.E. Zieve, Rational functions with linear relations, *Proc. Amer. Math. Soc.*,**136** (2008), 1403–1408.

[4] H.G. Park, Polynomials satisfying $f(x+a) = f(x) + c$ over finite fields, *Bull. Korean Math. Soc.*, **29** (1992), 277–283.

[5] J.F. Ritt, Permutable rational functions, *Trans. Amer. Math. Soc.*, **25** (1923), 399–448.

[6] K. Zimmerman, Commuting polynomials and self-similarity, *New York J. Math.*, **13** (2007), 89–96.



*Jeffrey Hatley*
Union College
Bailey Hall 202
Schenectady, NY 12308
E-mail: `hatleyj@union.edu`

*Mayah Teplitskiy*
Union College
Bailey Hall 202
Schenectady, NY 12308
E-mail: `teplitsm@union.edu`



**Received**: December 13, 2022 **Accepted**: February 6, 2023
**Communicated by Steven J. Miller**