LOCALLY NILPOTENT POLYNOMIALS OVER $\mathbb{Z}$

Sayak Sengupta
Department of Mathematics and Statistics, Binghamton University - SUNY,
Binghamton, New York
sengupta@math.binghamton.edu

Received: 6/1/23, Revised: 7/23/23, Accepted: 1/12/24, Published: 1/29/24

Abstract

For a polynomial $u = u(x)$ in $\mathbb{Z}[x]$ and $r \in \mathbb{Z}$, we consider the orbit of u at r denoted and defined by $\mathcal{O}_u(r) := \{u(r), u(u(r)), \ldots\}$. We ask two questions here: (i) what are the polynomials u for which $0 \in \mathcal{O}_u(r)$, and (ii) what are the polynomials for which $0 \notin \mathcal{O}_u(r)$ but, modulo every prime p, $0 \in \mathcal{O}_u(r)$? In this paper, we give a complete classification of the polynomials for which (ii) holds for a given r. We also present results for some special values of r where (i) can be answered.

1. Introduction

In Example 1 of [4], A. Borisov set up a polynomial map, called the *additive trap*, $F_{at} : \mathbb{A}^2_{\mathbb{Z}} \to \mathbb{A}^2_{\mathbb{Z}}$, that maps $(x, y) \mapsto (x^2y, x^2y + xy^2)$. This polynomial map satisfies many interesting properties. In particular, $F^{(p)}_{at}(x, y) \equiv (0, 0) \pmod p$ for every $(x, y) \in \mathbb{A}^2_{\mathbb{F}_p}$ and for all primes p, where $F^{(p)}_{at}$ is the pth iteration of F_{at}. To prove this, suppose that p is a prime. Note that all points $(x, y) \in \mathbb{A}^2_{\mathbb{F}_p}$ with either $x = 0$ or $y = 0$ are taken to (0,0) by F_{at}. Let $x \in \mathbb{F}^*_p$. Then for any $y \in \mathbb{F}^*_p$ one has

$$\frac{x^2y + xy^2}{x^2y} = \frac{y}{x} + 1.$$

So, after at most $p-1$ iterations, the second coordinate becomes 0 and thus, applying F_{at} once more, one gets (0,0). Since p is arbitrary, the proof follows. For more details, see [4]. One can see from the discussion that the pth iteration of F_{at} modulo p is the zero map, which follows from the fact that the polynomial $u(x) = x + 1$ has the following property: for every $n \in \mathbb{N}$, $u^{(n)}(x) = x + n$, so that, in particular, for every prime p, $u^{(p-1)}(1) = p \equiv 0 \pmod p$. Throughout this paper, $\mathbb{N}$ is the set of all positive integers, $u^{(0)}(x) = x$, and

$$u^{(n)}(x) := \underbrace{(u \circ u \circ \cdots \circ u)}_{n \text{ times}}(x),$$

DOI: 10.5281/zenodo.10580977

the nth iteration of a non-constant polynomial $u(x)$. We can write our first definition now, which is motivated by the behavior of the polynomial $x+1$. Suppose $r \in \mathbb{Z}$ and A is a finite subset of the set of all prime numbers. If for every prime p not contained in A, there exists an $m \in \mathbb{N}$ such that $u^{(m)}(r) \equiv 0 \pmod{p}$, we will say that *$u$ is weakly locally nilpotent at r outside A*. The set of all weakly locally nilpotent polynomials at r outside A of degree d will be denoted by $L^d_{r,A}$, and $L_{r,A}$ is the union of $L^d_{r,A}$'s, where the union is taken over all degrees $d \in \mathbb{N}$. When $A = \emptyset$, i.e., for all primes p, m exists satisfying $u^{(m)}(r) \equiv 0 \pmod{p}$, we say that u is *locally nilpotent at r*. Thus $u(x) = x+1$ is locally nilpotent at 1, i.e., $x+1 \in L^1_{1,\emptyset}$. If, in particular, a polynomial u is such that $u^{(n)}(r) = 0$ for some $n \in \mathbb{N}$, then we will say that u is *nilpotent at r*, and the *nilpotency index* is the least of such n's. We denote the set of all nilpotent polynomials at r of degree d and nilpotency index i by $N^d_{r,i}$. Also, N_r is the union of all such $N^d_{r,i}$, where the union is taken over $i, d \in \mathbb{N}$. Thus $u(x) = x-1$ is nilpotent at 1 of nilpotency index 1, i.e., $x-1 \in N^1_{1,1}$. One of the principal goals of this paper is to understand the polynomials that are locally nilpotent without being nilpotent at r, i.e., 0 is not in the orbit of a polynomial u at r but modulo every prime p, some iteration of u at r hits 0. This is an interesting question, and it is completely answered here. To classify these polynomials, we have used Theorem 5 of [2]. In particular, if one takes $K = \mathbb{Q}, g = 1, A_1 = \{0\}, T_1 = \{r\}$, and $\varphi_1 = u$ in this theorem, we get Fact 1.1 in our paper which says the following.

Fact 1.1. *If u is a polynomial that is of degree at least 2, and it is weakly locally nilpotent at r outside some finite set of primes A, then it must be nilpotent at r. Equivalently, if there is a polynomial u such that it is weakly locally nilpotent at r outside A but not nilpotent at r, then it must be a linear polynomial.*

It should be noted that Theorem 5 of [2] was built upon the work of Silverman in [8], and the works of Benedetto–Ghioca–Kurlberg–Tucker–Zannier in Lemma 4.1 of [3]. It should also be noted that the question of when an orbit passes through a given point modulo a prime came naturally from the study of the Dynamical Mordell–Lang (DML) Conjecture, which is a major open question in arithmetic dynamics. The paper [2] was developed to prove certain special cases of the DML Conjecture. Interested readers can also look at [1].

From Fact 1.1, it is imperative to study the behavior of linear polynomials to understand non-nilpotent, locally nilpotent polynomials. This is where we use Theorem 1 of [6] to derive a Lemma that we call CRS lemma (Lemma 3.2). This lemma will be stated and proved in Section 3.

The paper contains three main results:

(1) The complete classification of all polynomials in $L_{r,\emptyset}$ for $r \in \{0, -1, 1\}$, and that can be found in Theorems 4.1, 4.4, and Corollary 4.2.

(2) The complete classification of all polynomials in $L^1_{1,A}$ for any given finite

subset A of the set of prime numbers, and that can be found in Theorem 5.1. To establish this we use Lemma 3.2.

(3) The complete classification of all polynomials in S_r, where $S_r := L_{r,\emptyset} \setminus N_r$, and that can be found in Corollaries 4.3, 4.5, 5.4, and Theorem 5.3. Lemma 3.2 has also been used to establish this.

The main tools that we have used here are Facts 1.1 and 3.1, Lemma 3.2, and the reduction of polynomials, a technique described after Remark 3.3.

In Sections 2 and 3, respectively, we formalize the definitions and introduce the main tools. Section 4 contains the main results listed in (1) above. Section 5 is dedicated to the classification of polynomials in S_r. The last section has some open questions and discussions that arose from the study of the polynomials in this paper. The interested reader can also look at the work of Shallit and Vasiga in [9], and Odoni in [7].

2. Definitions, Notation, and Terminology

We will start by formally defining the polynomials mentioned in the introduction and fixing some basic terminology that we will use throughout this paper. Let $\mathcal{P}$ be the set of all positive primes in $\mathbb{Z}$. For a finite subset A of $\mathcal{P}$ and for $a \in \mathbb{Z}$, we define

$$\mathcal{P}_A := \mathcal{P} \setminus A, \ P_A(a) := \{p \in \mathcal{P}_A \mid p \text{ divides } a\}, \text{ and } \ P(a) := P_\emptyset(a).$$

So $P(a)$ is the set of all positive primes that divides a. Having fixed r in $\mathbb{Z}$, A a finite subset of $\mathcal{P}$, d in $\mathbb{N}$ a degree, and i in $\mathbb{N}$ an index, we make the following definitions.

We will say that $u(x)$ is a *weakly locally nilpotent polynomial* at r outside A if for each $p \in \mathcal{P}_A$, there exists $m \in \mathbb{N}$ (possibly depending on p) such that $u^{(m)}(r) \equiv 0 \pmod{p}$. For each $p \in \mathcal{P}_A$, we let m_p be the least of all such m's. We fix the following notation for weakly locally nilpotent polynomials at r outside A: $L^d_{r,A} := \{u \mid u, \text{ of degree } d, \text{ is weakly locally nilpotent at } r \text{ outside } A\}$, and $L_{r,A} := \sqcup_{d=1}^{\infty} L^d_{r,A}$. If $A = \emptyset$ then we will just drop the terms "weakly" and "outside A".

We will say that $u(x)$ is a *nilpotent polynomial* at r if there exists an $n \in \mathbb{N}$ such that $u^{(n)}(r) = 0$. We will call the smallest of all such n's the *nilpotency index/index of nilpotency* of $u(x)$ at r. If $u^{(n)}(r) \neq 0$ for all $n \in \mathbb{N}$, we will say that u is *non-nilpotent* at r. We fix the following notation for nilpotent polynomials at r. We set $N^d_{r,i} := \{u \mid u \text{ is nilpotent at } r \text{ of nilpotency index } i \text{ and degree } d\}$, $N_{r,i} := \sqcup_{d=1}^{\infty} N^d_{r,i}$, $N_r := \sqcup_{i=1}^{\infty} N_{r,i}$, and $S_r := L_r \setminus N_r$. For integers a, b, c $(c \neq 0)$, we will write $a \equiv_c b$ to mean $a \equiv b \pmod{c}$.

Remark 2.1. It is clear that $N_r \subset L_{r,\emptyset}$. But it turns out that for every given $r \in \mathbb{Z}$, S_r is non-empty (see Corollaries 4.3, 4.5 and 5.4, and Theorem 5.3 below).

We will now see some examples to help understand the definitions that we have made on the previous page.

2.1. Some Examples

(a) Let $r \in \mathbb{Z}$. For each non-zero $q(x) \in \mathbb{Z}[x]$ one has $(x-r)q(x) \in N_{r,1}$.

(b) If $u(x) = -2x-4$, then $u(-1) = -2$, and $u(-2) = 0$. So $u(x) \in N^1_{-1,2}$. If $r \in \mathbb{Z} \setminus \{-1\}$, then $u_r(x) := -(r+1)x + (r+1)^2 \in N^1_{r,2}$, and if $r \in \mathbb{Z} \setminus \{0\}$, then $u_r(x) := -2x + 4r \in N^1_{r,2}$. Also, if $r \in \mathbb{Z} \setminus \{0\}$, then $u(x) = x \pm 1 \in N^1_{r,r}$, where we use the negative sign when r is positive and positive sign otherwise.

(c) Let $u(x) = -2x^2 + 7x - 3$. Then $u(1) = 2,\ u(2) = 3$, and $u(3) = 0$. So $u(x) \in N^2_{1,3}$. From this and Fact 3.1 (stated and proved below), it follows that $v(x) := 2x^2 + 7x + 3 \in N^2_{-1,3}$.

(d) Let $u(x) = -x^3+9x^2-25x+25$. Then $u(2) = 3, u(3) = 4, u(4) = 5,$ and $u(5) = 0$. That means $u \in N^3_{2,4}$.

(e) Let $u(x) = x+1$. Then, by induction, it is easy to see that $u^{(n)}(1) = n+1$ for every $n \in \mathbb{N}$, and hence $u \notin N_1$. For each $p \in \mathcal{P}$, one has $u^{(p-1)}(1) = p \equiv_p 0$. Thus $u(x) \in S_1$. In Corollary 4.3, we will see that $S_1 = \{x+1\}$. (This example shows the existence of a non-nilpotent, locally nilpotent polynomial at 1.)

(f) For every $a \in \mathbb{Z} \setminus \{0\}$, let $u_a = u_a(x) := x + a$. By induction, we get $u_a^{(n)}(0) = na$, so it is clear that $u_a \notin N_0$. For each prime p, one has $u_a^{(p)}(0) = pa \equiv_p 0$. Thus $u_a \in S_0$.

(g) Let $u(x) = 4x-2$. Then $u(1) = 2$ and $u(2) = 6 \equiv_5 1$. This means $u^{(n)}(1)$ is either 1 or 2 (mod 5) for every $n \in \mathbb{N}$. This shows that $u(x) \notin L_{1,A}$ for every finite subset $A \subset \mathcal{P}_{\{5\}}$.

(h) Let $u(x)$ be as in (g). Then by induction we have $u^{(n)}(0) = \frac{2}{3}(1-4^n)$, which cannot be zero for any $n \in \mathbb{N}$, and so the above polynomial is not in N_0. Clearly $m_2 = 1$ and $m_3 = 3$, and for every other prime p, by Fermat's Little Theorem, one has $u^{(p-1)}(0) \equiv_p 0$. Thus, $u(x) \in S_0$.

Remark 2.2. The computation of polynomial iterations for a general polynomial is very complicated, but the linear polynomials have a simple iteration formula. Let

$u(x) = ax + b$ be a linear polynomial. Then by induction, it follows that for every $n \geq 1$,

$$u^{(n)}(x) = a^n x + b\left(\sum_{i=0}^{n-1} a^i\right).$$

So $u^{(n)}(r) = a^n r + b\left(\sum_{i=0}^{n-1} a^i\right)$ for each $n \in \mathbb{N}$. Throughout this paper we will refer to this formula as the *linear iteration formula.*

3. The Main Tools

In this section we will develop the necessary tools. We begin with the proof of Fact 3.1, which indicates that for our purposes it is enough to study the polynomials at non-negative values of r. In particular, it shows that there is a one-to-one correspondence between S_r and S_{-r}.

Fact 3.1. *Let $u(x)$ be a polynomial of degree d and let $r \in \mathbb{Z} \setminus \{0\}$. Define $v(x) := -u(-x)$. Then*

$$u(x) \in L^d_{r,\emptyset} \text{ if and only if } v(x) \in L^d_{-r,\emptyset}.$$

Similarly,

$$u(x) \in N^d_{r,n} \text{ if and only if } v(x) \in N^d_{-r,n}, \text{ and } u(x) \in S_r \text{ if and only if } v(x) \in S_{-r}.$$

Proof. Since $v(-x) = -u(x)$, one obtains by induction that $v^{(n)}(-r) = -u^{(n)}(r)$, from which the fact follows. □

We will now state and prove the CRS lemma that was mentioned in the introduction. We will also justify its importance in understanding linear locally nilpotent polynomials.

Lemma 3.2 (CRS lemma). *Let $\alpha, \beta, \gamma \in \mathbb{Z} \setminus \{0\}$ be such that there is no $k \in \mathbb{Z}$ such that $\frac{\beta}{\gamma} = \alpha^k$. Then $\mathcal{P} \setminus \cup_{n\in\mathbb{N}} P(\gamma\alpha^n - \beta)$ is an infinite set.*

Proof. Suppose that $\mathcal{P} \setminus \cup_{n\in\mathbb{N}} P(\gamma\alpha^n - \beta)$ is a finite set. This means that the set $\cup_{n\in\mathbb{N}} P(\gamma\alpha^n - \beta)$ contains all but finitely many primes. Then $\cup_{n\in\mathbb{N}} P(\gamma\alpha^n - \beta) \setminus P(\gamma)$ also contains all but finitely many primes. So, for almost all $p \in \mathcal{P}_{P(\gamma)}$, one has $\alpha^{n_p} \equiv_p \beta\gamma^{-1}$ for some $n_p \in \mathbb{N}$ (the choice of n_p possibly depends on p). So, if $k \in \mathbb{N}$ is such that $\alpha^k \equiv_p 1$, then $(\beta\gamma^{-1})^k \equiv_p (\alpha^{n_p})^k \equiv_p 1$. Thus, taking $\alpha = x$, $\beta\gamma^{-1} = y$ and $F = \mathbb{Q}$ in Theorem 1 of [6], one arrives at a contradiction. It follows that $\mathcal{P} \setminus \cup_{n\in\mathbb{N}} P(\gamma\alpha^n - \beta)$ is an infinite set. □

Remark 3.3 (Importance of the CRS lemma)**.** Let $r \in \mathbb{Z} \setminus \{0\}$ and $u = u(x) = ax + b \in L^1_{r,\emptyset}$ with $a \neq \pm 1$. By the linear iteration formula, one obtains

$$u^{(n)}(r) = \frac{a^n(r - ar - b) + b}{1 - a}.$$

Since $u \in L^1_{r,\emptyset}$, one sees that $\mathcal{P} \setminus \cup_{n \in \mathbb{N}} P(\gamma\alpha^n - \beta)$ is a finite set (in fact, it is an empty set), where $\alpha = a, \beta = -b$ and $\gamma = r - ar - b$. It follows from Lemma 3.2 that either $\frac{\beta}{\gamma}$ or $\frac{\gamma}{\beta}$ is a power of α, i.e., $b = -a^m(r - ar - b)$, for some $m \in \mathbb{Z}$. Moreover, if $m \in \mathbb{N}$, one sees that $u \in N_r$. To summarize, if u is in S_r (with $a \notin \{\pm 1\}$), then there exists $m \in \mathbb{N} \cup \{0\}$ such that $a^m b = b + ar - r$.

Now we describe the idea of *reduction of polynomials* that was mentioned in the introduction. Let $r \in \mathbb{N}$ and $u = u(x) \in \mathbb{Z}[x]$ be such that $r | u(0)$. Define $v = v(x) := \frac{1}{r} u(rx)$. Note that v is a polynomial over $\mathbb{Z}$ of the same degree as u and $rv(1) = u(r)$. By induction, it readily follows that $rv^{(n)}(1) = u^{(n)}(r)$ for all $n \in \mathbb{N}$. Thus, $u(x)$ is weakly locally nilpotent at r outside some A if and only if $v(x)$ is weakly locally nilpotent at 1 outside $A \cup P(r)$, and, similarly, $u(x)$ is nilpotent at r if and only if $v(x)$ is nilpotent at 1. This means one can reduce any polynomial $u(x)$ in $L^d_{r,\emptyset}$ with the extra condition that $r|u(0)$ to a polynomial $v(x)$ in $L^d_{1,P(r)}$. We will call this the *reduction of* $u(x)$ *to* $v(x)$.

4. Arbitrary d and $r \in \{0, 1, -1\}$

In this section, we state and prove two theorems that classify all locally nilpotent polynomials at r when $r \in \{0, \pm 1\}$. We start with $r = 1$.

Theorem 4.1. *The following is the list of all polynomials in* $L_{1,\emptyset}$*:*

(1) $(x-1)p(x)$ *with* $p(x) \in \mathbb{Z}[x] \setminus \{0\}$ *(Nilpotent of nilpotency index 1),*

(2) $-2x + 4 + p(x)(x-1)(x-2)$ *with* $p(x) \in \mathbb{Z}[x]$ *(Nilpotent of nilpotency index 2),*

(3) $-2x^2 + 7x - 3 + p(x)(x-1)(x-2)(x-3)$ *with* $p(x) \in \mathbb{Z}[x]$ *(Nilpotent of nilpotency index 3), and*

(4) $x + 1$ *(Locally nilpotent but not nilpotent).*

Proof. Let $u = u(x) \in L^d_{1,\emptyset}$. We will consider the following three cases.

`Case 1.` Suppose that $u(1) - 1 \notin \{\pm 1\}$. Then $P(u(1) - 1) \neq \emptyset$, and for each $p \in P(u(1) - 1)$, one has $u(1) \equiv_p 1$, i.e., for each $p \in P(u(1) - 1)$, m_p does not exist. This is a contradiction to the hypothesis that $u \in L^d_{1,\emptyset}$.

Case 2. Suppose that $u(1)-1=-1$. These are the polynomials in Theorem 4.1(1).

Case 3. Finally, suppose that $u(1)-1=1$. We now explore the possibilities for $u(2)$. If $u(2)=0$, then $u(x)$ is of the form listed in Theorem 4.1(2). So suppose that $u(2)\neq 0$. Of course, $u(2)\notin\{1,2\}$, as otherwise one gets $u^{(n)}(1)=1$ or 2 for every $n\in\mathbb{N}$, a contradiction to our assumption that u is in $L^d_{1,\emptyset}$. Thus $u(2)$ is either less than or equal to -1, or greater than or equal to 3, i.e., $|u(2)-1|\geq 2$. In other words, $P(u(2)-1)\neq\emptyset$. Let $p\in P(u(2)-1)$. Then $u(2)\equiv_p 1$. As u is locally nilpotent at 1, p must be 2 so that $u(2)-1$ must be of the form $\pm 2^t$, for some $t\in\mathbb{N}$. To arrive at a contradiction, suppose that $u(2)\neq 3$. That means $u(2)$ is either greater than or equal to 4, or less than or equal to -1. We consider these two possibilities one by one.

If $u(2)\geq 4$, then $u(2)\geq 5$, as $u(2)-1=2^t$. Thus there exists $p\in\mathcal{P}_{\{2\}}$ such that $p\in P(u(2)-2)$, and $u^{(n)}(2)\equiv_p 2$ for every $n\in\mathbb{N}$, a contradiction to the hypothesis that $u\in L^d_{1,\emptyset}$.

If $u(2)\leq -1$, then $u(2)-2$ is odd and that it is less than or equal to -3, which follows as $u(2)-1=-2^t$. Using the same argument as above, one reaches a contradiction.

Thus $u(2)$ must be 3. Next, we look at $u(3)$. If $u(3)=0$, then $u(x)$ is of the form listed in Theorem 4.1(3). Suppose that $u(3)\neq 0$. For the same reason as above, $u(3)\notin\{0,1,2,3\}$. Thus $u(3)$ is either less than or equal to -1, or greater than or equal to 4. To get to a contradiction, suppose that $u(3)\neq 4$. Then $u(3)-3\notin\{0,\pm 1,-2,-3\}$, and so $P(u(3)-3)\neq\emptyset$. Let $p\in P(u(3)-3)$. Then $u(3)\equiv_p 3$, so that $p\in\{2,3\}$, because $u\in L^d_{1,\emptyset}$. If $p=2$, then $u(1)\equiv_p 0$. Thus $u(3)\equiv_p 3\equiv_p 1\not\equiv_p u(1)$, which is an impossibility, as $3\equiv_p 1$ must imply $u(3)\equiv_p u(1)$. This means $p=3$, and $u(3)-3=\pm 3^s$ for some $s\in\mathbb{N}$. For a similar reason, $P(u(3)-1)\neq\emptyset$, and for each $q\in P(u(3)-1)$, one has $u(3)\equiv_q 1$, which implies that $q\in\{2,3\}$. But $q|u(3)-1=2\pm 3^s$, which is a contradiction to the fact that $q\in\{2,3\}$. Thus $u(3)=4$.

Next, we look at $u(4)$. We claim that no further iteration of u at 1 can be zero and we would like to prove this by showing that $u(n-1)=n$ for all $n\geq 4$, and that would mean $u(x)=x+1$. We use induction on n to prove this claim. Let $n\geq 4$, and let $u(j-1)=j$ for every $4\leq j\leq n$. We want to show that $u(n)=n+1$. Since $u(1)=2,\ u(2)=3,\ u(3)=4,\ \ldots,$ and $u(n-1)=n$, there is a polynomial $p(x)$ such that $u(x)=x+1+p(x)(x-1)(x-2)(x-3)\cdots(x-n+1)$. Therefore $u(n)=n+1+p(n)\cdot(n-1)$, which must be different from 0 as $n\geq 4$. If $u(n)=i$ for some $i\in\{1,\ldots,n\}$, then the iterations $u^{(m)}(1)\in\{1,\ldots,n\}$ for every $m\in\mathbb{N}$, and that means m_p can only exist for finitely many primes p. Thus u cannot be locally nilpotent at 1, and $u(n)\notin\{0,\ldots,n\}$. This means $u(n)$ is either greater than or equal to $n+1$, or less than or equal to -1. For a contradiction, suppose that $u(n)\neq n+1$. Then either $u(n)-n$ is greater than or equal to 2, or less than or equal to $-(n+1)$. In either case, one has $P(u(n)-n) \neq \emptyset$. For each $p \in P(u(n)-n)$, one has $u(n) \equiv_p n$, which is an impossibility unless p is at most n. If possible, suppose that $p < n$. Then $n \equiv_p a$ for some $a \in \{1, \ldots, p-1\}$. Note that a cannot be 0, as otherwise $n \equiv_p 0$, so that $u(0) \equiv_p u(n) \equiv_p n \equiv_p 0$, i.e., $p|u(0)$, and so $p|u(p) = p+1$, an impossibility. Now by the induction hypothesis one gets $u(a) = a+1$, and also that $a \equiv_p n \equiv_p u(n) \equiv_p u(a)$, i.e., $u(a) \equiv_p a$. However, this is absurd as it means m_p does not exist. Thus $p = n$, i.e., n is prime, and $u(n) = n \pm n^s$ for some $s \in \mathbb{N}$. For a similar reason, $P(u(n)-1) \neq \emptyset$. Therefore for every $q \in P(u(n)-1)$, $u(n) \equiv_q 1$, and it follows that q is less than or equal to n. But if $q = n$, then $n = q|u(n)-1 = (n-1) \pm n^s$, and so $n|1$, an impossibility. Thus one obtains $q \leq n-1$. One can choose $b \in \{0, \ldots, q-1\}$ such that $n \equiv_q b+1$. By the induction hypothesis, $u(b+1) = b+2$, and also $u(b+1) \equiv_q u(n) \equiv_q 1$. These two relations together imply $b+1 \equiv_q 0$, i.e., $q|n$. But, as n is a prime, n must be q, which is an impossibility. Thus $u(n) = n+1$. □

Corollary 4.2. *It follows from Fact 3.1 and Theorem 4.1 that the following is the list of all polynomials in $L_{-1,\emptyset}$:*

(1) $(x+1)p(x)$ *with* $p(x) \in \mathbb{Z}[x] \setminus \{0\}$ *(Nilpotent of nilpotency index 1),*

(2) $-2x-4+p(x)(x+1)(x+2)$ *with* $p(x) \in \mathbb{Z}[x]$ *(Nilpotent of nilpotency index 2),*

(3) $2x^2+7x+3+p(x)(x+1)(x+2)(x+3)$ *with* $p(x) \in \mathbb{Z}[x]$ *(Nilpotent of nilpotency index 3), and*

(4) $x-1$ *(Locally nilpotent but not nilpotent).*

Corollary 4.3. *The sets S_1 and S_{-1} are singleton sets.*

Proof. Let $u(x) \in S_1$. Then by Theorem 4.1, $u(x)$ must be $x+1$, as all the other polynomials in the list (1)-(4) in there are in N_1. Now by Fact 3.1, it follows that $S_{-1} = \{x-1\}$. □

We end this section with the classification of locally nilpotent polynomials at 0.

Theorem 4.4. *The following is the list of all polynomials in $L_{0,\emptyset}$:*

(1) $x+b$ *with* $b \in \mathbb{Z} \setminus \{0\}$ *(Locally nilpotent but not nilpotent),*

(2) $ax+b$ *with* $P(b) \supseteq P(a) \neq \emptyset$ *and* $b \neq 0$ *(Locally nilpotent but not nilpotent),*

(3) $xp(x)$ *with* $p(x) \in \mathbb{Z}[x] \setminus \{0\}$ *(Nilpotent of nilpotency index 1), and*

(4) $(x-a)p(x)$ *with* $a \in \mathbb{Z} \setminus \{0\}$ *and* $p(x) \in \mathbb{Z}[x]$ *such that* $p(0) = -1$ *(Nilpotent of nilpotency index 2).*

Proof. First suppose that u is nilpotent of nilpotency index m for some $m \in \mathbb{N}$. If $u(0) = 0$, then $m = 1$, and $u(x) = xp(x)$ for some non-zero $p(x) \in \mathbb{Z}[x]$, as seen in Theorem 4.4(3). So suppose that $u(0) \neq 0$. Define

$$u_0 := u(0),\ u_n := u^{(n+1)}(0) - u^{(n)}(0),\ n \in \mathbb{N}.$$

Then $u_{n+1} = u^{(n+2)}(0) - u^{(n+1)}(0) = u(u^{(n+1)}(0)) - u(u^{(n)}(0))$. That means u_n divides u_{n+1} for all $n \in \mathbb{Z}_{\geq 0}$. One also has $u^{(m)}(0) = 0$, so $u_m = u^{(m+1)}(0) - u^{(m)}(0) = u^{(m+1)}(0) = u_0$. As $u_0|u_1|\dots|u_m = u_0$, it follows that $u_n = \pm u_0$ for all n. Also note that $u_0 + \cdots + u_{m-1} = u^{(m)}(0) = 0$. This means m must be even and half of these integers are positive, and the other half are negative (since $|u_n| = |u_0|$ for all n). Therefore there exists $k \in \{1, \dots, m-1\}$ such that $u_{k-1} = -u_k$, i.e., $u^{(k)}(0) - u^{(k-1)}(0) = u^{(k)}(0) - u^{(k+1)}(0)$, i.e., $u^{(k+1)}(0) = u^{(k-1)}(0)$. Thus $u^{(n+2)}(0) = u^{(n)}(0)$ for all $n \geq k-1$ and so, in particular, $0 = u^{(m)}(0) = u^{(m+2)}(0) = u^{(2)}(0)$. Hence $m = 2$ and $u(x) = (x-a)p(x)$, with $a \in \mathbb{Z} \setminus \{0\}$ and $p(x) \in \mathbb{Z}[x]$ with $p(0) = -1$; here $a = u(1)$, which is in Theorem 4.4(4).

Now suppose that $u \in S_0$. Then by Fact 1.1, it must be linear. Let $u(x) := ax + b, a \neq 0$. Note that $b \neq 0$, as otherwise u would be nilpotent. When $a = 1$, every $u(x) \in S_0$: in fact if $u(x) = x + b$, then by the linear iteration formula, $u^{(n)}(0) = b(1 + \cdots + 1) = bn$, which is non-zero for all $n \in \mathbb{N}$. For each prime p, one has $u^{(p)}(0) = bp \equiv_p 0$. When $a = -1$, $u^{(2)}(0) = 0$, so a must be different from -1. Throughout the rest of the proof, we assume that $|a| \geq 2$, i.e., $P(a)$ is a non-empty, finite set. Again, using the linear iteration formula, one obtains $u^{(n)}(0) = b(1 + \cdots + a^{n-1})$, $n \in \mathbb{N}$. Suppose, if possible, there exists some prime p in $P_{P(b)}(a)$, i.e., there is a prime p such that $p|a$ but $p \nmid b$. Then $u^{(n)}(0) \equiv_p b$ for every $n \in \mathbb{N}$, which means u cannot be locally nilpotent. Thus $P(b) \supseteq P(a) \neq \emptyset$. If $p \in P(b)$, then $m_p = 1$. If $p \notin P(b) \cup P(a-1)$, then $u^{(p-1)}(0) = \frac{b}{a-1}(a^{p-1} - 1) \equiv_p 0$, which follows from Fermat's Little Theorem. Finally, if $p \in P(a-1)$, then $u^{(p)}(0) = b(1 + \cdots + a^{p-1}) \equiv_p b(1 + \cdots + 1) \equiv_p 0$. Thus m_p exists for every $p \in \mathcal{P}$. □

The next corollary follows directly from the above theorem.

Corollary 4.5. *The following is the list of all polynomials in $S_{0,\emptyset}$:*

(1) $x + b$ with $b \in \mathbb{Z} \setminus \{0\}$, and

(2) $ax + b$, with $P(b) \supseteq P(a) \neq \emptyset$ and $b \neq 0$.

5. Linear Case of $d = 1$

In this section, we classify all polynomials that are locally nilpotent but non-nilpotent at r. Since the cases $r = 0$ and $r = \pm 1$ have been covered in the previous section, our focus here will be on the values of r that lie in $\mathbb{Z} \setminus \{0, \pm 1\}$. First, we state and prove a classification theorem for polynomials that are weakly locally nilpotent at 1 outside some given finite subset A of $\mathcal{P}$. We will use this theorem to prove our final main result, Theorem 5.3.

Theorem 5.1. *Let $A = \{q_1, \ldots, q_k\}$, where $q_1, \ldots, q_k$ are k distinct primes. Then the following is the list of all the polynomials in $L^1_{1,A}$:*

(1) $x \pm q_1^{s_1} \cdots q_k^{s_k}$, where $s_i \in \mathbb{N} \cup \{0\}$;

(2) $\alpha(x-1)$, where $\alpha \in \mathbb{Z} \setminus \{0\}$;

(3) $\pm q_1^{s_1} \cdots q_k^{s_k} x + 1$, where $s_i \in \mathbb{N} \cup \{0\}$ is such that $\sum s_i \geq 1$;

(4) $-2x - 1$ (only when $2 \in A$); and

(5) $-2x + 4$.

Proof. Let $u = u(x) \in L^1_{1,A}$. Then by Fact 1.1, it must be linear, say $u(x) = ax + b$. By the linear iteration formula, $u^{(n)}(1) = a^n + b(1 + \cdots + a^{n-1})$ for every $n \in \mathbb{N}$. It is clear that $b \neq 0$, as otherwise $u^{(n)}(1)$ would just be a^n, which cannot be divisible by any prime outside $P(a)$. Note that if $a = 1$, then $u^{(m_p)}(1) = 1 + bm_p \equiv_p 0$ for every prime $p \notin A$, i.e., $bm_p \equiv_p -1$ for every prime $p \notin A$, i.e., b is invertible in $\mathbb{F}_p$ for every prime $p \notin A$, i.e., b is equal to $\pm q_1^{s_1} \cdots q_k^{s_k}$ for some s_i's in $\mathbb{N} \cup \{0\}$. One can check that the polynomials $x \pm q_1^{s_1} \cdots q_k^{s_k}$ are indeed in $L^1_{1,A}$, whenever all s_i are in $\mathbb{N} \cup \{0\}$.

If $a = -1$, then $u(x) = -x + b$, and $u^{(2)}(x) = x$. Thus u cannot be in $L^1_{1,A}$ unless $b = 1$, and, in that case, it is in fact in $N^1_{1,1}$. Throughout the rest of the proof, we assume that $|a| \geq 2$. Similar to the proof of Theorem 4.1, one has the following three cases.

Case 1. Suppose that $u(1) - 1 \notin \{\pm 1\}$. This means $P(u(1) - 1) \neq \emptyset$, so $a + b = 1 \pm q_1^{s_1} \cdots q_k^{s_k}$, i.e., $b = 1 - a \pm q_1^{s_1} \cdots q_k^{s_k}$, for some $s_i \in \mathbb{N} \cup \{0\}$ with $\sum s_i \geq 1$. Then by the linear iteration formula, one has

$$u^{(n)}(1) = \frac{b \pm a^n(1 - a - b)}{1 - a},$$

for each $n \in \mathbb{N}$, and it follows from Remark 3.3 that there exists an $m \in \mathbb{Z}$ such that $b = \pm a^m(1 - a - b)$. If $m = 0$ then $b = \pm(1 - a - b)$, i.e., $a + 2b = 1$, as otherwise a would be 1. One also has $a + b = 1 \pm q_1^{s_1} \cdots q_k^{s_k}$. Solving a and b from these two equations one obtains $a = 1 \pm 2q_1^{s_1} \cdots q_k^{s_k}$, $b = \mp q_1^{s_1} \cdots q_k^{s_k}$. Therefore $u(x) = (1 \pm 2q_1^{s_1} \cdots q_k^{s_k})x \mp q_1^{s_1} \cdots q_k^{s_k}$, and so $u^{(n)}(1) = \frac{1 + (1 \pm 2q_1^{s_1} \cdots q_k^{s_k})^n}{2}$ for every $n \in \mathbb{N}$. Letting $\alpha = 1 \pm 2q_1^{s_1} \cdots q_k^{s_k}, \beta = -1$, and $\gamma = 1$, it is clear that neither $\frac{\beta}{\gamma}$ nor $\frac{\gamma}{\beta}$ is a power of α. It follows from Lemma 3.2 that $(1 \pm 2q_1^{s_1} \cdots q_k^{s_k})x \mp q_1^{s_1} \cdots q_k^{s_k} \notin L^1_{1,A}$. Thus m must be a non-zero integer. Let us consider the following possibilities.

If $m \in \mathbb{N}$ and $b = a^m(1-a-b)$, then $b(1+a^m) = a^m(1-a)$. Since $\gcd(a^m, a^m + 1) = 1$, one obtains $a^m + 1|1-a$, which is only possible if $m = 1$. (Similarly one treats the possibility $m = -n$ with $n \in \mathbb{N}$.) If $m \in \mathbb{N}$ and $b = -a^m(1-a-b)$, then $b(1-a^m) = -a^m(1-a)$, i.e., $b(1+\cdots+a^{m-1}) = -a^m$. Since $\gcd(1+\cdots+a^{m-1}, a^m) = 1$, one obtains $1 + \cdots + a^{m-1} = \pm 1$, which is only possible if $m \in \{1, 2\}$. (Similarly one treats the possibility $m = -n$ with $n \in \mathbb{N}$.) Thus one only needs to look at $m = \pm 1, \pm 2$, which we investigate in the following four subcases.

`Subcase 1.` Let $m = -1$. Here one has $ba = \pm(1-a-b)$. First, suppose that $ba = 1-a-b$, i.e., $b(a+1) = 1-a$. This means $a+1|a-1$, which is only possible if $a = -2$ and $a = -3$. These values generate the polynomials $u(x) = -2x - 3$ and $u(x) = -3x - 2$, respectively. When $u(x) = -2x - 3$, the linear iteration formula gives

$$u^{(n)}(1) = 2(-2)^n - 1.$$

Letting $\alpha = -2, \beta = 1$, and $\gamma = 2$, it is clear that neither $\frac{\beta}{\gamma}$ nor $\frac{\gamma}{\beta}$ is a power of α. Therefore, by Lemma 3.2, $-2x - 3 \notin L^1_{1,A}$. Similarly one can show that $-3x - 2 \notin L^1_{1,A}$.

Now suppose $ba = -(1-a-b)$. This gives $b = 1$ and hence $a = \pm q_1^{s_1} \cdots q_k^{s_k}$. Thus $u(x) = \pm q_1^{s_1} \cdots q_k^{s_k} x + 1$, and it follows from the linear iteration formula that for each $n \in \mathbb{N}$, one has

$$u^{(n)}(1) = (\pm q_1^{s_1} \cdots q_k^{s_k})^n + [1 + \cdots + (\pm q_1^{s_1} \cdots q_k^{s_k})^{n-1}] = \frac{1 - (\pm q_1^{s_1} \cdots q_k^{s_k})^{n+1}}{1 - (\pm q_1^{s_1} \cdots q_k^{s_k})}.$$

If $p \in P_A(1 - (\pm q_1^{s_1} \cdots q_k^{s_k}))$, then $u^{(p)}(1) \equiv_p p \equiv_p 0$. So suppose that $p \notin P_A(1 - (\pm q_1^{s_1} \cdots q_k^{s_k}))$. Now if $2 \in A$, then the existence of m_2 is not a concern; if $2 \notin A$, then $2 \in P_A(1-(\pm q_1^{s_1} \cdots q_k^{s_k}))$, which was covered above. Finally, if p is in $A \cup \{2\}$, then $u^{(p-2)}(1) \equiv_p 0$ by Fermat's Little Theorem. So $u(x) = \pm q_1^{s_1} \cdots q_k^{s_k} x + 1$ is in $L^1_{1,A}$.

`Subcase 2.` Let $m = 1$. Here one has $b = \pm a(1-a-b)$. First, suppose that $b = a(1-a-b)$, i.e., $b(a+1) = a(1-a)$. The same reasoning as above implies $a+1|a-1$, so the only possibilities one obtains are $(a, b) = (-2, 6)$ or $(-3, 6)$. These values produce the polynomials $u(x) = -2x + 6$, and $u(x) = -3x + 6$, respectively. When $u(x) = -2x + 6$, the linear iteration formula gives

$$u^{(n)}(1) = -(-2)^n + 2.$$

Letting $\alpha = -2, \beta = -2$, and $\gamma = -1$, it is clear that neither $\frac{\beta}{\gamma}$ nor $\frac{\gamma}{\beta}$ is a power of α. Therefore, by Lemma 3.2, $-2x + 6 \notin L^1_{1,A}$. Similarly, one can show that $-3x + 6 \notin L^1_{1,A}$.

`Subcase 3.` Let $m = -2$. Here one has $ba^2 = \pm(1-a-b)$. First, suppose $ba^2 = 1-a-b$, i.e., $b(a^2+1) = 1-a$. This means $a^2+1|a-1$, which is not possible, as $|1-a| \le 1+|a| < 1+a^2$. Thus $ba^2 = -(1-a-b)$, i.e., $b(a+1)=1$, i.e., $b = a+1 = \pm 1$. So $u(x) = -2x-1$. It follows from the linear iteration formula that

$$u^{(n)}(1) = (-2)^n - [1+\cdots+(-2)^{n-1}] = \frac{(-2)^{n+2}-1}{3},\ n \in \mathbb{N}.$$

It is easy to see that m_2 does not exist, $m_3 = 1$, and for all $p \in \mathcal{P}_{\{2,3\}}$, one has $u^{(p-3)}(1) \equiv_p 0$. So $-2x-1$ is in $L^1_{1,A}$ if and only if $2 \in A$.

Subcase 4. Let $m = 2$. Here one has $b = \pm a^2(1-a-b)$. First, suppose that $b = a^2(1-a-b)$, i.e., $b(1+a^2) = a^2(1-a)$. Since $\gcd(1+a^2, a^2) = 1$, one obtains $1+a^2|1-a$, which is impossible (see Subcase 3 above). So $b = -a^2(1-a-b)$, i.e., $b(a+1) = -a^2$ which means $a+1 = \pm 1$ and $b = \mp a^2$. Since $|a| \ge 2$, this means $a = -2$ and $b = 4$. But then $u(1)-1 = 1 \in \{\pm 1\}$, an impossibility in this case.

This concludes Case 1. Now we look at the remaining two cases.

Case 2. Suppose that $u(1)-1 = -1$. These are the polynomials in $N^1_{1,1}$.

Case 3. Finally, suppose that $u(1)-1 = 1$. If $u(2) = 0$, then $u(x) = -2x+4$. One can suppose that $u(2) \notin \{0,1,2\}$, i.e., $u(2)$ is either less than or equal to -1, or greater than or equal to 3, i.e., $|u(2)-1| \ge 2$, i.e., $P(u(2)-1) \ne \emptyset$. If $u(2) = 3$, then $u(x) = x+1 \in S_1$. Thus one can further assume that $u(2) \ne 3$. Since $u(1) = 2$, $b = 2-a$ and so $u(x) = ax+(2-a)$. Then by the linear iteration formula, one obtains

$$u^{(n)}(1) = \frac{2-a-a^n}{1-a},\quad n \in \mathbb{N}.$$

Since $u \in L^1_{1,A}$, it follows from Remark 3.3 that $2-a = a^m$, for some $m \in \mathbb{Z}$. Note that m cannot be a non-positive integer as otherwise it would follow that a must be equal to ± 1. Thus $m \in \mathbb{N}$ and $2 = a(1+a^{m-1})$. Therefore $a = \pm 2$ and $1+a^{m-1} = \pm 1$, i.e., $a^{m-1} = -2$, i.e., $a = -2$. But $a = -2$ implies that $b = 4$ and hence $u(2) = 2a+b = 0$, which cannot happen as $u(2) \notin \{0,1,2,3\}$. Thus $ax+(2-a) \notin L^1_{1,A}$. □

The next corollary follows directly from Theorem 5.1.

Corollary 5.2. *Let $A = \{q_1,\ldots,q_k\}$, where $q_1,\ldots,q_k$ are k distinct primes. Then the following is the list of all polynomials in $L^1_{1,A} \setminus N_1$:*

(1) $x + q_1^{s_1}\cdots q_k^{s_k}$, where $s_i \in \mathbb{N}\cup\{0\}$;

(2) $x - q_1^{s_1}\cdots q_k^{s_k}$, where $s_i \in \mathbb{N}\cup\{0\}$ such that $\sum s_i \ge 1$;

(3) $\pm q_1^{s_1}\cdots q_k^{s_k}x + 1$, where $s_i \in \mathbb{N}\cup\{0\}$ such that $\sum s_i \ge 1$; and

(4) $-2x-1$ (only when $2 \in A$).

Finally, we state and prove the last (main) result of this paper.

Theorem 5.3. *Let r be a natural number greater than or equal to 2 and $r = q_1^{a_1} \cdots q_k^{a_k}$ be its prime decomposition. Then the following is the list of all polynomials in S_r:*

(1) $x + q_1^{s_1} \cdots q_k^{s_k}$, where $s_i \in \mathbb{N} \cup \{0\}$;

(2) $x - q_1^{s_1} \cdots q_k^{s_k}$, where $s_i \in \mathbb{N} \cup \{0\}$ with at least one $j \in \{1, \dots, k\}$ such that $s_j > a_j$;

(3) $\pm q_1^{s_1} \cdots q_k^{s_k} x + r$, where $s_i \in \mathbb{N} \cup \{0\}$ with $\sum\limits_i s_i \geq 1$; and

(4) $-2x - r$ (only when r is even).

Proof. Let $u = u(x) \in S_r$ and $A := P(r)$. Then by Fact 1.1, u must be linear, say $u(x) = ax + b$. First, we will look at the instances when $a = \pm 1$. Note that if $a = 1$, then $u^{(m_p)}(r) = r + bm_p \equiv_p 0$ for every prime p, i.e., $bm_p \equiv_p -r$ for every prime p, i.e., b is invertible in $\mathbb{F}_p$ for every prime $p \notin A$, i.e., b is equal to $\pm q_1^{s_1} \cdots q_k^{s_k}$ for some s_i's in $\mathbb{N} \cup \{0\}$. Thus when $a = 1$, one expects $u(x)$ to be of the form $x \pm q_1^{s_1} \cdots q_k^{s_k}$. First, suppose that $u(x) = x + q_1^{s_1} \cdots q_k^{s_k}$. Then by the linear iteration formula, $u^{(n)}(r) = q_1^{a_1} \cdots q_k^{a_k} + n \cdot q_1^{s_1} \cdots q_k^{s_k}$, which is always nonzero for every $n \in \mathbb{N}$. One can check that these polynomials are locally nilpotent, and they are in Theorem 5.3(1). Now suppose that $u(x) = x - q_1^{s_1} \cdots q_k^{s_k}$. Then by the linear iteration formula, $u^{(n)}(r) = q_1^{a_1} \cdots q_k^{a_k} - n \cdot q_1^{s_1} \cdots q_k^{s_k}$ for all $n \in \mathbb{N}$. If, for all $i \in \{1, \dots, k\}$, $s_i \leq a_i$, then one has $u^{(q_1^{a_1-s_1} \cdots q_k^{a_k-s_k})}(r) = 0$, which is a contradiction, as u is non-nilpotent. That means one must have at least one $j \in \{1, \dots, k\}$ such that $a_j < s_j$. It can now be checked that u is non-nilpotent but locally nilpotent, and so one obtains the polynomials in Theorem 5.3(2).

If $a = -1$, $u(x) = -x + b$ and $u^{(2)}(x) = x$. Therefore u cannot be in $L^1_{r,\emptyset}$ unless $b = r$, and, in that case, it is in fact in $N^1_{r,1}$, a contradiction. Thus $a \neq -1$. Throughout the rest of the proof, we suppose that $|a| \geq 2$. It follows from Remark 3.3 that there exists an $m \in \mathbb{N} \cup \{0\}$ such that $a^m b = b + ar - r$. If $m = 0$, then $r(1 - a) = 0$, which is an impossibility, as $r \neq 0$ and $|a| \geq 2$. That means $m \in \mathbb{N}$ and $b(a^m - 1) = r(a - 1)$, i.e., $b(1 + \cdots + a^{m-1}) = r$, and so $b|r$.

We want to show that $u(r) - r \notin \{\pm 1\}$. Suppose otherwise, i.e., $u(r) = r \pm 1$. This means $b = r - ar \pm 1$, i.e., $u(x) = ax + (r - ar \pm 1)$. We will only consider the possibility $b = r - ar - 1$ as the other possibility can be rejected using the same argument. Applying the linear iteration formula, one obtains

$$u^{(n)}(r) = \frac{a^n + r - ar - 1}{1 - a} = \frac{a^n + b}{1 - a} \quad \text{for all } n \in \mathbb{N}.$$

From Remark 3.3, it follows that $r - ar - 1 = -a^t$, for some $t \in \mathbb{Z}$. It is clear that $t \neq 0$, as otherwise $r - ar = 0$, i.e., $r(1 - a) = 0$, i.e., either $r = 0$ or $a = 1$, which is not true. If $t = -n$ for some $n \in \mathbb{N}$, then $a^n(r - ar - 1) = -1$, again an impossibility, as $|a| \geq 2$. Thus $t \in \mathbb{N}$, and $r(1-a) = 1 - a^t$, i.e., $r = 1 + \cdots + a^{t-1}$. That means $t \geq 2$, $a|r-1$, and $u^{(t)}(r) = 0$, i.e., u is nilpotent at r, a contradiction. Thus $u(r) - r$ cannot be a unit, and $u(r) = r \pm q_1^{s_1} \cdots q_k^{s_k}$ for suitable s_i's in $\mathbb{N} \cup \{0\}$ with $\sum_i s_i \geq 1$. Thus $b = r - ar \pm q_1^{s_1} \cdots q_k^{s_k}$. However, $b|r$ implies that $b|q_1^{s_1} \cdots q_k^{s_k}$, i.e., there exist $t_i \in \mathbb{N} \cup \{0\}$ with $t_i \leq s_i$ for every i such that $b = \pm q_1^{t_1} \cdots q_k^{t_k}$. From $b = r - ar \pm q_1^{s_1} \cdots q_k^{s_k}$, one obtains $ra = r - b \pm q_1^{s_1} \cdots q_k^{s_k} = r - b(\pm 1 \pm q_1^{s_1 - t_1} \cdots q_k^{s_k - t_k})$, i.e., $r|b(\pm 1 \pm q_1^{s_1 - t_1} \cdots q_k^{s_k - t_k})$. Suppose, if possible, all the t_i's are zero. Then $b = \pm 1$, and so r must divide $\pm 1 \pm q_1^{s_1} \cdots q_k^{s_k}$, which is clearly absurd, as $\gcd(r, \pm 1 \pm q_1^{s_1} \cdots q_k^{s_k}) = \gcd(q_1^{a_1} \cdots q_k^{a_k}, \pm 1 \pm q_1^{s_1} \cdots q_k^{s_k}) = 1$. Thus $\sum_i t_i \geq 1$. All of these now reduce to the following two cases.

Case 1. There exists $j \in \{1, \ldots, k\}$ such that $s_j > t_j$. Since

$$\gcd(r, \pm 1 \pm q_1^{s_1 - t_1} \cdots q_k^{s_k - t_k}) = 1,$$

r must divide b, so one can deduce that $r = \pm b$. Thus $a_i = t_i \leq s_i$ for all $i \in \{1, \ldots, k\}$. We use the technique of reduction of polynomials here. Define $v = v(x) := \frac{1}{r} u(rx) = ax \pm 1$. Then

$$v(1) = \frac{1}{r} u(r) = \frac{1}{r}(r \pm q_1^{s_1} \cdots q_k^{s_k}) = 1 \pm q_1^{s_1 - a_1} \cdots q_k^{s_k - a_k}$$

and $v \in L_{1,A}^1 \setminus N_1$. It now follows from the list in Corollary 5.2 that one has two possibilities for v (since $|a| \geq 2$):

(i) $v(x) = \pm q_1^{s_1 - a_1} \cdots q_k^{s_k - a_k} x + 1$, in which case $u(x) = \pm q_1^{s_1 - a_1} \cdots q_k^{s_k - a_k} x + r$, or

(ii) $v(x) = -2x - 1$ (only when $2 \in A$), in which case $u(x) = -2x - r$.

One can check that both (i) and (ii) are indeed in S_r.

Case 2. For all $i \in \{1, \ldots, k\}$, $s_i = t_i$. Then $\pm q_1^{s_1} \cdots q_k^{s_k} = b|r$, i.e., $a_i \geq s_i$ for each i. From $b = r - ar \pm q_1^{s_1} \cdots q_k^{s_k}$, one obtains $r(1-a) = \pm 2 q_1^{s_1} \cdots q_k^{s_k} = \pm 2b$. Thus either $r = \pm b$ or $r = \pm 2b$. The first possibility has been taken care of in Case 1. So one can assume that $r = 2 q_1^{s_1} \cdots q_k^{s_k} = \pm 2b$. That would mean $a = 2$ and that $2 \in A$. Without loss of generality, let $q_1 = 2$, and so $r = 2^{s_1 + 1} \cdots q_k^{s_k}$. Rewriting $b = r - ar \pm q_1^{s_1} \cdots q_k^{s_k}$ gives us $2r = r - 2b$, i.e., $r = -2b$. This means $u(x) = 2x - \frac{r}{2}$. It follows from the linear iteration formula that

$$u^{(n)}(r) = \frac{r}{2} \cdot (2^n + 1), \; n \in \mathbb{N}.$$

Letting $\alpha = 2, \beta = -1, \gamma = 1$, one sees that neither $\frac{\beta}{\gamma}$ nor $\frac{\gamma}{\beta}$ is a power of α. Thus from Lemma 3.2, $\mathcal{P} \setminus P(2^n + 1)$ is an infinite set so that $\mathcal{P} \setminus P(\frac{r}{2} \cdot (2^n + 1))$ is also an infinite set. So $2x - \frac{r}{2} \notin S_r$. This completes the proof. □

From Fact 3.1 and Theorem 5.3 the next corollary is immediate.

Corollary 5.4. *If $r = -q_1^{a_1} \cdots q_k^{a_k}$ is the prime decomposition of an integer $r \leq -2$, then the following is the list of all polynomials in S_r:*

(1) $x - q_1^{s_1} \cdots q_k^{s_k}$, where $s_i \in \mathbb{N} \cup \{0\}$;

(2) $x + q_1^{s_1} \cdots q_k^{s_k}$, where $s_i \in \mathbb{N} \cup \{0\}$ with at least one $j \in \{1, \ldots, k\}$ such that $s_j > a_j$;

(3) $\pm q_1^{s_1} \cdots q_k^{s_k} x - r$, where $s_i \in \mathbb{N} \cup \{0\}$ with $\sum_i s_i \geq 1$; and

(4) $-2x + r$ (only when r is even).

6. Some Open Problems

For $u(x)$, a non-constant polynomial over $\mathbb{Z}$, let

$$N(u) := \{r \in \mathbb{Z} \mid u \in N_r\}, \quad LN(u) := \{r \in \mathbb{Z} \mid u \in L_{r,\emptyset}\}.$$

Then one can consider the following problems:

Q1. Describe all u's such that $N(u)$ is finite.

Q2. Describe all u's such that $LN(u)$ is finite.

Q3. Given $r \in \mathbb{Z}$, describe all u's such that $r \in LN(u)$.

We would like to say a few words about the problems Q1-Q3. The methods used in the paper are useful for linear polynomials, and due to Fact 1.1, we were able to achieve our goal by studying the linear polynomials only. It is clear that if u is assumed to be linear, then $N(u)$ is finite for every u except for the polynomials of the form $\pm x \pm c$, $c \in \mathbb{Z} \setminus \{0\}$. This answers Q1 for linear polynomials $u(x)$. It should be noted that $LN(u) = N(u) \cup \{r \in \mathbb{Z} \mid u \in S_r\}$. Therefore, for Q2, due to Fact 1.1 again, if the degree of u is greater than or equal to 2, then $LN(u)$ is finite so that $N(u)$ is finite. For linear polynomials of the form $\pm x \pm c$, $c \in \mathbb{Z} \setminus \{0\}$, $N(u)$ is infinite and so $LN(u)$ is infinite. If $u = ax + b$ with $a \neq 1$, then one readily sees that $u^{(n)}(r) = \frac{a^n(r-a-b)+b}{1-a}$. Note that $\frac{b}{a+b-r} = a^k$ for some $k \in \mathbb{Z}$, can only be true for finitely many values of r. So it follows from Lemma 3.2 that $\mathcal{P} \setminus \cup_{n \in \mathbb{N}} P((r-a-b)a^n + b)$ is finite for only finitely many values of r. Thus for these polynomials, $LN(u)$ is indeed finite. In this paper, we have fully classified S_r for every integer r. Also, given an r, using the linear iteration formula, it should be easy enough to describe the linear u's such that $r \in N(u)$. Therefore we have a partial answer for Q3 here. Thus if one knows enough about the form of the nilpotent polynomials of degree higher than or equal to 2, one should potentially be able to answer all of the questions above. This is a work in progress and it is of course important enough to be considered as a separate work.

Acknowledgements. The author acknowledges his Professors Alexander Borisov and Adrian Vasiu, for their constant support, encouragement, and very helpful suggestions. The author would also like to thank Professor Jeremy Rouse for suggesting [6], which was one of the main tools used to prove Theorems 5.1 and 5.3; Professor Kiran Kedlaya for maintaining a wonderful archive of William Lowell Putnam Mathematics Competition questions and answers here `https://kskedlaya.org/putnam-archive/`, which was very helpful in the proof of Theorem 4.4; and also Dr. Sarah Lamoureux for proofreading the manuscript and providing numerous helpful suggestions that greatly improved the formatting and the readability of the manuscript. Finally, the author would like to thank Professor Thomas Tucker for his suggestion to use Theorem 5 of [2], which led to Fact 1.1 and that was very useful to reduce the possible candidates for locally nilpotent polynomials.

References

[1] J. P. Bell, D. Ghioca, and T. J. Tucker, The dynamical Mordell-Lang conjecture, *Math. Surveys Monogr.*, **210** (2016), xiv+280 pp.

[2] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. J. Tucker, Periods of rational maps modulo primes, *Math. Ann.*, **355** (2013), 637-660.

[3] R. Benedetto, D. Ghioca, P. Kurlberg, T. J. Tucker, and U. Zannier, A case of the dynamical Mordell-Lang conjecture (with an appendix by Umberto Zannier), *Math. Ann.* **352** (2012), 1-26.

[4] A. Borisov, Iterations of integer polynomial maps modulo primes, *J. Integer Seq.* Vol. **16** (2013), Article 13.8.3.

[5] A. Borisov, Geometrically nilpotent subvarieties, *Finite Fields Appl.*, **50** (2018), 366-371.

[6] C. Corrales-Rodrigáñez, and R. Schoof, The support problem and its elliptic analogue, *J. Number Theory*, **64** (1997), Article No. NT972114, 276-290.

[7] R. W. K. Odoni, The Galois theory of iterates and composites of polynomials, *Proc. Lond. Math. Soc. (3)* **51** (1985), 385-414.

[8] J. H. Silverman, Integer points, Diophantine approximation, and iteration of rational maps, *Duke Math. J.* **71**(3) (1993), 793-829.

[9] M. J. T. Vasiga, and J. O. Shallit, On the iteration of certain quadratic maps over GF(p), *Discrete Math.*, **277** (2004), no. 1-3, 219-240.