DIGIT PATTERNS AND THE FORMAL ADDITIVE GROUP

GREG W. ANDERSON

Abstract. We prove an elementary result concerning the relationship between the multiplicative groups of the coordinate and endomorphism rings of the formal additive group over a field of characteristic $p > 0$. Both statement and proof of the main result involve the combinatorics of base p representations of positive integers in a striking way.

1. Introduction

Our main result (Theorem 1.2 below) concerns the relationship between the multiplicative groups of the coordinate and endomorphism rings of the formal additive group over a field of characteristic $p > 0$. Our result is elementary and does not require a great deal of apparatus for its statement. Both statement and proof of the main result involve the combinatorics of base p representations of positive integers in a striking way.

1.1. Statement of the main result.

1.1.1. *Rings and groups of power series.* Fix a prime number p and a field K of characteristic p. Let q be a power of p. Consider: the (commutative) power series ring

$$K[[X]] = \left\{ \sum_{i=0}^{\infty} a_i X^i \,\middle|\, a_i \in K \right\};$$

the (in general noncommutative) ring

$$R_{q,K} = \left\{ \sum_{i=0}^{\infty} a_i X^{q^i} \,\middle|\, a_i \in K \right\},$$

in which by definition multiplication is power series composition; and the subgroup

$$\Gamma_{q,K} = \left\{ X + \sum_{i=1}^{\infty} a_i X^{q^i} \,\middle|\, a_i \in K \right\} \subset R_{q,K}^{\times},$$

where in general $A^{\times}$ denotes the group of units of a ring A with unit. Note that $K[[X]]^{\times}$ is a right $\Gamma_{q,K}$-module via composition of power series.

Date: February 25, 2006.
MSC-classification: 11S31.
Keywords: characteristic p, formal additive group, digit expansions.

1.1.2. *Logarithmic differentiation.* Given $F = F(X) \in K[[X]]^\times$, put

$$\mathbf{D}[F](X) = XF'(X)/F(X) \in XK[[X]].$$

Note that

$$\mathbf{D}[F(\alpha X)] = \mathbf{D}[F](\alpha X) \tag{1}$$

for all $\alpha \in K^\times$. Note that the sequence

(2)

$$1 \to K[[X^p]]^\times \subset K[[X]]^\times \xrightarrow{\mathbf{D}} \left\{ \sum_{i\in\mathbb{N}} a_i X^i \in XK[[X]] \,\middle|\, a_{pi} = a_i^p \text{ for all } i \in \mathbb{N} \right\} \to 0$$

is exact, where $\mathbb{N}$ denotes the set of positive integers.

1.1.3. *q-critical integers.* Given $c \in \mathbb{N}$, let

$$O_q(c) = \{n \in \mathbb{N} | (n,p) = 1 \text{ and } n \equiv p^i c \bmod q-1 \text{ for some } i \in \mathbb{N}\cup\{0\}\}.$$

Given $n \in \mathbb{N}$, let $\operatorname{ord}_p n$ denote the exact order with which p divides n. We define

$$C_q^0 = \left\{ c \in \mathbb{N} \cap (0,q) \,\middle|\, (c,p) = 1 \text{ and } \frac{c+1}{p^{\operatorname{ord}_p(c+1)}} = \min_{n \in O_q(c)\cap(0,q)} \frac{n+1}{p^{\operatorname{ord}_p(n+1)}} \right\},$$

and we call elements of this set *q-critical integers.* In the simplest case $p = q$ one has $C_p^0 = \{1,\ldots,p-1\}$, but in general the set C_q^0 is more complicated. Put

$$C_q = \bigcup_{c\in C_q^0} \{q^i(c+1) - 1 | i \in \mathbb{N}\cup\{0\}\}.$$

Note that the union is disjoint, since the sets in the union are contained in different congruence classes modulo $q-1$. See below for informal "digital" descriptions of the sets C_q^0 and C_q.

1.1.4. *The homomorphism ψ_q.* We define a homomorphism

$$\psi_q : XK[[X]] \to X^2 K[[X]]$$

as follows: given $F = F(X) = \sum_{i\in\mathbb{N}} a_i X^i \in XK[[X]]$, put

$$\psi_q[F] = X \cdot \sum_{k\in C_q} a_k X^k.$$

Note that the composite map

$$\psi_q \circ \mathbf{D} : K[[X]]^\times \to \left\{ \sum_{k\in C_q} a_k X^{k+1} \,\middle|\, a_k \in K \right\}$$

is surjective by exactness of sequence (2). Further, since the set $\{k+1 | k \in C_q\}$ is stable under multiplication by q, the target of $\psi_q \circ \mathbf{D}$ comes equipped with the structure of left $R_{q,K}$-module. More precisely, the target of $\psi_q \circ \mathbf{D}$ is a free left $R_{q,K}$-module for which the set $\{X^{k+1} | k \in C_q^0\}$ is a basis.

The following is the main result of the paper.

Theorem 1.2. *The formula*

$$\psi_q[\mathbf{D}[F\circ\gamma]] = \gamma^{-1} \circ \psi_q[\mathbf{D}[F]] \tag{3}$$

holds for all $\gamma \in \Gamma_{q,K}$ and $F \in K[[X]]^\times$.

In §§2–4 we give the proof of the theorem. More precisely, we first explain in §2 how to reduce the proof of the theorem to a couple of essentially combinatorial assertions (Theorems 2.2 and 2.3 below), and then we prove the latter in §3 and §4, respectively.

1.3. **Informal discussion.**

1.3.1. *"Digital" description of* C_q^0. The definition of C_q^0 can readily be understood in terms of simple operations on digit strings. For example, to verify that 39 is 1024-critical, begin by writing out the base 2 representation of 39 thus:

$$39 = 100111_2$$

Then put enough place-holding 0's on the left so as to represent 39 by a digit string of length $\mathrm{ord}_2\, 1024 = 10$:

$$39 = 0000100111_2$$

Then calculate as follows:

$$\begin{array}{cclr}
\text{permute cyclically} & 0000100111_2 & \xrightarrow{\text{strike trailing 1's and leading 0's}} & 100_2 \\
 & 0001001110_2 & \text{ignore: terminates with a 0} & \\
 & 0010011100_2 & \text{ignore: terminates with a 0} & \\
\downarrow & 0100111000_2 & \text{ignore: terminates with a 0} & \\
 & 1001110000_2 & \text{ignore: terminates with a 0} & \\
 & 0011100001_2 & \xrightarrow{\text{strike trailing 1's and leading 0's}} & 1110000_2 \\
 & 0111000010_2 & \text{ignore: terminates with a 0} & \\
 & 1110000100_2 & \text{ignore: terminates with a 0} & \\
\downarrow & 1100001001_2 & \xrightarrow{\text{strike trailing 1's and leading 0's}} & 110000100_2 \\
 & 1000010011_2 & \xrightarrow{\text{strike trailing 1's and leading 0's}} & 10000100_2
\end{array}$$

Finally, conclude that 39 is 1024-critical because the first entry of the last column is the smallest in that column. This numerical example conveys some of the flavor of the combinatorial considerations coming up in the proof of Theorem 1.2.

1.3.2. *"Digital" description of* C_q. Given $c \in C_q^0$, let $[c_1, \cdots, c_m]_p$ be a string of digits representing c in base p. (The digit string notation is defined below in §2.) Then each digit string of the form

$$[c_1, \ldots, c_m, \underbrace{p-1, \ldots, p-1}_{n\, \mathrm{ord}_p\, q}]_p$$

represents an element of C_q. Moreover, each element of C_q arises this way, for unique $c \in C_q^0$ and $n \in \mathbb{N} \cup \{0\}$.

1.3.3. *Miscellaneous remarks.*

(i) Theorem 1.2 will be applied in a joint work with D. Thakur on Ihara power series for $\mathbb{F}_q[t]$. The theorem will be used to extract arithmetical information from the Coleman-type power series which arise as values of the Ihara-type cocycle which we construct.

(ii) The set C_q is a subset of the set of *magic numbers* (relative to q) as defined and studied in [Goss, §8.22, p. 309]. For now we only understand this connection "numerologically" but we suspect that it goes much deeper. See [Thak] for further material on digit phenomena in function field arithmetic.

(iii) A well-ordering of the set of positive integers distinct from the usual one, which we call the *p-digital well-ordering*, plays a key role in the proof of Theorem 1.2, via Theorems 2.2 and 2.3 below. In particular, Theorem 2.3, via Proposition 2.4, characterizes the sets C_q^0 and C_q in terms of the p-digital well-ordering and congruences modulo $q-1$.

(iv) The results of this paper were discovered by extensive computer experimentation with base p expansions and binomial coefficients modulo p. No doubt refinements of our results can be discovered by continuing such experiments.

(v) It is an open problem to find a minimal set of generators for $K[[X]]^\times$ as a topological right $\Gamma_{q,K}$-module, the topologies here being the X-adically induced ones. It seems very likely that the module is always infinitely generated, even when K is a finite field. Computer experimentation (based on the method of proof of Proposition 2.5 below) with the simplest case of the problem (in which K is the two-element field and $p = q = 2$) has revealed some interesting patterns. But still we are unable to hazard any detailed guess about the solution.

2. Reduction of the proof

In this section we explain how to reduce the proof of Theorem 1.2 to a couple of combinatorial assertions.

2.1. **Digital apparatus.**

2.1.1. *Base p expansions.* Given an additive decomposition

$$n = \sum_{i=1}^{s} n_i p^{s-i} \quad (n_i \in \mathbb{Z} \cap [0,p),\ n \in \mathbb{N}),$$

we write

$$n = [n_1, \ldots, n_s]_p,$$

we call the latter a *base p expansion* of n and we call the coefficients n_i *digits*. Note that we allow base p expansions to have leading 0's. We say that a base p expansion is *minimal* if the first digit is positive. For convenience, we set the empty base p expansion $[]_p$ equal to 0 and declare it to be minimal. We always read base p expansions left-to-right, as though they were words spelled in the alphabet $\{0, \ldots, p-1\}$. In this notation the well-known theorem of Lucas takes the form

$$\left(\begin{array}{c} [a_1, \ldots, a_n]_p \\ [b_1, \ldots, b_n]_p \end{array}\right) \equiv \left(\begin{array}{c} a_1 \\ b_1 \end{array}\right) \cdots \left(\begin{array}{c} a_n \\ b_n \end{array}\right) \bmod p.$$

(For all $n \in \mathbb{N} \cup \{0\}$ and $k \in \mathbb{Z}$ we set $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ if $0 \leq k \leq n$ and $\binom{n}{k} = 0$ otherwise.) The theorem of Lucas implies that for all integers $k, \ell, m \geq 0$ such that $m = k + \ell$, the binomial coefficient $\binom{m}{k}$ does not vanish modulo p if and only if the addition of k and ℓ in base p requires no "carrying".

2.1.2. *The p-core function κ_p.* Given $n \in \mathbb{N}$, we define

$$\kappa_p(n) = (n/p^{\mathrm{ord}_p n} + 1)/p^{\mathrm{ord}_p (n/p^{\mathrm{ord}_p n} + 1)} - 1.$$

We call $\kappa_p(n)$ the *p-core* of n. For example, $\kappa_p(n) = 0$ iff $n = p^{k-1}(p^\ell - 1)$ for some $k, \ell \in \mathbb{N}$. The meaning of the p-core function is easiest to grasp in terms of minimal base p expansions. One calculates $\kappa_p(n)$ by discarding trailing 0's and then discarding trailing $(p-1)$'s. For example, to calculate the 3-core of $963 = [1, 0, 2, 2, 2, 0, 0]_3$, first discard trailing 0's to get $[1,0,2,2,2]_3 = 107$, and then discard trailing 2's to get $\kappa_3(963) = [1,0]_3 = 3$.

2.1.3. *The p-defect function δ_p.* For each $n \in \mathbb{N}$, let $\delta_p(n)$ be the length of the minimal base p representation of $\kappa_p(n)$. We call $\delta_p(n)$ the *p-defect* of n. For example, since as noted above $\kappa_3(963) = [1,0]_3$, one has $\delta_3(963) = 2$.

2.1.4. *The p-digital well-ordering.* We equip the set of positive integers with a well-ordering $\leq_p$ by declaring $m \leq_p n$ if

$$\kappa_p(m) < \kappa_p(n)$$

or

$$\kappa_p(m) = \kappa_p(n) \text{ and } m/p^{\operatorname{ord}_p m} < n/p^{\operatorname{ord}_p n}$$

or

$$\kappa_p(m) = \kappa_p(n) \text{ and } m/p^{\operatorname{ord}_p m} = n/p^{\operatorname{ord}_p n} \text{ and } m \leq n.$$

In other words, to verify $m \leq_p n$, first compare p-cores of m and n, then in case of a tie compare numbers of $(p-1)$'s trailing the p-core, and then in case of yet another tie compare numbers of trailing 0's. We call $\leq_p$ the *p-digital well-ordering.* In the obvious way we derive order relations $<_p$, $\geq_p$ and $>_p$ from $\leq_p$. We remark that

$$\delta_p(m) < \delta_p(n) \Rightarrow m <_p n, \quad m \leq_p n \Rightarrow \delta_p(m) \leq \delta_p(n);$$

in other words, the function δ_p gives a reasonable if rough approximation to the p-digital well-ordering.

2.1.5. *The function μ_q.* Given $c \in \mathbb{N}$, let $\mu_q(c)$ be the unique element of the set

$$\{n \in \mathbb{N} | n \equiv p^i c \bmod q-1 \text{ for some } i \in \mathbb{N} \cup \{0\}\}$$

minimal with respect to the p-digital well-ordering. Note that $\mu_q(c)$ cannot be divisible by p. Consequently $\mu_q(c)$ may also be characterized as the unique element of the set $O_q(c)$ minimal with respect to the p-digital well-ordering.

2.1.6. *p-admissibility.* We say that a quadruple $(j,k,\ell,m) \in \mathbb{N}^4$ is *p-admissible* if

$$(m,p) = 1, \quad m = k + j(p^\ell - 1), \quad \left(\begin{array}{c} k-1 \\ j \end{array}\right) \not\equiv 0 \bmod p.$$

This is the key technical definition of the paper. Let $\mathcal{A}_p$ denote the set of p-admissible quadruples.

Theorem 2.2. *For all $(j,k,\ell,m) \in \mathcal{A}_p$, one has (i) $k <_p m$, and moreover (ii) if $\kappa_p(k) = \kappa_p(m)$, then $j = (p^{\operatorname{ord}_p k} - 1)/(p^\ell - 1)$.*

We will prove this result in §3. Note that the conclusion of part (ii) of the theorem implies $\operatorname{ord}_p k > 0$ and $\ell | \operatorname{ord}_p k$.

Theorem 2.3. *One has*

$$\max_{c \in \mathbb{N}} \mu_q(c) < q, \tag{4}$$

$$\begin{aligned} &\{(\mu_q(c)+1)q^i - 1 \mid i \in \mathbb{N} \cup \{0\},\ c \in \mathbb{N}\} \\ = &\left\{c \in \mathbb{N} \,\middle|\, (c,p) = 1,\ \kappa_p(c) = \min_{n \in O_q(c)} \kappa_p(n)\right\}. \end{aligned} \tag{5}$$

We will prove this result in §4. We have phrased the result in a way emphasizing the p-digital well-ordering. But perhaps it is not clear what the theorem means in the context of Theorem 1.2. The next result provides an explanation.

Proposition 2.4. *Theorem 2.3 granted, one has*

$$C_q^0 = \{\mu_q(c) | c \in \mathbb{N}\}, \tag{6}$$

$$C_q = \{c \in \mathbb{N} \,|\, (c,p) = 1,\ \kappa_p(c) = \kappa_p(\mu_q(c))\}\,. \tag{7}$$

Proof. The definition of C_q^0 can be rewritten

$$C_q^0 = \left\{ c \in \mathbb{N} \cap (0,q) \,\middle|\, (c,p) = 1,\ \kappa_p(c) = \min_{n \in O_q(c) \cap (0,q)} \kappa_p(n) \right\}.$$

Therefore relation (4) implies containment $\supset$ in (6) and moreover, supposing failure of equality in (6), there exist $c, c' \in C_q^0$ such that

$$c = \mu_q(c) \neq c', \quad \kappa_p(c) = \kappa_p(c').$$

But $c' = q^i(c+1) - 1$ for some $i \in \mathbb{N}$ by (5), hence $c' \geq q$, and hence $c' \notin C_q^0$. This contradiction establishes equality in (6) and in turn containment $\subset$ in (7). Finally, (5) and (6) imply equality in (7). $\square$

The following is the promised reduction of the proof of Theorem 1.2.

Proposition 2.5. *If Theorems 2.2 and 2.3 hold, then Theorem 1.2 holds, too.*

Before turning to the proof, we pause to discuss the groups in play.

2.6. **Generators for $K[[X]]^\times$, $\mathbf{D}[K[[X]]^\times]$ and $\Gamma_{q,K}$.** Equip $K[[X]]^\times$ with the topology for which the family $\{1 + X^n K[[X]] | n \in \mathbb{N}\}$ is a neighborhood base at the origin. Then the set

$$\{1 + \alpha X^k | \alpha \in K^\times,\ k \in \mathbb{N}\} \cup K^\times$$

generates $K[[X]]^\times$ as a topological group. Let $\mathbb{F}_p$ be the residue field of $\mathbb{Z}_p$. Let $E_p = E_p(X) \in \mathbb{F}_p[[X]]$ be the reduction modulo p of the Artin-Hasse exponential

$$\exp\left(\sum_{i=0}^{\infty} \frac{X^{p^i}}{p^i}\right) \in (\mathbb{Q} \cap \mathbb{Z}_p)[[X]],$$

noting that

$$\mathbf{D}[E_p] = \sum_{i=0}^{\infty} X^{p^i}.$$

Since $E_p(X) = 1 + X + O(X^2)$, the set

$$\{E_p(\alpha X^k) \mid \alpha \in K^\times,\ k \in \mathbb{N},\ (k,p) = 1\} \cup K[[X^p]]^\times$$

generates $K[[X]]^\times$ as a topological group. For each $k \in \mathbb{N}$ such that $(k,p) = 1$ and $\alpha \in K^\times$, put

$$W_{k,\alpha} = W_{k,\alpha}(X) = k^{-1}\mathbf{D}[E_p(\alpha X^k)] = \sum_{i=0}^{\infty} \alpha^{p^i} X^{kp^i} \in XK[[X]].$$

Equip $\mathbf{D}[K[[X]]^\times]$ with the relative X-adic topology. The set

$$\{W_{k,\alpha} | k \in \mathbb{N},\ (k,p) = 1,\ \alpha \in K^\times\}$$

generates $\mathbf{D}[K[[X]]^\times]$ as a topological group, cf. exact sequence (2). Equip $\Gamma_{q,K}$ with the relative X-adic topology. Note that

$$(X+\beta X^{q^\ell})^{-1}=\sum_{i=0}^\infty (-1)^i\beta^{\frac{q^{\ell i}-1}{q^\ell-1}}X^{q^{\ell i}}\in\Gamma_{q,K}$$

for all $\ell\in\mathbb{N}$ and $\beta\in K^\times$. The inverse operation here is of course understood in the functional rather than multiplicative sense. The set

$$\{X+\beta X^{q^\ell}\mid \beta\in K^\times,\ \ell\in\mathbb{N}\}$$

generates $\Gamma_{q,K}$ as a topological group.

2.7. **Proof of the proposition.** It is enough to verify (3) with F and γ ranging over sets of generators for the topological groups $K[[X]]^\times$ and $\Gamma_{q,K}$, respectively. The generators mentioned in the preceding paragraph are the convenient ones. So fix $\alpha,\beta\in K^\times$ and $k,\ell\in\mathbb{N}$ such that $(k,p)=1$. It will be enough to verify that

$$\psi_q[M_{k,\alpha,\ell,\beta}]=\begin{cases}\alpha X^{k+1}+\sum\limits_{\ell|f\in\mathbb{N}}(-1)^{f/\ell}\alpha^{q^f}\beta^{\frac{q^f-1}{q^\ell-1}}X^{q^f(k+1)} & \text{if } k\in C_q,\\ 0 & \text{otherwise,}\end{cases}\tag{8}$$

where

$$\begin{aligned}M_{k,\alpha,\ell,\beta}&=M_{k,\alpha,\ell,\beta}(X)=k^{-1}\mathbf{D}[E_p(\alpha(X+\beta X^{q^\ell})^k)]\\ &=W_{k,\alpha}+\sum_{i=0}^\infty\sum_{j=1}^\infty\binom{p^ik-1}{j}\alpha^{p^i}\beta^jX^{p^ik+j(q^\ell-1)}.\end{aligned}\tag{9}$$

By Theorem 2.2, many terms on the right side of (9) vanish, and more precisely, we can rewrite (9) as follows:

$$M_{k,\alpha,\ell,\beta}\equiv\alpha X^k+\sum_{\substack{m\in O_q(k)\\ m>_pk}}\left(\sum_{\substack{i\in\mathbb{N}\cup\{0\},j\in\mathbb{N}\\ (j,p^ik,\operatorname{ord}_p q^\ell,m)\in\mathcal{A}_p}}\binom{p^ik-1}{j}\alpha^{p^i}\beta^j\right)X^m \mod X^pK[[X^p]].\tag{10}$$

By Theorem 2.3 as recast in the form of Proposition 2.4, along with formula (10) and the definitions, both sides of (8) vanish unless $k\in C_q$. So now fix $c\in C_q^0$ and $g\in\mathbb{N}\cup\{0\}$ and put

$$k=(c+1)q^g-1\in C_q$$

for the rest of the proof of the proposition. Also fix $f\in\mathbb{N}\cup\{0\}$ and put

$$m=q^f(k+1)-1=(c+1)q^{f+g}-1\in C_q$$

for the rest of the proof. It is enough to evaluate the coefficient of X^m in (10). By part (ii) of Theorem 2.2, there is no term in the sum on the right side of (10) of degree m unless $\ell|f$, in which case there is exactly one term, namely

$$\binom{q^fk-1}{\frac{q^f-1}{q^\ell-1}}\alpha^{q^f}\beta^{\frac{q^f-1}{q^\ell-1}}X^m,$$

and by the theorem of Lucas, the binomial coefficient mod p evaluates to $(-1)^{f/\ell}$. Therefore (8) does indeed hold. □

2.8. **Remarks.**

(i) By formula (10), the p-digital well-ordering actually gives rise to a $\Gamma_{q,K}$-stable complete separated filtration of the quotient $K[[X]]^\times/K[[X^p]]^\times$ distinct from the X-adically induced one. Theorem 1.2 merely describes the structure of $K[[X]]^\times/K[[X^p]]^\times$ near the top of the "p-digital filtration".

(ii) Computer experimentation based on formula (9) was helpful in making the discoveries detailed in this paper. We believe that continuation of such experiments could lead to further progress, e.g., to the discovery of a minimal set of generators for $K[[X]]^\times$ as a topological right $\Gamma_{q,K}$-module.

3. Proof of Theorem 2.2

Lemma 3.1. *Fix $(j,k,\ell,m)\in\mathcal{A}_p$. Put*

$$e=\mathrm{ord}_p(m+1),\quad f=\mathrm{ord}_p\,k,\quad g=\mathrm{ord}_p(k/p^f+1).$$

Then there exists a unique integer r such that

$$0\leq r\leq e+\ell-1,\ \ r\equiv 0 \bmod \ell,\ \ j\equiv\frac{p^r-1}{p^\ell-1}\bmod p^e, \tag{11}$$

and moreover

$$f+g\geq e, \tag{12}$$

$$\kappa_p(m)\geq\kappa_p(k). \tag{13}$$

This lemma is the key technical result of the paper.

3.2. **Completion of the proof of the theorem, granting the lemma.** Fix $(j,k,\ell,m)\in\mathcal{A}_p$. Let e,f,g,r be as defined in Lemma 3.1. Since the number of digits in the minimal base p expansion of k cannot exceed the number of digits in the minimal base p expansion of m, one has

$$\delta_p(k)+f+g\leq\delta_p(m)+e. \tag{14}$$

Combining (12) and (14), one has

$$\delta_p(k)=\delta_p(m)\Rightarrow f+g=e. \tag{15}$$

Now in general one has

$$m+1=(\kappa_p(m)+1)p^e,\quad k+p^f=(\kappa_p(k)+1)p^{f+g},$$

and hence

$$\kappa_p(k)=\kappa_p(m)\Rightarrow\left(j=\frac{p^f-1}{p^\ell-1}\text{ and }e>g\right) \tag{16}$$

via (15). Theorem 2.2 now follows from (13), (16) and the definition of the p-digital well-ordering. □

3.3. **Proof of Lemma 3.1.** Since e is the number of trailing $(p-1)$'s in the minimal base p expansion of m, the lemma is trivial in the case $e=0$. We therefore assume that $e>0$ for the rest of the proof.

Let

$$m=[m_1,\dots,m_t]_p \quad (t>0,\ m_1>0,\ \ m_t>0)$$

be the minimal base p expansion of m. For convenience, put

$$d=\delta_p(m)\geq 0, \quad m_\nu=0 \text{ for } \nu<1.$$

Then

$$t=e+d, \quad m_{d+1}=\dots=m_{d+e}=p-1, \quad m_d<p-1.$$

By hypothesis

$$\binom{k-1}{j}=\binom{m-jp^\ell-1+j}{m-jp^\ell-1}>0,$$

hence

$$m>jp^\ell,$$

and hence the number of digits in the minimal base p of expansion of jp^ℓ does not exceed that of m. Accordingly,

$$t>\ell$$

and one has a base p expansion for j of the form

$$j=[j_1,\dots,j_{t-\ell}]_p,$$

which perhaps is not minimal. For convenience, put

$$j_\nu=0 \text{ for } \nu<1 \text{ and also for } \nu>t-\ell.$$

This state of affairs is summarized by the "snapshot"

$$m=[m_1,\dots,m_t]=[m_1,\dots,m_d,\underbrace{p-1,\dots,p-1}_{e}]_p, \quad \kappa_p(m)=[m_1,\dots,m_d]_p,$$

$$jp^\ell=[j_1,\dots,j_t]_p=[j_1,\dots,j_{t-\ell},\underbrace{0,\dots,0}_{\ell}]_p,$$

which the reader should keep in mind as we proceed.

We are ready now to prove the existence and uniqueness of r. One has

$$m-jp^\ell-1=k-1-j=[m'_1,\dots,m'_d,p-1-j_{d+1},\dots,p-1-j_{t-1},p-2]_p,$$

where the digits $m'_1,\dots,m'_d$ are defined by the equation

$$\kappa_p(m)-[j_1,\dots,j_d]_p=[m'_1,\dots,m'_d]_p. \tag{17}$$

By hypothesis and the theorem of Lucas, the addition of $k-1-j$ and j in base p requires no "carrying", and hence

(18)

$$k-1=\left\{\begin{array}{l}[m'_1+j_{1-\ell},\dots,m'_d+j_{d-\ell},\\ p-1-j_{d+1}+j_{d+1-\ell},\dots,p-1-j_{d+e-1}+j_{d+e-1-\ell},p-2+j_{d+e-\ell}]_p.\end{array}\right.$$

From the system of inequalities for the last $e+\ell$ digits of the base p expansion of jp^ℓ implicit in (18), it follows that there exists $r_0\in\mathbb{N}\cup\{0\}$ such that

$$jp^\ell=[j_{1-\ell},\dots,j_{d-\ell},\overbrace{0,\dots,0,\underbrace{\underbrace{1,0,\dots,0}_{\ell},\dots,\underbrace{1,0,\dots,0}_{\ell}}_{r_0\text{ blocks}},0}^{e+\ell}]_p. \tag{19}$$

Therefore $r = r_0\ell$ has the required properties (11). Uniqueness of r is clear. For later use, note the relation

$$r \geq e \Leftrightarrow [j_{d-\ell+1}, \ldots, j_d]_p \neq 0 \Rightarrow [j_{d-\ell+1}, \ldots, j_d]_p = p^{r-e}, \tag{20}$$

which is easy to see from the point of view adopted here to prove (11).

By (11) one has

$$k + p^r - (m+1) + j'p^e(p^\ell - 1) = 0 \quad \text{for some } j' \in \mathbb{N} \cup \{0\}, \tag{21}$$

and hence one has

$$r \geq \min(f, e), \quad f \geq \min(r, e). \tag{22}$$

This proves (12), since either one has $f \geq e$, in which case (12) holds trivially, or else $f < e$, in which case $r = f$ by (22), and hence (12) holds by (21).

Put

$$k - 1 = [k'_1, \ldots, k'_{d+e}]_p, \quad \mathbf{1}_{r\geq e} = \begin{cases} 1 & \text{if } r \geq e, \\ 0 & \text{if } r < e. \end{cases}$$

Comparing (18) and (19), we see that the digits $k'_{d+1}, \ldots, k'_{d+e}$ are all $(p-1)$'s with at most one exception, and the exceptional digit if it exists is a $p-2$. Further, one has

$$k'_{d+1} = \cdots = k'_{d+e} = p - 1 \Leftrightarrow f \geq e \Leftrightarrow \mathbf{1}_{r\geq e} = 1$$

by (22). Therefore one has

$$\kappa_p(k) \leq [k'_1, \ldots, k'_d]_p + \mathbf{1}_{r\geq e}.$$

Finally, via (17), (18) and (20), it follows that

$$\begin{array}{rcl} \kappa_p(k) & \leq & [m'_1 + j_{1-\ell}, \ldots, m'_d + j_{d-\ell}]_p + \mathbf{1}_{r\geq e} \\ & = & \kappa_p(m) - [j_1, \ldots, j_d]_p + [j_{1-\ell}, \ldots, j_{d-\ell}]_p + \mathbf{1}_{r\geq e} \\ & = & \kappa_p(m) - [j_{1-\ell}, \ldots, j_d]_p + [j_{1-\ell}, \ldots, j_{d-\ell}]_p + \mathbf{1}_{r\geq e} \\ & = & \kappa_p(m) - [j_{d-\ell+1}, \ldots, j_d]_p + \mathbf{1}_{r\geq e} \\ & & -[j_{1-\ell}, \ldots, j_{d-\ell}, \underbrace{0, \ldots, 0}_{\ell}]_p + [j_{1-\ell}, \ldots, j_{d-\ell}]_p \\ & = & \kappa_p(m) - \mathbf{1}_{r\geq e}(p^{r-e} - 1) - (p^\ell - 1)[j_{1-\ell}, \ldots, j_{d-\ell}]_p \\ & \leq & \kappa_p(m). \end{array}$$

Thus (13) holds and the proof of the lemma is complete. □

4. Proof of Theorem 2.3

4.1. **Further digital apparatus.** Put $\lambda = \operatorname{ord}_p q$. For each $c \in \mathbb{N}$, let

$$\langle c \rangle_q = \min\{n \in \mathbb{N} | n \equiv c \bmod q - 1\}, \quad \tau_p(c) = c/p^{\operatorname{ord}_p c}.$$

Note that

$$0 < \langle c \rangle_q < q, \quad \langle c \rangle_q = \langle c' \rangle_q \Leftrightarrow c \equiv c' \bmod q - 1$$

for all $c, c' \in \mathbb{N}$. Given $c \in \mathbb{N}$, and writing $\langle c \rangle_q = [c_1, \ldots, c_\lambda]_p$, note that

$$\{c_1, \ldots, c_\lambda\} \neq \{0\}, \quad \langle pc \rangle_q = [c_2, \ldots, c_\lambda, c_1]_p,$$

$$\langle c \rangle_q \geq \tau_p(\langle c \rangle_q) = [c_1, \ldots, c_{\max\{i|c_i\neq 0\}}]_p \geq \kappa_p(\langle c \rangle_q).$$

Lemma 4.2. $\langle p^i c \rangle_q \leq p^i - 1 \Rightarrow \tau_p(\langle c \rangle_q) \leq \langle p^i c \rangle_q$ *for* $c \in \mathbb{N}$ *and* $i \in \mathbb{N} \cap (0, \lambda)$.

Lemma 4.3. $\min_{i=0}^{\lambda-1} \tau_p(\langle p^i c + 1 \rangle_q) = 1 + \min_{i=0}^{\lambda-1} \kappa_p(\langle p^i c \rangle_q) = 1 + \kappa_p(\mu_q(c))$ *for* $c \in \mathbb{N}$.

Lemma 4.4. $i \not\equiv 0 \bmod \lambda \Rightarrow p^i(\mu_q(c)+1)-1 \notin O_q(c)$ *for* $i, c \in \mathbb{N}$.

4.5. **Completion of the proof of the theorem, granting the lemmas.** Relation (4) holds by Lemma 4.3. Relation (5) holds by Lemma 4.4. □

4.6. **Proof of Lemma 4.2.** Write $\langle c\rangle_q = [c_1, \ldots, c_\lambda]_p$. By hypothesis

$$\langle p^i c\rangle_q = [\underbrace{0, \ldots, 0}_{\lambda-i}, c_1, \ldots, c_i]_q, \quad c = [c_1, \ldots, c_i, \underbrace{0, \ldots, 0}_{\lambda-i}]_p,$$

and hence $\tau_p(c) \le \langle p^i c\rangle_q$. □

4.7. **Proof of Lemma 4.3.** Since

$$\mu_q(c) = (\kappa_p(\mu_q(c))+1)p^g - 1 \in O_q(c),$$

for some $g \in \mathbb{N}\cup\{0\}$, one has

$$\kappa_p(\mu_q(c)) + 1 \ge \min_{i=0}^{\lambda-1}\min_{j=0}^{\lambda-1}\langle p^i(p^j c+1)\rangle_q.$$

One has

$$\tau_p(\langle n+1\rangle_q) \ge 1 + \kappa_p(\langle n\rangle_q)$$

for all $n \in \mathbb{N}$, as can be verified by a somewhat tedious case analysis which we omit. Clearly, the inequalities $\ge$ hold in the statement we are trying to prove. Therefore it will be enough to prove that

$$\min_{i=0}^{\lambda-1}\min_{j=0}^{\lambda-1}\langle p^i(p^j c+1)\rangle_q \ge \min_{j=0}^{\lambda-1}\tau_p(\langle p^j c+1\rangle_q).$$

Fix $i = 1, \ldots, \lambda-1$ and $j = 0, \ldots, \lambda-1$. It will be enough just to prove that

$$\langle p^i(p^j c+1)\rangle_q < \tau_p(\langle p^j c+1\rangle_q) \Rightarrow \langle p^i(p^j c+1)\rangle_q \ge \tau_p(\langle p^{i+j} c+1\rangle_q). \tag{23}$$

But by the preceding lemma, under the hypothesis of (23), one has

$$p^i - 1 < \langle p^i(p^j c+1)\rangle_q$$

and hence

$$\langle p^i(p^j c+1)\rangle_q = \langle p^{i+j}c+1\rangle_q + p^i - 1 \ge \tau_p(\langle p^{i+j}c+1\rangle_q).$$

Thus (23) is proved, and with it the lemma. □

4.8. **Proof of Lemma 4.4.** We may assume without loss of generality that $0 < i < \lambda$ and $c = \mu_q(c)$. By the preceding lemma $c < q$. Write $c = [c_1, \ldots, c_\lambda]_p$ and define c_k for all k by enforcing the rule $c_{k+\lambda} = c_k$. Supposing that the desired conclusion does not hold, one has

$$\begin{aligned}
p^{\lambda-i}[c_1, \ldots, c_\lambda, \underbrace{p-1, \ldots, p-1}_{i}]_p &\equiv [c_1, \ldots, c_\lambda, \underbrace{p-1, \ldots, p-1}_{i}, \underbrace{0, \ldots, 0}_{\lambda-i}]_p \\
&\equiv [c_1, \ldots, c_\lambda]_p + [\underbrace{p-1, \ldots, p-1}_{i}, \underbrace{0, \ldots, 0}_{\lambda-i}]_p \\
&\equiv [c_1, \ldots, c_\lambda]_p - [\underbrace{0, \ldots, 0}_{i}, \underbrace{p-1, \ldots, p-1}_{\lambda-i}]_p \\
&\equiv [c_{1+m}, \ldots, c_{\lambda+m}]_p = \langle p^m c\rangle_q
\end{aligned}$$

for some integer $m \ge 0$, where all the congruences are modulo $q-1$. It is impossible to have $c_1 = \cdots = c_i = 0$ since this would force the frequency of occurrence of the digit 0 to differ in the digit strings $c_1, \ldots, c_\lambda$ and $c_{1+m}, \ldots, c_{\lambda+m}$, which after all are just cyclic permutations one of the other. Similarly we can rule out the possibility $c_{i+1} = \cdots = c_\lambda = p-1$. Thus the base p expansion of c takes the form

$$c = [\underbrace{0,\ldots,0}_{\alpha},\underbrace{\bullet,\ldots,\bullet}_{\beta},\underbrace{p-1,\ldots,p-1}_{\gamma}]_p,$$

where

$$\alpha < i, \quad \beta > 0, \quad \gamma < \lambda - i, \quad \alpha+\beta+\gamma = \lambda,$$

and the bullets hold the place of a digit string not beginning with a 0 and not ending with a $p-1$. Then one has

$$\begin{array}{rcl} 1+\kappa_p(c) & = & (c+1)/p^\gamma \\ & > & (c+1-p^{\lambda-i})/p^\gamma + 1 \ \ \text{(strict inequality!)} \\ & \geq & \tau_p(c+1-p^{\lambda-i})+1 \\ & = & \tau_p(\langle p^m c\rangle_q)+1 \\ & \geq & \kappa_p(\langle p^m c\rangle_q)+1 \end{array}$$

in contradiction to the preceding lemma. This contradiction finishes the proof. □

References

[Goss] D. Goss, *Basic structures of function field arithmetic,* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **35**, Springer-Verlag, Berlin, 1996.

[Thak] D. Thakur, *Function Field Arithmetic,* World Scientific Pub., 2004.

University of Minnesota, Mpls., MN 55455
E-mail address: gwanders@umn.edu