FIXED POINTS OF THE \( p \)-ADIC \( q \)-BRACKET

ERIC BRUSSEL

(Communicated by Matthew A. Papanikolas)

Abstract. The \( q \)-bracket \( [X]_q : \mathbb{O}_{C_p} \to \mathbb{O}_{C_p} \), which is the \( q \)-analog of the identity function, is also a norm-preserving isometry, for each \( q \in \mathbb{B}(1, p^{-1/(p-1)}) \). In this paper we investigate its fixed points.

I. Introduction

We start with an example from complex analysis. Let \( D \) be the unit disk in the complex plane \( \mathbb{C} \). An isometry of \( D \) is a continuous, distance-preserving map from \( D \) to \( D \). All analytic isometries of \( D \) are rotations and preserve the complex norm. They are parameterized in a natural way by \( \mathbb{R}/\mathbb{Z} \), with \( t \in \mathbb{R}/\mathbb{Z} \) corresponding to the rotation \( \rho_t : z \mapsto e^{2\pi i t}z \). The quotient topology on \( \mathbb{R}/\mathbb{Z} \) makes the isometries into a continuous family, since for all \( z \in D \), \( \lim_{t \to t_0} \rho_t(z) = \rho_{t_0}(z) \). The fixed point set of this family is uninteresting, since a nontrivial rotation fixes only the origin. A more interesting set of fixed points is provided by the larger family of analytic automorphisms of \( D \). By Schwarz’s Lemma, this family is continuously parameterized by \( \mathbb{R}/\mathbb{Z} \times \mathbb{D} \), with \( (t, z_0) \) corresponding to the Möbius transformation \( z \mapsto e^{2\pi i t} \frac{z_0-z}{1-z_0^{-1}z} \). A direct computation shows that an analytic automorphism has either one interior fixed point or one boundary fixed point or two boundary fixed points.

This paper grew from an interest in the fixed points on the \( p \)-adic unit disk \( \mathbb{Z}_p \).

Let \( p \) be a prime, and let \( \mathbb{Z}_p \) denote the additive group of \( p \)-adic integers. There is a continuous family of norm-preserving isometries \( [X]_q : \mathbb{Z}_p \to \mathbb{Z}_p \) parameterized by the elements \( q \) of the topological group \( \mathbb{B}(1, p^{-1/(p-1)}) \), which is \( 1+p\mathbb{Z}_p \) if \( p \) is odd, and \( 1+4\mathbb{Z}_p \) if \( p = 2 \). The function \( [X]_q \) is called the \( q \)-bracket, and it is an interpolation to \( \mathbb{Z}_p \) of the arithmetic function on \( \mathbb{N} \cup \{0\} \) given by

\[
[X]_q = 1 + q + q^2 + \cdots + q^{n-1}.
\]

The \( q \)-bracket is also known as the \( q \)-analog (or \( q \)-extension) of the identity function, and its values are \( q \)-numbers. It is the canonical 1-cocycle \( [X]_q \in Z^1(\mathbb{Z}_p, \mathbb{Z}_p) \) sending 1 to 1, where \( \mathbb{Z}_p \) is viewed as a \( \mathbb{Z}_p \)-module via the action \( 1 \ast 1 = q \). Since \( q \) is in \( \mathbb{B}(1, p^{-1/(p-1)}) \), we have \( [X]_q \in Z^1(\mathbb{Z}_p, \mathbb{Z}_p) \) and \( [X]_q \mod p^n \in Z^1(\mathbb{Z}/p^n, \mathbb{Z}/p^n) \).

Our results show that if \( p \neq 3 \), or if \( q \equiv 1 \mod p^2 \), then \( [X]_q \) has only the “trivial” fixed points 0 and 1 in \( \mathbb{Z}_p \). However, if \( p = 3 \), \( q \equiv 1 \mod 3 \), and
coefficients. The structure of the space of continuous functions
of the form the two balls $B(1,1)$ and $B(0,1)$, and the map $Q(X)$ taking $x$ to $q$ is a
bijection.

It turns out to be easier to analyze our problem in the following more general context.

Let $\mathbb{C}_p$ denote the $p$-adic complex numbers. Write $|\cdot|$ for the metric on $\mathbb{C}_p$, and
let $\mathcal{O}_p = \mathbb{C}_p$. Write $v$ for the corresponding additive valuation, so that $|x| = p^{-v(x)}$. Let $B(a, r)$ denote the set \{ $b \in \mathbb{C}_p : |b - a| < r$ \}. If $x \in \mathcal{O}_p$ and $q \in B(1, p^{-1/(p-1)})$, then $x \log q \in x \cdot B(0, p^{-1/(p-1)}) \subset \mathcal{O}_p$, and
so $q^x = \exp(x \log q)$ is well defined. We define the $q$-bracket $[X]_q$ on $\mathcal{O}_p$ by

$$[x]_q = \begin{cases}
q^{x/q - 1} & \text{if } q \neq 1, \\
x & \text{if } q = 1.
\end{cases}$$

As above, the $q$-bracket is an interpolation to $\mathcal{O}_p$ of the $q$-number function on $\mathbb{N}$,
defined by $[n]_q = 1 + q + q^2 + \cdots + q^n$. The $q$-bracket is also the canonical
1-cocycle $[X]_q \in \mathbb{Z}[\mathcal{O}_p, \mathcal{O}_p]$ sending 1 to 1, where $\mathcal{O}_p$ is viewed as an $\mathcal{O}_p$-module
via the action $1 \ast 1 = q$.

In this setting, we will show that $x \in \mathcal{O}_p$ is a nontrivial fixed point of $[X]_q$ for
some $q$ if and only if $|A_{p-2}(x)| > p^{-1/(p-1)}$, where $A_{p-2}(X) \overset{df}{=} (X-2) \cdots (X-(p-1))$, and then $|A_{p-2}(x)| = |p(q-1)^{2-p}|$. The set of nontrivial pairs $(x,q)$
such that $[x]_q = x$ forms a manifold whose standard projections each have degree
$p-2$. If $[x]_q = x$, then we have a surjective analytic map $Q(X) : B(x, |A_{p-2}(x)|) \to
B(q, |q-1|)$ such that $[x']_{Q(x')} = x'$ for all $x' \in B(x, |A_{p-2}(x)|)$, and this map is a
(bijection) contraction if and only if the residue $\bar{x}$ has multiplicity one in the fiber
over $q$, if and only if the residue $\bar{x}$ is not a root of the polynomial $A_{p-2}^{(1)}(X)$, i.e., if and only if
$|A_{p-2}^{(1)}(x)| = 1$.

For a reference on the basic concepts, see the beautiful book [G] by Gouvêa.
The study of $q$-functions for a general variable $q$ tending to 1 is old, and the study
of $q$-numbers and $q$-identities goes back at least to Jackson in [J]. In [F] Fray
proved $p$-adic $q$-analogues of theorems of Legendre, Kummer, and Lucas on $q$-binomial
coefficients. The structure of the space of continuous functions $C(K, \mathbb{Q}_p)$, where
$K$ is a local field, was studied by Dieudonné in [D], and Mahler constructed an
explicit basis for this space in [M]. In [C] Conrad proved that the set of $q$-binomial
coefficients (which includes the $q$-identity function) forms a basis for $C(\mathbb{Z}_p, \mathbb{Q}_p)$.
Isometries on $\mathbb{Z}_p$ or on locally compact connected one-dimensional abelian groups
were studied in [A], [B], and [S].

II. Results

Notation. The letters $q$, $u$, and $x$ will always denote elements of $B(1, p^{-1/(p-1)})$, $\mathcal{O}_p^*$,
and $\mathcal{O}_p$, respectively, and the first two will frequently be related by $q = 1 + p^m u$, where
$m_0 = \nu(q-1) > 1/(p-1)$. The capitals $Q, U$, and $X$ will denote coordinate
functions defined on these sets, related to each other in a similar manner.

Proposition 1. Fix $q \in B(1, p^{-1/(p-1)})$. Then $[X]_q : \mathcal{O}_p \to \mathcal{O}_p$ is a norm-
 preserving isometry.
Proof: This is clear for \( q = 1 \), so assume \( q \neq 1 \). \([X]_q\) is the composition of analytic isomorphisms
\[
\begin{align*}
\mathcal{O}_p \xrightarrow{\log q} B(0, |q - 1|) \xrightarrow{\exp(-1)} B(0, |q - 1|) \xrightarrow{\partial} \mathcal{O}_p,
\end{align*}
\]
a dilation by \(|q - 1|\), an isometry, and a contraction by \(|q - 1|\). Tracing through the maps shows that \([X]_q\) preserves the norm. \(\square\)

Since \([X]_q\) is an isometry of the \( p \)-adic unit disk onto itself, the notion of a fixed point makes sense. Set
\[
f(X, Q) = [X]_Q - X.
\]

For fixed \( q \in B(1, p^{-1/(p-1)}) \) the set of fixed points of \([X]_q\) is the set of solutions \( \{ x : f(x, q) = 0 \} \). We see that \( f(X, Q) \) is analytic on \( \mathcal{O}_p \times B(1, p^{-1/(p-1)}) \), since
\[
f(X, Q) = \sum_{n=1}^{\infty} \left( \frac{X}{n+1} \right) (Q - 1)^n
\]
is in \( \mathbb{C}_p[[X, Q - 1]] \) and converges on \( \mathcal{O}_p \times B(0, p^{-1/(p-1)}) \).

It is obvious that \( f(x, 1) = 0 \) for all \( x \in \mathcal{O}_p \), and \( f(0, q) = f(1, q) = 0 \) for all \( q \in B(1, p^{-1/(p-1)}) \). We call these solutions trivial and define the set of nontrivial fixed points
\[
M \overset{\text{def}}{=} V \left( \frac{[X]_Q - X}{(Q - 1)X(X - 1)} \right) = \{ (x, q) : [x]_q = x \}.
\]

**Proposition 2.** The set \( M \) is a submanifold of \( \mathcal{O}_p \times B(1, p^{-1/(p-1)}) \). If \( (x, q) \in M \), then there is an analytic function \( Q(X) \) in a neighborhood \( N \) of \( x \) such that \( q = Q(x) \), and \( (x', Q(x')) \in M \) for all \( x' \in N \).

**Proof.** Define
\[
g(X, Q) \overset{\text{def}}{=} \frac{f(X, Q)}{(Q - 1)X(X - 1)}.
\]

We show that \( dg \) does not vanish on \( M \) by showing that \( \frac{\partial g}{\partial Q} (x, q) \neq 0 \) or all \( (x, q) \in M \). Then \( M \) is a submanifold of \( \mathcal{O}_p \times B(1, p^{-1/(p-1)}) \) by [Sc], Chapter III, Section 11, and there is an analytic function \( Q(x) \) such that \( (x', Q(x')) \in M \) in a neighborhood of \( (x, q) \) by the \( p \)-adic implicit function theorem. Directly from the definition of \( f \),
\[
\frac{\partial f}{\partial Q} = \frac{\partial [X]_Q}{\partial Q} = \frac{XQ^{-1} - [X]_Q}{Q - 1}.
\]

If \( (x, q) \in M \), then \( (x, q) \in V(f) \), so \([x]_q = x \). Therefore
\[
\frac{\partial f}{\partial Q}(x, q) = x[x - 1]_q.
\]

Since \( g = f/((Q - 1)X(X - 1)) \),
\[
\frac{\partial g}{\partial Q} = \frac{1}{(Q - 1)X(X - 1)} \frac{\partial f}{\partial Q} - \frac{g}{Q - 1}.
\]

By the power series expression for \( g \) we have \( g(X, 1) = 1/2 \), so in particular if \( (x, q) \in M \), then \( q \neq 1 \); hence \( g((Q - 1))(x, q) = 0 \), and hence
\[
\frac{\partial g}{\partial Q}(x, q) = \frac{1}{(q - 1)x(x - 1)} \frac{\partial f}{\partial Q}(x, q) = \frac{[x - 1]_q}{(q - 1)(x - 1)}.
\]
Using $q^X = e^{X \log q}$, we compute

$$[X]_q = \sum_{n=1}^{\infty} \frac{(\log q)^n}{(q-1)n!} X^n.$$ 

Therefore $\frac{[X-1]_q}{X-1} = \sum_{n=0}^{\infty} \frac{(\log q)^{n+1}}{(q-1)(n+1)!} (X-1)^n$. This has (nonzero) value $\log q/(q-1)$ at $X = 1$, and if $X \neq 1$, then it is nonzero since $[X-1]_q$ preserves the norm in $O_p$ by Proposition 1. We conclude that $\frac{\partial}{\partial q}(x, q) \neq 0$ for all $(x, q) \in M$. □

**Definitions.** Let $\phi_1 : M \to O_p$ and $\phi_2 : M \to B(1, p^{-1/(p-1)})$ be the projections, and let $M_q = \phi_2^{-1}(q)$ denote the fiber of $\phi_2$ over $q$. We identify $M_q$ with $\phi_1(M_q)$, which is the set of nontrivial fixed points of $[X]_q$.

**Series A.** For any $x \in O_p$ and $q \in B(1, p^{-1/(p-1)})$,

$$[X]_q - X = \sum_{n=0}^{\infty} c_n(x, q)(X-x)^n = (\llbracket x \rrbracket_q - x) + \left(\frac{q^x \log q}{q - 1} - 1\right)(X-x) + \sum_{n=2} q^x (\log q)^n (X-x)^n.$$ 

This series converges on $O_p$. Note that since $c_2$ is nonzero, any fixed point can have a maximum multiplicity of two.

**Proposition 3.** If $p = 2$, then $M = \emptyset$. If $p \neq 2$, then $\phi_2$ has degree $p - 2$, and

$$\phi_2(M) = B(1, p^{-1/(p-1)}) - B(1, p^{-1/(p-2)}).$$

**Proof.** Fix $q \in B(1, p^{-1/(p-1)})$, and let $m_0 = v(q-1)$. For $x \in O_p$, let $c_n = c_n(x, q)$ be the coefficient from Series A. By the $p$-adic Weierstrass preparation theorem [G, Theorem 6.2.6], the number of zeros of $[X]_q - X$ (in $O_p$) is $N = \sup\{n : v(c_n) = \inf_m v(c_m)\}$, counting multiplicities. Since $\{0, 1\}$ are both zeros, we know that $N \geq 2$, and since $M$ excludes these solutions, $M_q$ has cardinality $N - 2$. We compute $N$: If $n \geq 2$,

$$v(c_n) = (n-1)m_0 - \frac{n-s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the coefficients of the $p$-adic expansion of $n$. It is easy to see that $v(c_n) > v(c_p)$ whenever $n > p$, and

$$v(c_n(x, q)) = \begin{cases} (n-1)m_0 & \text{if } 2 \leq n \leq p - 1, \\ (p-1)m_0 - 1 & \text{if } n = p. \end{cases}$$

Thus if $p = 2$ or $m_0 > 1/(p-2)$, then $N = 2$; hence $M_q = \emptyset$. If $p \neq 2$ and $m_0 \leq 1/(p-2)$, then $v(c_p) \leq v(c_2)$; hence $N = p$, and hence $M_q$ has cardinality $p-2$, counting multiplicities. We conclude that $\phi_2$ has degree $p-2$ for $1/(p-1) < m_0 \leq 1/(p-2)$. □

Set $A_0(X) = 1$, and for $n > 0$, set

$$A_n(X) \overset{df}{=} (X-2)(X-3) \cdots (X-(n+1)).$$

Let $A^{(i)}_n (X)$ denote the $i$-th (formal) derivative.
Series B. Set $U = p^{-m_0}(Q - 1)$ for $m_0 > 1/(p - 1)$. For any $u \in \mathcal{O}_p$ we compute

$$g(x, Q) = \frac{[x]_Q - x}{(Q - 1)x(x - 1)} = \sum_{n=0}^{\infty} d_n(x, u)(U - u)^n,$$

where $d_n(x, u) = \sum_{k=n}^{\infty} \frac{A_n(x)}{(k+2)!} p^k m_0 u^{k-n}$. Note that $d_n(x, 0) = \frac{A_n(x)}{(n+2)!} p^{nm_0}$.

**Proposition 4.** Suppose $p \neq 2$. Then $\phi_1$ has degree $p - 2$, and

$$\phi_1(M) = \{ x \in \mathcal{O}_p : |A_{p-2}(x)| > p^{-1/(p-1)} \}.$$

If $(x, q) \in M$, then $|A_{p-2}(x)| = p^{(p-2)m_0 - 1}$, where $m_0 = v(q - 1)$.

**Proof.** We use Series B with $u = 0$. Set $d_n = d_n(x, 0)$. Then

$$v(d_n) = v(A_n(x)) + nm_0 + \frac{s_p(n + 2) - (n + 2)}{p - 1},$$

and from this we get

\begin{equation}
(\ast) \quad v(d_n(0, x)) = \begin{cases} v(A_n(x)) + nm_0 & \text{if } 0 \leq n \leq p - 3, \\ v(A_{p-2}(x)) + (p - 2)m_0 - 1 & \text{if } n = p - 2. \end{cases}
\end{equation}

If this series has a solution $U = u \in \mathcal{O}_p^*$, then $p \neq 2$ and $1/(p - 2) \geq m_0 > 1/(p - 1)$ by Proposition 3. If $n > p - 2$ and $m_0 > 1/(p - 1)$, then using the fact that $A_{p-2}(X)$ divides $A_n(X)$, we easily compute $v(d_n) - v(d_{p-2}) > 0$:

$$v(d_n) - v(d_{p-2}) = v(A_n(x)) - v(A_{p-2}(x)) + (n - (p - 2)m_0 + 1$$

$$+ \frac{s_p(n + 2) - (n + 2)}{p - 1}$$

$$> v(A_n(x)) - v(A_{p-2}(x)) + \frac{s_p(n + 2) - 1}{p - 1} \geq 0.$$

Thus the Weierstrass polynomial has nonzero degree if and only if $v(d_{p-2}) \leq v(d_0)$, i.e., $v(A_{p-2}(x)) \leq 1 - (p - 2)m_0$, in which case the degree is $p - 2$. For a given $x$ this holds for some $m_0$ in the range $1/(p - 2) \geq m_0 > 1/(p - 1)$ if and only if $v(A_{p-2}(x)) < 1/(p - 1)$. Now given $x \in \mathcal{O}_p$ such that $|A_{p-2}(x)| > p^{-1/(p-1)}$, set $m_0 = (1 - A_{p-2}(x))/(p - 2)$. Then $v(d_0) = v(d_{p-2})$, so that all $p - 2$ solutions are units $u$ such that $(x, q) \in M$, where $q = 1 + p^{m_0}u$. \hfill \Box

**Proposition 5.** For each $q \in B(1, p^{-1/(p-1)}) - B(1, p^{-1/(p-2)})$, let $m_0 = v(q - 1)$, and let $\mathcal{M}_q$ denote the set of residues of the elements $\phi_1(\phi_2^{-1}(q))$.

a) If $m_0 < 1/(p - 2)$, $\mathcal{M}_q = \{2, \ldots, p - 1\}$, and Card($\mathcal{M}_q$) = $p - 2$.

b) If $m_0 = 1/(p - 2)$, $\mathcal{M}_q \cap \{2, \ldots, p - 1\} = \emptyset$, and Card($\mathcal{M}_q$) $\geq p - 3$.

In particular, $m_0 = 1/(p - 2)$ if and only if $|A_{p-2}(x)| = 1$.

**Proof.** The Weierstrass polynomial for $[X]_q - X$ in Series A has degree $p$ by Proposition 3. Suppose $x \in \mathcal{M}_q$. Then $v(A_{p-2}(x)) = 0$ if and only if $\bar{x} \notin \{2, \ldots, p - 1\}$ if and only if $m_0 = 1/(p - 2)$ by Proposition 4. Therefore $\mathcal{M}_q \subset \{2, \ldots, p - 1\}$ if $m_0 < 1/(p - 2)$, and $\mathcal{M}_q \cap \{2, \ldots, p - 1\} = \emptyset$ if $m_0 = 1/(p - 2)$.

If $m_0 < 1/(p - 2)$, then $v(c_n(x, q)) > v(c_p(x, q))$ for $n = 2, \ldots, p - 1$ by (\ast). Since not every fixed point of $[X]_q$ has the same residue we must have $v(c_1(x, q)) = v(c_p(x, q))$ by [G] Corollary 6.4.11; hence there is at most one $x \in \mathcal{M}_q$ with any given residue and Card($\mathcal{M}_q$) = $p - 2$.\hfill \Box
If \( m_0 = 1/(p - 2) \), then \( v(c^p(x, q)) = v(c_p(x, q)) = m_0 \) by \((*)\), and the Newton polygon for Series A shows there are at most two zeros with residue \( \bar{x} \), using \((*)\) and [G Corollary 6.4.11]. Suppose \([X] \) has fixed points \( x, x' \), and \( x'' \), such that \( x \neq x'' \) and \( \bar{x} = \bar{x'} = \bar{x''} \). We compute \( c_1(x', q) - c_1(x, q) = ([x]'_q - [x]_q) \log q \). Since \( x' - x \) has nonzero residue it is a unit; hence \( [x]'_q - [x]_q \) is a unit by Proposition 1, so \( v(c_1(x', q) - c_1(x, q)) = m_0 \). Since \( x \neq x'' \) and \( \bar{x} = \bar{x''} \), we have \( v(c_1(x, q)) > m_0 \) by the Newton polygon, and it follows that \( v(c_1(x', q)) = m_0 \), so that \( x' \) is the only fixed point with residue \( \bar{x} \). Thus there are at most two points in \( M_\bar{q} \) with the same residue; hence \( \text{Card}(M_\bar{q}) \geq p - 3 \). The last statement is immediate.

**Remark.** If 0 or 1 is in \( M_\bar{q} \), then \( |M_\bar{q}| = p - 2 \), since these are also trivial fixed points. By Proposition 4 and Proposition 5, we compute

\[
\phi_1(M) = \bigcup_{a \in \mathbb{O}_p} B(a, 1) \cup \bigcup_{a \in \{2, \ldots, p-1\}} B(a, 1) - B(a, p^{-1/(p-1)}),
\]

where the left union corresponds to \( v(q-1) = 1/(p-2) \), the right union to \( v(q-1) < 1/(p-2) \). Note that a rational integer may be a fixed point of some \([x]_q \) only if it is congruent to 0 or 1 (mod \( p \)).

**Theorem 6.** Suppose \( x \in \mathbb{O}_p \) is a nontrivial fixed point of \([X]_q \), for some \( q \in B(1,p^{-1/(p-1)}) \). Then \( \text{Card}(\phi^{-1}_q(x)) = p - 2 \), and each \((x, q) \in \phi^{-1}_q(x) \) determines a distinct residue \( \bar{u} \), for \( q = 1 + p^{-v(q-1)}u \). If \((x, q) \in M \) and \( x' \in B(x, |A_{p-2}(x)|) \), then there exists a unique \( q' \in B(q, |q-1|) \) such that \((x', q') \in M \), and the resulting map

\[
Q(X) : B(x, |A_{p-2}(x)|) \to B(q, |q-1|)
\]

defined by \( Q(x') = q' \) is an analytic surjection satisfying \( |q' - q| = |((x')_q - x')/(x'(x'-1))| \). The map is a (bijective) contraction (by \( p^{1/(p-1)v(q-1)} \)) if and only if \( |A_{p-2}(x)| = 1 \), if and only if the multiplicity of \( \bar{x} \) in \( M_\bar{q} \) is one. This occurs for all but finitely many residue classes for \( x \).

**Proof.** Let \( m_0 = v(q-1) \). Since \( x \) is a nontrivial fixed point, \( \phi_1 \) has degree \( p - 2 \) by Proposition 4. We show that the cardinality of \( \phi^{-1}_1(x) \) is \( p - 2 \) by showing that the various \( u \) appearing in \( q = 1 + p^{m_0}u \in \phi^{-1}_1(x) \) have distinct residues. Suppose that \((x, q) \in \phi^{-1}_1(x) \), \( q = 1 + p^{m_0}u \), and \( d_n(x, u) \) is the coefficient of Series B for \( g(x, 1 + p^{m_0}U) \), expanded around \( u \). Then \( d_0(x, u) = 0 \), and using \((***)\), the identity \( d_n(x, u) = \sum_{i=0}^{n} \binom{n+1}{n} d_{n+i}(x, 0) u^i \), and the fact that \( v(d_{p-2}(x, 0)) = 0 \) (by Proposition 4), we compute \( v(d_n(x, u)) = 0 \) for \( 1 \leq n \leq p - 2 \). Thus the Newton polygon contains the points \((n, v(d_n(x, u))) = (0, \infty), (1, 0), \ldots, (p-2, 0) \), so that no other solution \( U = u' \) has the same residue as \( u \) by [G Corollary 6.4.11]. We conclude that \( \text{Card}(\phi^{-1}_1(x)) = p - 2 \) and the \( p - 2 \) roots \( u \) have distinct residues.

Next, for \( x' \in B(x, |A_{p-2}(x)|) \), we compute \( |g(x', q)| \) in terms of \(|x' - x|\). We will show that \( |g(x', q)| = p^{1/(p-2)m_0} |x' - x| \) except when \( m_0 = 1/(p-2) \) and \( |A_{p-2}(x)| = 1 \), in which case \( |g(x', q)| = |x' - x| \), and that \( |A_{p-2}(x)| = 1 \) for finitely many residue classes \( \bar{x} \).

Since \( g(x, q) = 0 \), by Series B we have

\[
g(x', q) = (x' - x) \sum_{k=1} a_k = (x' - x) \sum_{k=1} \frac{D_k(x')}{(k+2)!} b^k m_0 b^k,
\]
Thus for all but finitely many residue classes $\bar{A}$, we conclude that
\[|A_p| p^{k+2} \bar{\delta} + \frac{s_p(k+2)-2}{p-1},\]

where $\delta = m_0 - 1/(p-1) > 0$. If $k \neq p^r - 2$, then $s_p(k+2) - 2 \geq 0$, so $v(a_k) > 0$
in this case. If $k = p^r - 2$, $v(a_k) = v(D_{p^r-2}(x')) + (p^r-2)\bar{\delta} - 1/(p-1)$.

If $m_0 < 1/(p-2)$, then $|A_{p-2}(x)| < 1$ by Proposition 5, and $|A_{p-2}^{(1)}(x)| = 1$ since
$A_{p-2}(X)$ is separable (mod $p$). But $|A_{p-2}^{(1)}(x)| < 1$ for $r > 1$, since $x$ is a multiple
root of $A_{p-2}(X)$ (mod $p$) for $r > 1$. Since
\[D_k(x') = A_k^{(1)}(x) + \frac{1}{2!}A_k^{(2)}(x)(x' - x) + \cdots + \frac{1}{k!}A_k^{(k)}(x)(x' - x)^{k-1},\]
we conclude that $v(D_{p^r-2}(x')) > v(D_{p^r-2}(x')) = 0 > v(A_{p-2}(x)) - v(x' - x)$
for $r > 1$ and $x' \in B(x, |A_{p-2}(x)|)$. Since $(p^r - 2)\bar{\delta} - (p-2)\bar{\delta} = (p^r - p)\bar{\delta} > 0$
for $r > 1$, $v(a_{p-2}) > v(a_{p-2})$ for $m_0 < 1/(p-2)$, and so $v(a_{p-2}) = (p^r - 2)m_0 - 1$
is the unique minimum value of all of the coefficients. We conclude that $|g(x', q)| = p^{1-(p-2)m_0}|x' - x| = |A_{p-2}(x)|^{-1}|x' - x|$, and since $x' \in B(x, |A_{p-2}(x)|)$, this shows
that $1 > |g(x', q)| > |x' - x|$ when $m_0 < 1/(p-2)$.

If $m_0 = 1/(p-2)$, then $|A_{p-2}(x)| = 1$ by Proposition 5. We compute
\[A_{p-2}^{(1)}(x) = (p-2)X^{p-3} + (p-3)X^{p-4} + \cdots + 2X + 1 (\text{mod } p).\]

Thus for all but finitely many residue classes $\bar{x}$, we have $A_{p-2}^{(1)}(x) \neq 0$ (mod $p$); hence
$D_{p^2}^{(1)}(x') = A_{p-2}^{(1)}(x) \neq 0$ (mod $p$) whenever $x' \in B(x, 1)$, and hence $v(a_{p-2}) = 0$.
We also compute $v(a_k) \geq m_0$ for $k \neq p^r - 2$ for some $r$, and since $v(a_{p^r-2}) \geq (p^r - p)/(p-2) > 0$
for $r > 1$, this shows that $|g(x', q)| = |x' - x|$ when $(m_0 = 1/(p-2)$ and $|A_{p-2}^{(1)}(x)| = 1$.

If $m_0 = 1/(p-2)$ and $|A_{p-2}^{(1)}(x)| < 1$, then $|D_{p^2}^{(1)}(x')| < 1$, so $v(a_{p-2}) > (p-2)m_0 - 1 = 0$. Checking by hand, we find that $A_{p-2}^{(1)}(0) = A_{p-2}^{(1)}(1) = 1$ (mod $p$), so $\bar{x} \neq 0, 1$, and $A_{p-2}^{(1)}(1/2) = 0$ (mod $p$), so $\bar{x} \neq 1/2$. Since $A_{p^r-2}(X) = A_{p^r-2}(X)(X(X-1))^{r-1}$ (mod $p$), the product rule shows that when $r > 1$, $A_{p^r-2}^{(1)}(x) \neq 0$ (mod $p$), since $\bar{x} \neq 0, 1, 1/2$. Therefore $|D_{p^r-2}^{(1)}(x')| = 1$, and hence $v(a_{p^r-2}) = (p^r - p)/(p-2)(p-1) > 0$ for $r > 1$. We conclude at any rate that $|g(x', q)| < |x' - x|$ when $(m_0 = 1/(p-2))$ and $|A_{p-2}^{(1)}(x)| < 1$.

We have shown that $|A_{p-2}^{(1)}(x)| = 1$ implies $|g(x', q)| = p^{1-(p-2)m_0}|x' - x|$, hence
that $g(x', q) \neq 0$ if $\bar{x} = \bar{x}$; i.e., the multiplicity of $\bar{x}$ in $\mathcal{M}_q$ is one. Conversely,
suppose that $x \in M_q$ and $\bar{x}$ has multiplicity one in $\mathcal{M}_q$. We have already seen that
$|A_{p^2-2}^{(1)}(x)| = 1$ if $\bar{x} \in \{0, 1\}$, and otherwise $v(c_i(x, q)) = v(c_p(x, q)) = (p-1)m_0 - 1$
are the minimum values in Series A for $f(X, q)$, and $v(f(x', q)) = v(c_i(x, q)(x' - x)) = v(x' - x) + (p-1)m_0 - 1$. Therefore $|g(x', q)| = p^{1-(p-2)m_0}|x' - x| \geq |x' - x|$, for all $x' \in B(x, 1)$, and it follows from the above that $|A_{p^2-2}^{(1)}(x)| = 1$.

Next we construct the map $Q(X) : B(x, |A_{p-2}(x)|) \to B(q, |q - 1|)$ by looking at the polygon for
$g(x', 1 + p^mU)$ expanded in Series B around $u$, for $x' \in B(x, |A_{p-2}(x)|)$. We have already shown that $v(d_0(x', u)) \equiv v(g(x', q)) > 0$, and we
now claim that \( v(d_1(x', u)) = v(d_{p-2}(x', 0)) = 0 \). Consider the series
\[
d_1(x', u) = \sum_{k=1}^{\infty} k d_k(x', 0) u^{k-1} = \sum_{k=1}^{\infty} k A_k(x') \frac{u^k}{(k+2)!}.
\]
We have seen that \( v(d_k(x', 0)) > v(d_{p-2}(x', 0)) \) unless \( k = p^r - 2 \) for some \( r \), and we compute as before, \( v(d_{p^r-2}(x', 0)) = v(A_{p^r-2}(x)) + (p^r - 2) \delta - 1/(p-1) \), where \( \delta = m_0 - 1/(p-1) \). Since \( A_{p^r-2}(x) \) divides \( A_{p^r-2}(x) \), we have \( v(A_{p^r-2}(x)) > v(A_{p^r-2}(x)) \), and now it is easy to see that \( v(d_{p^r-2}(x', 0)) \) is strictly minimized at \( r = 1 \); hence \( v(d_1(x', u) = v(d_{p-2}(x', 0)) \). Since \( v(D_{p^r-2}(x')) \geq 0 \), we have \( v(A_{p^r-2}(x') - A_{p^r-2}(x)) \geq v(x' - x) > v(A_{p^r-2}(x)) \); hence \( v(A_{p^r-2}(x')) = v(A_{p^r-2}(x)) = 1 - (p - 2) m_0 \), and we compute \( v(d_{p^r-2}(x', 0)) = 0 \). Therefore \( v(d_1(x', u)) = 0 \).

Since \( v(d_0(x', u)) > v(d_1(x', u)) = 0 \), the Newton polygon for \( g(x', 1 + p^m u) \) expanded around \( u \) shows that for each \( x' \in B(x, |A_{p-2}(x)|) \) there is a root \( U = u' \in B(u, 1) \), so that \( u'' = u \), and \( v(u' - u) = v(d_0(x', u)) = v(g(x', q)) \). Setting \( q' = 1 + p^m u' \), we compute
\[
|q' - q| = p^{-m}|g(x', q)| = |(x)| - x')/(x'(x' - 1))|.
\]
If \( |A_p(x)| = 1 \), then \( |q' - q| = p^{1-(p-1)m} |x' - x| \), so \( Q(X) \) is a contraction. If \( |A_p(x)| < 1 \), then \( |q' - q| < p^{1-(p-1)m} |x' - x| \) and \( Q(X) \) is not a contraction.

For then the explicit formula for \( D_{p-2}(x) \) shows that \( D_{p-2}(x') \) is in the limit as \( x' - x \) approaches \( 1 = |A_{p-2}(x)| \); hence \( |q' - q| \) approaches \( p^{1-(p-1)m} |x' - x| \) arbitrarily closely for \( x' \in B(x, 1) \).

This \( u' \) is unique since the \( p - 2 \) solutions for \( U \) in \( g(x', 1 + p^m u) \) have distinct residues by the preceding argument. Thus we have a well-defined map
\[
Q(X) : B(x, |A_{p-2}(x)|) \to B(q, |q - 1|)
\]
sending \( x' \) to \( q' = Q(x') = 1 + p^m u' \). This map is analytic by Proposition 2.

Next we show that \( Q(X) \) is surjective. Suppose \( (x, q) \in M \) and \( q' = B(q, |q - 1|) \). Since \( |q' - q| < |q - 1| \), \( |q' - 1| = |q - 1| = p^{-m_0} \). Define \( u \) and \( u' \) by \( q = 1 + p^m u \) and \( q' = 1 + p^m u' \), and let \( \epsilon = u' - u \) so that \( v(\epsilon) > 0 \). Since \( g(x, q) = 0 \), in Series B we have
\[
g(x, q') = g(x, q') - g(x, q) = \sum_{n=1}^{\infty} d_n(x, 0)((u + \epsilon)^n - u^n).
\]
By the binomial theorem, \( \epsilon \) is a factor of each \( (u + \epsilon)^n - u^n \), and so \( v(g(x, q')) \geq v(\epsilon) > 0 \).

We show that there exists an \( x' \in B(x, |A_{p-2}(x)|) \cap M_{q'}. \) First assume \( \bar{x} \neq 0, 1 \), so that \( v(f(x, q')) = v(g(x, q')) + m_0 \). Let \( c_n(x, q') \) be the coefficient of Series A for \( f(x, q') \) expanded around \( x \). Since \( v(g(x, q')) > 0 \), we have \( c_0(x, q') = v(g(x, q')) + m_0 > m_0 \geq (p - 1)m_0 - 1 = v(c_p(x, q')) \); hence \( c_0(x, q') > v(c_p(x, q')) \). Therefore \( f(X, q') \) has a solution \( X = x' \) such that \( |x' - x| < 1 \), and \( x' \in B(x, 1) \cap M_{q'} \). If \( m_0 = 1/(p - 2) \), then \( |A_{p-2}(x)| = 1 \), and we are done. If \( m_0 < 1/(p - 2) \), then the residue multiplicity of \( x' \) is in \( M_{q'} \) is one by Proposition 5, so that \( v(c_1(x, q')) = v(c_p(x, q')) = (p - 1)m_0 - 1 \), and by the above computation we have \( v(c_0(x, q')) > m_0 \). Since \( v(A_{p-2}(x)) = 1 - (p - 2)m_0 \) by Proposition 4, we conclude that \( v(x' - x) = v(c_0(x, q')) - v(c_1(x, q')) > v(A_{p-2}(x)) \), as desired.
Next, suppose that \( \bar{x} = 0 \). Then \( m_0 = 1/(p-2) \) by Proposition 5 and \(|A_{p-2}(x)| = 1\). Since \( 0 \in B(x,1) \) and \( Q(X) : B(x,1) \to B(q,|q-1|) \), we may assume that \( x = 0 \in M_q \). Series \( A \) for \( f(X,q') \) expanded around 0 has the trivial fixed point 0, so \( c_0(0,q') = 0 \). We will show that \( v(c_1(0,q')) > v(c_2(0,q')) \). Since \( m_0 = 1/(p-2) \), we compute \( v(c_2(0,q')) = m_0 = v(c_0(0,q')) \) by (\(*)\), so we have to show \( v(c_1(0,q')) > m_0 \). The series for \( c_1(0,q') = \log q'/(q'-1) - 1 \) is

\[
-1 + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}(q' - 1)^{n-1} = \sum_{n=0}^{\infty} \frac{(-1)^{n+1}}{n+2}(q' - 1)^{n+1} = -(q' - 1)/2 + (q' - 1)^2/3 - \cdots + (q' - 1)^{p-1}/p - \cdots .
\]

We see at once that only the \( n = 0 \) and \( n = p-2 \) terms in the right parentheses have value \( m_0 = v(q' - 1) \). Since \( c_1(0,q) = 0 \), it suffices to show that \( v(q' - q) > m_0 \) and \( v(q' - 1)^{p-1} - (q - 1)^{p-1} > v(p) + m_0 \). Writing \( q' - 1 = q - 1 + p^mq \) with \( v(q) > 0 \), as before, we immediately verify that \( v(q' - q) > m_0 \), and applying the binomial theorem, we see that \( v(q - 1 + p^mq)(p-1) - (q - 1)^{p-1} > 1 + m_0 \). We conclude that \( v(c_1(0,q')) > v(c_2(0,q')) \), and the Newton polygon shows that there exists an \( x' \in B(0,1) \cap M_q \), as desired.

Next, suppose \( \bar{x} = 1 \). Then again \( m_0 = 1/(p-2) \) by Proposition 5 and \(|A_{p-2}(x)| = 1\). Again we may assume \( x = 1 \), since \( 1 \in B(x,1) \), and the proof that \( B(x,1) \cap M_q \) is nonempty is exactly like the \( \bar{x} = 0 \) case. We reduce immediately to showing \( v(c_1(1,q')) > v(c_2(1,q')) \) = \( m_0 \). The series for \( c_1(1,q') = q' \log q'/(q'-1) - 1 \) is

\[
-1 + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}q'(q' - 1)^{n-1} = -1 + q' + \sum_{n=1}^{\infty} \frac{(-1)^n}{n+1}q'^n = -(q' - 1)^2/2 + (q' - 1)^3/3 - \cdots + \frac{q'}{p}(q' - 1)^{p-1} - \cdots .
\]

Again \( v(c_1(1,q')) > m_0 \) is equivalent to \( v(c_1(1,q') - c_1(1,q)) > m_0 \), which is equivalent to \( v(-(q'/2 - 1)(q' - 1) + (q'/2 - 1)(q - 1) + q'/p(q' - 1)^{p-1} - q/p(q - 1)^{p-1}) > m_0 \), and the verification is routine. It follows that \( x' \in B(1,1) \cap M_q \) exists, as desired.

We have shown that for each \( (x,q) \in M \) and \( q' \in B(q,|q-1|) \), there exists an \( x' \in B(x,|A_{p-2}(x)|) \cap M_q \). Thus the map \( Q(X) : B(x,|A_{p-2}(x)|) \to B(q,|q-1|) \) is onto. This completes the proof. \( \square \)

Remark. If the multiplicity of the residue \( \bar{x} \) in \( M_q \) is not equal to one, then by Proposition 5 and Theorem 6, its multiplicity is two, \( \text{Card}(M_q) = p-3 \), \(|A_{p-2}(x)| = 1\), and \(|A_{p-2}^{(1)}(x)| < 1\). It follows that \(|A_{p-2}(x')| = 1\) and \(|A_{p-2}^{(1)}(x')| < 1\) for each \( x' \in B(x,1) \), and each residue \( \bar{x'} \) has multiplicity two in \( M_{Q(x')} \). We leave aside the problem of proving the existence of such points, and more especially of proving the existence of nontrivial fixed points \( x \) of multiplicity two in \( M_q \). Of course, if \( p = 3 \), there is no issue.

We next restrict Theorem 6 to the ordinary \( p \)-adic integers, which served as the initial motivation for this investigation.
Corollary 7. Let $M(\mathbb{Z}_p) = \{(x, q) \in M : x, q \in \mathbb{Z}_p\}$. Then

$$M(\mathbb{Z}_p) \neq \emptyset \iff p = 3.$$ 

The elements $x \in \mathbb{Z}_3$ that are nontrivial fixed points for some $[X]_q$ form the union

$$\phi_1(M(\mathbb{Z}_3)) = B(1, 1) \cup B(0, 1),$$

and we have an analytic bijection

$$Q(X) : B(1, 1) \rightarrow B(4, 3^{-1})$$

$$B(0, 1) \rightarrow B(7, 3^{-1})$$

with $|Q(x') - q| = |x' - x|/3$.

Proof. By Proposition 3, $M \neq \emptyset$ if and only if $1/(p-1) < v(q-1) \leq 1/(p-2)$, so we have the first statement. Assume $p = 3$. By Proposition 4, $\phi_1(M) \cap \mathbb{Z}_3 = \{x \in \mathbb{Z}_3 : x \neq 2 \pmod{3}\}$, and by Proposition 3, $\phi_2(M) \cap \mathbb{Z}_3 = \{q-1 : |q-1| = 3^{-1}\}$. Since the Weierstrass polynomial for Series B has degree one, we see that $x \in \mathbb{Z}_3$ if and only if $Q(x) = q \in \mathbb{Z}_3$, so these sets are $\phi_1(M(\mathbb{Z}_3))$ and $\phi_2(M(\mathbb{Z}_3))$, respectively. Locally the map $Q(X)$ takes $B(x, 1)$ onto $B(q, 3^{-1})$ and is a contraction by $1/3$, by Theorem 6. By sheer luck we find the nontrivial fixed point $x = -1/2$ for $q = 4$, and since $-1/2$ has residue 1, we conclude that $Q(X)$ takes $B(1, 1)$ onto $B(4, 3^{-1})$ and $B(0, 1)$ onto $B(7, 3^{-1})$. \hfill \Box

Remark. Using the 3-adic Weierstrass preparation theorem together with Series A one can approximate the nontrivial fixed point of $[X]_q$ for any $q \in B(4, 3^{-1})$ (or $q \in B(7, 3^{-1})$) to arbitrary accuracy, and conversely using Series B one can approximate the value $q$ for which any $x \in B(1, 1)$ (or $x \in B(0, 1)$) is a fixed point for $[X]_q$. For example, we find that $x = 0$ is a nontrivial fixed point for $[X]_q$, where

$$q \approx 1 + 2 \cdot 3 + 3^2 + 2 \cdot 3^3 + 3^6 + 2 \cdot 3^7.$$

The fixed points of the maps $[X]_q \pmod{3^n} : \mathbb{Z}/3^n \rightarrow \mathbb{Z}/3^n$ for $q$ such that $|q-1| = 3^{-1}$ exhibit a remarkable, seemingly erratic pattern that is nevertheless completely governed by the unique nontrivial fixed point $x \in \mathbb{Z}_3$. For example, it can be shown that if $n > 2v(x(x - 1)) + 1$, then there are $2 \cdot 3^{v(x(x - 1))+1} + 3$ fixed points, and otherwise there are $3^n - [n/2] + 3$.

As was pointed out earlier, the nontrivial 3-adic fixed point for $[X]_4$ is $-1/2 = 1 + 3 + 3^2 + 3^3 + 3^4 + \cdots$. In the following table we list the values of $[X]_4 \pmod{3^4}$ on $\mathbb{Z}/3^4\mathbb{Z}$ from 0 to $3^3$, which is where the fixed point pattern repeats. We box the fixed points:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>5</th>
<th>5</th>
<th>4</th>
<th>17</th>
<th>69</th>
<th>34</th>
<th>56</th>
<th>63</th>
<th>10</th>
<th>41</th>
<th>3</th>
<th>13</th>
<th>53</th>
<th>51</th>
<th>43</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>19</td>
<td>77</td>
<td>66</td>
<td>22</td>
<td>8</td>
<td>33</td>
<td>52</td>
<td>47</td>
<td>27</td>
<td>28</td>
<td>32</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By contrast, here is the table for $[X]_4 \pmod{3^5}$ on $\mathbb{Z}/3^5\mathbb{Z}$, listed up to $3^4$:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>5</th>
<th>21</th>
<th>85</th>
<th>98</th>
<th>150</th>
<th>115</th>
<th>218</th>
<th>144</th>
<th>91</th>
<th>122</th>
<th>3</th>
<th>13</th>
<th>53</th>
<th>213</th>
<th>124</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>181</td>
<td>239</td>
<td>228</td>
<td>184</td>
<td>8</td>
<td>33</td>
<td>133</td>
<td>47</td>
<td>189</td>
<td>28</td>
<td>113</td>
<td>210</td>
<td>112</td>
<td>206</td>
<td>96</td>
<td>142</td>
<td>83</td>
</tr>
<tr>
<td>90</td>
<td>118</td>
<td>230</td>
<td>192</td>
<td>40</td>
<td>161</td>
<td>159</td>
<td>151</td>
<td>119</td>
<td>234</td>
<td>208</td>
<td>104</td>
<td>174</td>
<td>211</td>
<td>116</td>
<td>222</td>
<td>160</td>
<td>155</td>
</tr>
<tr>
<td>135</td>
<td>55</td>
<td>221</td>
<td>156</td>
<td>189</td>
<td>71</td>
<td>42</td>
<td>169</td>
<td>191</td>
<td>36</td>
<td>145</td>
<td>95</td>
<td>138</td>
<td>67</td>
<td>26</td>
<td>105</td>
<td>178</td>
<td>227</td>
</tr>
</tbody>
</table>

| 180 | 235 | 212 | 120 | 238 | 224 | 168 | 187 | 20 | 81 | 82 | ... |
ACKNOWLEDGEMENT

We would like to thank the referee of a previous version of this paper for suggestions that dramatically simplified the proofs and improved the results.

REFERENCES


Department of Mathematics, Emory University, Atlanta, Georgia 30322