

=

## Fixed Points of the p-Adic q-Bracket

Eric Brussel

Emory University

**Abstract.** The  $q$ -bracket  $[X]_q : \mathcal{O}_{\mathbb{C}_p} \rightarrow \mathcal{O}_{\mathbb{C}_p}$ , which is the  $q$ -analog of the identity function, is also a norm-preserving isometry, for each  $q \in B(1, p^{-1/(p-1)})$ . In this paper we investigate its fixed points. We show  $x \in \mathcal{O}_{\mathbb{C}_p}$  is a “nontrivial” fixed point of  $[X]_q$  for some  $q$  if and only if  $|A_{p-2}(x)| > p^{-1/(p-1)}$ , where  $A_{p-2}(X) \stackrel{\text{df}}{=} (X-2) \cdots (X-(p-1))$ . We then define a surjective analytic map  $Q(X) : B(x, |A_{p-2}(x)|) \rightarrow B(q, |q-1|)$  such that  $[x']_{Q(x)} = x'$  for all  $x' \in B(x, |A_{p-2}(x)|)$ , which is a contraction if and only if the residue  $\bar{x}$  is not a “double point”, if and only if  $A_{p-2}^{(1)}(\bar{x}) \neq 0$ . The nontrivial pairs  $(x, q-1)$  such that  $[x]_q = x$  form a manifold whose standard projections each have degree  $p-2$ . Restricting to  $\mathbb{Z}_p$ , we find the theory to be trivial unless  $p=3$ , in which case  $Q(X) : B(0, 1) \cup B(1, 1) \rightarrow B(7, 1/3) \cup B(4, 1/3)$  is an analytic bijection, which is a contraction by  $1/3$ .

## 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  $\rho_t : z \mapsto ze^{2\pi it}$ . The quotient topology on  $\mathbb{R}/\mathbb{Z}$  makes the isometries into a *continuous family*, since for all  $z \in D$ ,  $\lim_{t \rightarrow t_0} \rho_t(z) = \rho_{t_0}(z)$ . 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  $\mathbb{R}/\mathbb{Z} \times D$ , with  $(t, z_0)$  corresponding to the mobius transformation  $z \mapsto e^{2\pi it} \frac{z_0 - z}{1 - \bar{z}_0 z}$ . 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

$$[X]_q : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$

parameterized by the elements  $q$  of the topological group  $B(1, p^{-1/(p-1)})$ , which is  $1 + p\mathbb{Z}_p$  if  $p$  is odd, and  $1 + 4\mathbb{Z}_2$  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

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

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  $1 * 1 = q$ . Since  $q$  is in  $B(1, p^{-1/(p-1)})$ , we have  $[X]_q \in Z^1(\mathbb{Z}_p, \mathbb{Z}_p)$  and  $[X]_q(\text{mod } p^n) \in Z^1(\mathbb{Z}/p^n, \mathbb{Z}/p^n)$ .

Our results show that if  $p \neq 3$ , or if  $q \equiv 1(\text{mod } p^2)$ , then  $[X]_q$  has only the “trivial” fixed points 0 and 1 in  $\mathbb{Z}_p$ . However, if  $p = 3$ ,  $q \equiv 1(\text{mod } 3)$ , and  $q \not\equiv 1(\text{mod } 9)$ , then  $[X]_q$  has a unique nontrivial fixed point in  $\mathbb{Z}_3$  for all  $q$ . For example, if  $p = 3$  and  $q = 4$ , then  $-1/2$  is the nontrivial fixed point of  $[X]_q$  when  $q = 4$ :  $[-1/2]_4 = -1/2$ . The admissible  $q$  in  $B(1, 3^{-1/2})$  form two (disjoint) balls,  $B(4, 3^{-1})$  and  $B(7, 3^{-1})$ , the set of nontrivial fixed points  $x$  for these  $q$  respectively form the two balls  $B(1, 1)$  and  $B(0, 1)$ , and the map  $Q(X)$  taking  $x$  to  $q$  is a bijective analytic contraction by the factor 3.

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  $O_p = O_{\mathbb{C}_p}$  denote the unit disk in  $\mathbb{C}_p$ . 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  $x \in O_p$  and  $q \in B(1, p^{-1/(p-1)})$  then  $x \cdot \log q \in x \cdot B(0, p^{-1/(p-1)}) \subset B(0, p^{-1/(p-1)})$ , so  $q^x = \exp(x \log q)$  is well defined. We define the  $q$ -bracket  $[X]_q$  on  $O_p$  by

$$[x]_q \stackrel{\text{df}}{=} \begin{cases} \frac{q^x - 1}{q - 1} & \text{if } q \neq 1 \\ x & \text{if } q = 1 \end{cases}$$

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

In this setting, we will show that  $x \in O_{\mathbb{C}_p}$  is a nontrivial fixed point of  $[X]_q$  for some  $q$  if and only if  $|A_{p-2}(x)| > p^{-1/(p-1)}$ , where  $A_{p-2}(X) \stackrel{\text{df}}{=} (X - 2) \cdots (X - (p - 1))$ , and then  $|A_{p-2}(x)| = |p(q - 1)^{2-p}|$ . The set of nontrivial pairs  $(x, q - 1)$  such that  $[x]_q = x$  form a manifold whose standard projections each have degree  $p - 2$ . If  $[x]_q = x$ , then we have a surjective analytic map  $Q(X) : B(x, |A_{p-2}(x)|) \rightarrow B(q, |q - 1|)$  such that  $[x']_{Q(x')} = x'$  for all  $x' \in B(x, |A_{p-2}(x)|)$ , and this map is a (bijective) contraction if and only if the residue  $\bar{x}$  has multiplicity one in the fiber over  $q - 1$ , if and only if  $\bar{x}$  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 reference on 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  $q$ -analogs 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), form a basis for  $C(\mathbb{Z}_p, \mathbb{Z}_p)$ . Isometries on  $\mathbb{Z}_p$  or on locally compact connected one-dimensional abelian groups were studied in [A], [B], and [Su].

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.

## II. Results.

**Notation.** The letters  $q, u$ , and  $x$  will always denote elements of  $B(1, p^{-1/(p-1)})$ ,  $O_p^*$ , and  $O_p$ , respectively, and the first two will frequently be related by  $q = 1 + p^{m_0}u$ , for some number  $m_0 > 1/(p-1)$ . The capitals  $X, Q$ , and  $U$  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  $[X]_q : O_p \rightarrow O_p$  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

$$O_p \xrightarrow{\log q} B(0, |q-1|) \xrightarrow{\exp(-)-1} B(0, |q-1|) \xrightarrow{\frac{1}{q-1}} O_p$$

a dilation by  $|q-1|$ , an isometry, and a contraction by  $|q-1|$ . Tracing through the maps shows  $[X]_q$  preserves the norm. ■

Since  $[X]_q$  is an isometry of the  $p$ -adic unit disk onto itself, the notion of fixed point makes sense. Set

$$f(X, Q-1) = [X]_Q - X$$

For fixed  $q \in B(1, p^{-1/(p-1)})$  the set of fixed points of  $[X]_q$  is the set of solutions  $\{x : f(x, q-1) = 0\}$ . We see that  $f(X, Q-1)$  is analytic on  $O_p \times B(0, p^{-1/(p-1)})$ , since

$$f(X, Q-1) = \sum_{n=1}^{\infty} \binom{X}{n+1} (Q-1)^n$$

is in  $\mathbb{C}_p[[X, Q-1]]$  and converges on  $O_p \times B(0, p^{-1/(p-1)})$ .

It is obvious that  $f(x, 0) = 0$  for all  $x \in O_p$ , and  $f(0, q-1) = f(1, q-1) = 0$  for all  $q-1 \in B(0, p^{-1/(p-1)})$ . We call these solutions *trivial*, and define the set of *nontrivial fixed points*

$$M \stackrel{\text{df}}{=} V \left( \frac{[X]_Q - X}{(Q-1)X(X-1)} \right) = \{(x, q-1) : [x]_q = x\}$$

**Proposition 2.** *The set  $M$  is a submanifold of  $O_p \times B(0, p^{-1/(p-1)})$ . If  $(x, q-1) \in M$  then there is an analytic function  $Q(x)$  in a neighborhood  $N$  of  $x$  such that  $q = Q(x)$ , and  $(x', Q(x')-1) \in M$  for all  $x' \in N$ .*

*Proof.* Let  $Y = Q-1$  and

$$g(X, Y) \stackrel{\text{df}}{=} \frac{f(X, Y)}{YX(X-1)}$$

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

$$\frac{\partial f}{\partial Y} = \frac{\partial [X]_Q}{\partial Q} = \frac{XQ^{X-1} - [X]_Q}{Q-1}$$

If  $(x, y) \in M$ , then  $(x, y) \in V(f)$ , so  $[x]_q = x$ . Therefore

$$\frac{\partial f}{\partial Y}(x, y) = x[x-1]_q$$

Since  $g = f/YX(X-1)$ ,

$$\frac{\partial g}{\partial Y} = \frac{1}{YX(X-1)} \frac{\partial f}{\partial Y} - \frac{g}{Y}$$

By the power series expression for  $g$  we have  $g(X, 0) = 1/2$ , so in particular if  $(x, y) \in M$  then  $y \neq 0$ , hence  $(g/Y)(x, y) = 0$ , hence

$$\frac{\partial g}{\partial Y}(x, y) = \frac{1}{yx(x-1)} \frac{\partial f}{\partial Y}(x, y) = \frac{[x-1]_q}{y(x-1)}$$

Using  $q^X \stackrel{\text{df}}{=} e^{X \log q}$ , 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 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  $\frac{\partial g}{\partial Y}(x, y) \neq 0$  for all  $(x, y) \in M$ . ■

**Definitions.** Let  $\phi_1 : M \rightarrow O_p$  and  $\phi_2 : M \rightarrow B(0, p^{-1/(p-1)})$  be the projections, and let  $M_y = \phi_2^{-1}(y)$  denote the fiber of  $\phi_2$  over  $y \in B(0, p^{-1/(p-1)})$ . We identify  $M_y$  with  $\phi_1(M_y)$ , which is the set of nontrivial fixed points of  $[X]_q$ , for  $q = 1 + y$ .

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

$$\begin{aligned} [X]_q - X &= \sum_{n=0}^{\infty} c_n(x, q)(X-x)^n \\ &= ([x]_q - x) + \left( \frac{q^x \log q}{q-1} - 1 \right) (X-x) + \sum_{n=2}^{\infty} \frac{q^x (\log q)^n}{(q-1)n!} (X-x)^n \end{aligned}$$

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*

$$\phi_2(M) = \{q-1 \in B(0, p^{-1/(p-1)}) : p^{-1/(p-2)} \leq |q-1| < p^{-1/(p-1)}\}$$

*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  $N \geq 2$ , and since  $M$  excludes these solutions,  $M_{q-1}$  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  $v(c_n) > v(c_p)$  whenever  $n > p$ , and

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

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

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

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

Let  $A_n^{(i)}(X)$  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

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

where  $d_n(x, u) = \sum_{k=n}^{\infty} \binom{k}{n} \frac{A_k(x)}{(k+2)!} p^{km_0} u^{k-n}$ . Note  $d_n(x, 0) = \frac{A_n(x)}{(n+2)!} p^{nm_0}$ .

**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  $(x, q-1) \in M$ , 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 read off

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

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  $v(d_n) - v(d_{p-2}) > 0$ :

$$\begin{aligned} v(d_n) - v(d_{p-2}) &= v(A_n(x)) - v(A_{p-2}(x)) + (n - (p-2))m_0 + 1 + \frac{s_p(n+2) - (n+2)}{p-1} \\ &> v(A_n(x)) - v(A_{p-2}(x)) + \frac{s_p(n+2) - 1}{p-1} \geq 0 \end{aligned}$$

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  $(x, q-1) \in M$ , where  $q = 1 + p^{m_0}u$ . ■

**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  $\overline{M}_{q-1}$  denote the set of residues of the elements  $\phi_1(\phi_2^{-1}(q-1))$ .

- a) If  $m_0 < 1/(p-2)$ ,  $\overline{M}_{q-1} = \{2, \dots, p-1\}$ , and  $\text{Card}(M_{q-1}) = p-2$ .
- b) If  $m_0 = 1/(p-2)$ ,  $\overline{M}_{q-1} \cap \{2, \dots, p-1\} = \emptyset$ , and  $\text{Card}(M_{q-1}) \geq p-3$ .

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  $x \in M_{q-1}$ . Then  $v(A_{p-2}(x)) = 0$  if and only if  $\bar{x} \notin \{2, \dots, p-1\}$ , if and only if  $m_0 = 1/(p-2)$  by Proposition 4. Therefore  $\overline{M}_{q-1} \subset \{2, \dots, p-1\}$  if  $m_0 < 1/(p-2)$ , and  $\overline{M}_{q-1} \cap \{2, \dots, p-1\} = \emptyset$  if  $m_0 = 1/(p-2)$ .

If  $m_0 < 1/(p-2)$  then  $v(c_n(x, q)) > v(c_p(x, q))$  for  $n = 2, \dots, p-1$  by (\*). 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  $x \in M_{q-1}$  with any given residue, and  $\text{Card}(M_{q-1}) = p-2$ .

If  $m_0 = 1/(p-2)$  then  $v(c_2(x, q)) = v(c_p(x, q)) = m_0$  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  $[X]_q$  has fixed points  $x, x'$ , and  $x''$ , such that  $x \neq x''$  and  $\bar{x} = \bar{x}'' \neq \bar{x}'$ . 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  $M_{q-1}$  with the same residue, hence  $\text{Card}(M_{q-1}) \geq p-3$ . The last statement is immediate. ■

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

$$\phi_1(M) = \bigcup_{\substack{a \in O_p \\ \bar{a} \notin \{2, \dots, p-1\}}} B(a, 1) \cup \bigcup_{a \in \{2, \dots, p-1\}} B(a, 1) - \overline{B}(a, p^{-1/(p-1)})$$

where the left union corresponds to  $v(q-1) = 1/(p-2)$ , the right union to  $v(q-1) < 1/(p-2)$ . Note no rational integer not congruent to 0 or 1 (mod  $p$ ) may be a fixed point of any  $[X]_q$ .

**Theorem 6.** Suppose  $x \in O_p$  is a nontrivial fixed point of  $[X]_q$ , for some  $q \in B(1, p^{-1/(p-1)})$ . Then  $\text{Card}(\phi_1^{-1}(x)) = p-2$ , and each  $(x, q-1) \in \phi_1^{-1}(x)$  determines a distinct residue  $\bar{u}$ , for  $q-1 = p^{m_0}u$  and  $m_0 = v(q-1)$ . If  $(x, q-1) \in M$  and  $x' \in B(x, |A_{p-2}(x)|)$  then there exists a unique  $q' \in B(q, |q-1|)$  such that  $(x', q'-1) \in M$ , and the resulting map

$$Q(X) : B(x, |A_{p-2}(x)|) \rightarrow B(q, |q-1|)$$

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  $p^{1-(p-1)m_0}$ ) if and only if  $|A_{p-2}^{(1)}(x)| = 1$ , if and only if the multiplicity of  $\bar{x}$  in  $\overline{M}_{q-1}$  is one. This occurs for all but finitely many residue classes for  $x$ .

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

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

Since  $g(x, q-1) = 0$ , by Series B we have

$$g(x', q-1) = (x' - x) \sum_{k=1}^{\infty} a_k = (x' - x) \sum_{k=1}^{\infty} \frac{D_k(x')}{(k+2)!} p^{km_0} u^k$$

where  $D_k(X) = (A_k(X) - A_k(x))/(X - x)$ . Compute

$$\begin{aligned} v(a_k) &= v(D_k(x')) + km_0 - \frac{k+2 - s_p(k+2)}{p-1} \\ &= v(D_k(x')) + k\delta + \frac{s_p(k+2) - 2}{p-1} \end{aligned}$$

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  $k = p^r - 2$ ,  $v(a_k) = v(D_{p^r-2}(x')) + (p^r - 2)\delta - 1/(p-1)$ .

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  $|A_{p^r-2}^{(1)}(x)| < 1$  for  $r > 1$ , since  $x$  is a multiple root of  $A_{p^r-2}(X) \pmod{p}$  for  $r > 1$ . Since

$$D_k(x') = A_k^{(1)}(x) + \frac{1}{2!} A_k^{(2)}(x)(x' - x) + \dots + \frac{1}{k!} A_k^{(k)}(x)(x' - x)^{k-1}$$

we conclude  $v(D_{p^r-2}(x')) > v(D_{p-2}(x')) = 0 > v(A_{p-2}(x)) - v(x' - x)$  for  $r > 1$  and  $x' \in B(x, |A_{p-2}(x)|)$ . Since  $(p^r - 2)\delta - (p-2)\delta = (p^r - p)\delta > 0$  for  $r > 1$ ,  $v(a_{p^r-2}) > v(a_{p-2})$  for  $m_0 < 1/(p-2)$ , and so  $v(a_{p-2}) = (p-2)m_0 - 1$  is the unique minimum value of all of the coefficients. We conclude  $|g(x', q-1)| = p^{1-(p-2)m_0}|x' - x| = |A_{p-2}(x)|^{-1}|x' - x|$ , and since  $x' \in B(x, |A_{p-2}(x)|)$ , this shows  $1 > |g(x', q-1)| > |x' - x|$  when  $m_0 < 1/(p-2)$ .

If  $m_0 = 1/(p-2)$ , then  $|A_{p-2}(x)| = 1$  by Proposition 5. We compute

$$A_{p-2}^{(1)}(X) = (p-2)X^{p-3} + (p-3)X^{p-4} + \dots + 2X + 1 \pmod{p}$$

Thus for all but finitely many residue classes  $\bar{x}$ , we have  $A_{p-2}^{(1)}(x) \not\equiv 0 \pmod{p}$ , hence  $D_{p-2}(x') = A_{p-2}^{(1)}(x) \not\equiv 0 \pmod{p}$  whenever  $x' \in B(x, 1)$ , 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  $v(a_{p^r-2}) \geq (p^r - p)/(p-1)(p-2) > 0$  for  $r > 1$ , this shows  $|g(x', q-1)| = |x' - x|$  when  $(m_0 = 1/(p-2) \text{ and } |A_{p-2}^{(1)}(x)| = 1)$ .

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

We have shown that  $|A_{p-2}^{(1)}(x)| = 1$  implies  $|g(x', q-1)| = p^{1-(p-2)m_0}|x' - x|$ , hence that  $g(x', q-1) \neq 0$  if  $\bar{x}' = \bar{x}$ , i.e., the multiplicity of  $\bar{x}$  in  $\overline{M}_{q-1}$  is one. Conversely, suppose  $x \in M_{q-1}$  and  $\bar{x}$  has multiplicity one in  $\overline{M}_{q-1}$ . We have already seen that  $|A_{p-2}^{(1)}(x)| = 1$  if  $\bar{x} \in \{0, 1\}$ , and otherwise  $v(c_1(x, q)) = v(c_p(x, q)) = (p-1)m_0 - 1$  are the minimum values in Series A for  $f(X, q-1)$ , and  $v(f(x', q-1)) = v(c_1(x, q)(x' - x)) = v(x' - x) + (p-1)m_0 - 1$ . Therefore  $|g(x', q-1)| = p^{1-(p-2)m_0}|x' - x| \geq |x' - x|$ , for all  $x' \in B(x, 1)$ , and it follows from the above that  $|A_{p-2}^{(1)}(x)| = 1$ .

Next we construct the map  $Q(X) : B(x, |A_{p-2}(x)|) \rightarrow B(q, |q-1|)$ , by looking at the polygon for  $g(x', p^{m_0}U)$  expanded in Series B around  $u$ , for  $x' \in B(x, |A_{p-2}(x)|)$ . We've already shown  $v(d_0(x', u)) \equiv v(g(x', q-1)) > 0$ , and now claim  $v(d_1(x', u)) = v(d_{p-2}(x', 0)) = 0$ . Consider the series

$$d_1(x', u) = \sum_{k=1} kd_k(x', 0)u^{k-1} = \sum_{k=1} k \frac{A_k(x')}{(k+2)!} p^{km_0} u^{k-1}$$

We've seen  $v(d_k(x', 0)) > v(d_{p-2}(x', 0))$  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  $A_{p-2}(X)$  divides  $A_{p^r-2}(X)$ , we have  $v(A_{p^r-2}(x)) \geq v(A_{p-2}(x))$ , and now it is easy to see  $v(d_{p^r-2}(x', 0))$  is strictly minimized at  $r = 1$ , hence  $v(d_1(x', u)) = v(d_{p-2}(x', 0))$ . Since  $v(D_{p-2}(x')) \geq 0$ , we have  $v(A_{p-2}(x') - A_{p-2}(x)) \geq v(x' - x) > v(A_{p-2}(x))$ , hence  $v(A_{p-2}(x')) = v(A_{p-2}(x)) = 1 - (p-2)m_0$ , and we compute  $v(d_{p-2}(x', 0)) = 0$ . Therefore  $v(d_1(x', u)) = 0$ .

Since  $v(d_0(x', u)) > v(d_1(x', u)) = 0$ , the Newton polygon for  $g(x', p^{m_0}U)$  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  $\bar{u}' = \bar{u}$ , and  $v(u' - u) = v(d_0(x', u)) = v(g(x', q-1))$ . Setting  $q' = 1 + p^{m_0}u'$ , we compute

$$|q' - q| = p^{-m_0}|g(x', q-1)| = |([x']_q - x')/x'(x' - 1)|$$

If  $|A_{p-2}^{(1)}(x)| = 1$ , then  $|q' - q| = p^{1-(p-1)m_0}|x' - x|$ , so  $Q(X)$  is a contraction. If  $|A_{p-2}^{(1)}(x)| < 1$ , then  $|q' - q| < p^{1-(p-1)m_0}|x' - x|$ , and  $Q(X)$  is not a contraction. For then the explicit formula for  $D_{p-2}(X)$  shows that  $|D_{p-2}(x')| = 1$  in the limit as  $|x' - x|$  approaches  $1 = |A_{p-2}(x)|$ , hence  $|q' - q|$  approaches  $p^{1-(p-1)m_0}|x' - x|$  arbitrarily closely for  $x' \in B(x, 1)$ .

This  $u'$  is unique since the  $p-2$  solutions for  $U$  in  $g(x', p^{m_0}U)$  have distinct residues, by the preceding argument. Thus we have a well defined map

$$Q(X) : B(x, |A_{p-2}(x)|) \rightarrow B(q, |q-1|)$$

sending  $x'$  to  $q' = Q(x') = 1 + p^{m_0}u'$ . This map is analytic by Proposition 2.

Next we show  $Q(X)$  is surjective. Suppose  $(x, q-1) \in M$ , and  $q' \in B(q, |q-1|)$ . Since  $|q'-q| < |q-1|$ ,  $|q'-1| = |q-1| = p^{-m_0}$ . Define  $u$  and  $u'$  by  $q = 1 + p^{m_0}u$  and  $q' = 1 + p^{m_0}u'$ , and let  $\epsilon = u' - u$ , so that  $v(\epsilon) > 0$ . Since  $g(x, q-1) = 0$ , in Series B we have

$$g(x, q' - 1) = g(x, q' - 1) - g(x, q - 1) = \sum_{n=1}^{\infty} d_n(x, 0)((u + \epsilon)^n - u^n)$$

By the binomial theorem,  $\epsilon$  is a factor of each  $(u + \epsilon)^n - u^n$ , and so  $v(g(x, q' - 1)) \geq v(\epsilon) > 0$ .

We show there exists an  $x' \in B(x, |A_{p-2}(x)|) \cap M_{q'-1}$ . First assume  $\bar{x} \neq 0, 1$ , so that  $v(f(x, q' - 1)) = v(g(x, q' - 1)) + m_0$ . Let  $c_n(x, q')$  be the coefficient of Series A for  $f(X, q' - 1)$  expanded around  $x$ . Since  $v(g(x, q' - 1)) > 0$ , we have  $v(c_0(x, q')) = v(g(x, q' - 1)) + m_0 > m_0 \geq (p-1)m_0 - 1 = v(c_p(x, q'))$ , hence  $v(c_0(x, q')) > v(c_p(x, q'))$ . Therefore  $f(X, q' - 1)$  has a solution  $X = x'$  such that  $|x' - x| < 1$ , and  $x' \in B(x, 1) \cap M_{q'-1}$ . 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  $\bar{x}'$  in  $\bar{M}_{q'-1}$  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  $v(x' - x) = v(c_0(x, q')) - v(c_1(x, q')) > v(A_{p-2}(x))$ , as desired.

Next, suppose  $\bar{x} = 0$ , then  $m_0 = 1/(p-2)$  by Proposition 5, and  $|A_{p-2}(x)| = 1$ . Since  $0 \in B(x, 1)$ , and  $Q(X) : B(x, 1) \rightarrow B(q, |q-1|)$ , we may assume  $x = 0 \in M_{q'-1}$ . Series A for  $f(X, q' - 1)$  expanded around 0 has the trivial fixed point 0, so  $c_0(0, q') = 0$ / we will show  $v(c_1(0, q')) > v(c_2(0, q'))$ . Since  $m_0 = 1/(p-2)$ , we compute  $v(c_2(0, q')) = m_0 = v(c_p(0, q'))$  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

$$\begin{aligned} -1 + \sum_{n=1} \frac{(-1)^{n+1}}{n} (q' - 1)^{n-1} &= \sum_{n=0} \frac{(-1)^{n+1}}{n+2} (q' - 1)^{n+1} \\ &= -(q' - 1)/2 + (q' - 1)^2/3 - \dots + (q' - 1)^{p-1}/p - \dots \end{aligned}$$

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  $v(q' - q) > m_0$  and  $v((q' - 1)^{p-1} - (q - 1)^{p-1}) > v(p) + m_0$ . Writing  $q' - 1 = q - 1 + p^{m_0}\epsilon$  with  $v(\epsilon) > 0$ , as before, we immediately verify  $v(q' - q) > m_0$ , and applying the binomial theorem, we see  $v((q - 1 + p^{m_0}\epsilon)^{p-1} - (q - 1)^{p-1}) > 1 + m_0$ . We conclude  $v(c_1(0, q')) > v(c_2(0, q'))$ , and the Newton polygon shows there exists an  $x' \in B(0, 1) \cap M_{q'-1}$ , 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  $B(x, 1) \cap M_{q'-1}$  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

$$\begin{aligned} -1 + \sum_{n=1} \frac{(-1)^{n+1}}{n} q'(q' - 1)^{n-1} &= -1 + q' + \sum_{n=1} \frac{(-1)^n}{n+1} q'(q' - 1)^n \\ &= -(\frac{q'}{2} - 1)(q' - 1) + \frac{q'}{3}(q' - 1)^2 - \dots + \frac{q'}{p}(q' - 1)^{p-1} - \dots \end{aligned}$$

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  $x' \in B(1, 1) \cap M_{q'-1}$  exists, as desired.

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

**Remark.** If the multiplicity of the residue  $\bar{x}$  in  $\overline{M}_{q-1}$  is not equal to one, then by Proposition 5 and Theorem 6, its multiplicity is two,  $\text{Card}(\overline{M}_{q-1}) = p - 3$ ,  $|A_{p-2}(x)| = 1$ , 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  $\overline{M}_{Q(x')-1}$ . 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  $M_{q-1}$ ). 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  $M(\mathbb{Z}_p) = \{(x, q - 1) \in M : x, q \in \mathbb{Z}_p\}$ . 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*

$$\begin{aligned} Q(X) : B(1, 1) &\longrightarrow B(4, 3^{-1}) \\ B(0, 1) &\longrightarrow B(7, 3^{-1}) \end{aligned}$$

*with  $|q' - q| = |x' - x|/3$ .*

*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,  $\phi_1(M) \cap \mathbb{Z}_3 = \{x \in \mathbb{Z}_3 : x \not\equiv 2 \pmod{3}\}$ , 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  $B(7, 3^{-1})$ . ■

**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

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

## References.

- [A] Arens, R.: *Homeomorphisms preserving measure in a group*, Ann. of Math., **60**, no. 3, (1954), pp. 454–457.
- [B] Bishop, E.: *Isometries of the  $p$ -adic numbers*, J. Ramanujan Math. Soc. **8** (1993), no. 1-2, 1–5.
- [C] Conrad, K.: *A  $q$ -analogue of Mahler expansions. I*, Adv. Math. **153** (2000), no. 2, 185–230.
- [D] Dieudonné, J.: *Sur les fonctions continues  $p$ -adiques*, Bull. Sci. Math. (2) **68** (1944), 79–95.
- [F] Fray, R. D.: *Congruence properties of ordinary and  $q$ -binomial coefficients*, Duke Math. J. **34** (1967), 467–480.
- [G] F. Q. Gouvêa,  *$p$ -adic Numbers, An Introduction* Second edition, Springer-Verlag, New York, 2003.
- [J] Jackson, Rev. F. H.:  *$q$ -difference equations*, Amer. J. Math. **32** (1910), 305–314.
- [M] Mahler, K.: *An interpolation series for continuous functions of a  $p$ -adic variable*, J. Reine Angew. Math. **199** (1958) 23–34.
- [Se] J.-P. Serre, *Lie Algebras and Lie Groups*, LNM 1500, Springer-Verlag, New York, 1992.
- [Su] Sushchanskiĭ, V. I.: *Standard subgroups of the isometry group of the metric space of  $p$ -adic integers*, VBisnik Kiïv. UnBiïv. Ser. Mat. Mekh. **117** no. 30 (1988), 100–107.