

COMPOSITIO MATHEMATICA

HUA-CHIEH LI

Counting periodic points of p -adic power series

Compositio Mathematica, tome 100, n° 3 (1996), p. 351-364

<http://www.numdam.org/item?id=CM_1996__100_3_351_0>

© Foundation Compositio Mathematica, 1996, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Counting periodic points of p -adic power series

HUA-CHIEH LI

Department of Mathematics, Brown University, Providence, Rhode Island, U.S.A.

Received 23 June 1994; accepted in final form 2 February 1995

Abstract. Lubin conjectures that for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background. Our main theorem gives us an effective method to compute the number of periodic points of these invertible series. It turns out that this computation lends support to the conjecture of Lubin.

1. Introduction

Let K be an algebraic extension of \mathbf{Q}_p and let \mathcal{O} be its integer ring with maximal ideal \mathcal{M} and residue field k . If \overline{K} is an algebraic closure of K , we denote by $\overline{\mathcal{O}}$ and $\overline{\mathcal{M}}$ the integral closure of \mathcal{O} in \overline{K} and the maximal ideal of $\overline{\mathcal{O}}$, respectively.

When $f(x) \in \mathcal{O}[[x]]$, but not all coefficients of $f(x)$ are in \mathcal{M} , then the lowest degree in which a unit coefficient appears will be called the Weierstrass degree of $f(x)$, denoted $\text{wided}(f)$. According to the Weierstrass Preparation Theorem there exist a unit power series $U(x) \in \mathcal{O}[[x]]$ and a distinguished polynomial $P(x) \in \mathcal{O}[[x]]$ such that $f(x) = P(x)U(x)$ and $\text{deg}(P) = \text{wided}(f)$. All roots of P are in $\overline{\mathcal{M}}$. If $\text{wided}(f) = d$, then, counting multiplicity, there are d of them and they exhaust all roots of f that are in $\overline{\mathcal{M}}$.

The set of all power series over \mathcal{O} without constant terms is a monoid (non-commutative, associative, with unit) under composition. A series $u(x) \in \mathcal{O}[[x]]$ without constant term is called invertible if there exists a series $w(x) \in \mathcal{O}[[x]]$ such that $u \circ w(x) = x$. A necessary and sufficient condition for $u(x)$ to be invertible is that $u'(0) \in \mathcal{O}^*$. Let $u(x)$ be an invertible series without constant term in $\mathcal{O}[[x]]$. Since $\text{wided}(u) = 1$, $u(x)$ has no other roots than 0 in $\overline{\mathcal{M}}$. We denote $u^{on}(x)$ the n -fold iteration of $u(x)$ with itself. The point $\alpha \in \overline{\mathcal{M}}$ is a fixed point for $u(x)$ if $u(\alpha) = \alpha$. The point α is a periodic point of period n if $u^{on}(\alpha) = \alpha$. The least positive n for which $u^{on}(\alpha) = \alpha$ is called the prime period of α . We assume that the series $u(x)$ always satisfies $u'(0) \in 1 + \mathcal{M}$; finiteness of the residue field guarantees that any invertible series has an iterate with this property. Let $p \nmid m$. It is important to know that if α is a periodic point of period $p^n m$, then it is a periodic point of period p^n (see Li [2, Corollary 2.3.2]). Therefore, we only have to study periodic points whose periods are powers of p .

To count the number of periodic points of $u(x)$ brings in very delicate questions about automorphisms of local fields. We define the number of fixed points of

$u^{\circ p^n}(x)$ (i.e. the number of periodic points of period p^n), counting multiplicity, by $i_n(u)$. Thus $i_n(u) = \text{widedeg}(u^{\circ p^n}(x) - x)$. Sen's theorem [6] shows that when $i_n(u) < \infty$ then $i_{n-1}(u) \equiv i_n(u) \pmod{p^n}$. Keating [1], using local class field theory, says that under certain circumstance we have $i_n(u) = 2 + bp + \dots + bp^n$, for some $0 < b < p$. In this paper we give a formula for $i_n(u)$ when u is an automorphism of a formal group.

If $f(x) \in \mathcal{O}[[x]]$ without constant term and $f'(0) \in \mathcal{M}$, then we call $f(x)$ a noninvertible series. A noninvertible series can have no other fixed points than 0, but the roots of iterates are of serious interest. In the invertible series case, the periodic points now play a role parallel to the roots of a noninvertible series. These two studies become no longer disjoint in case an invertible series commutes with a noninvertible series (Lubin [4]). In the case that a dynamical system over the ring of local integers \mathcal{O} arises from a formal group, i.e. when we are discussing the properties of the iterates of an endomorphism of a formal group defined over \mathcal{O} , the full commuting family contains both invertible and noninvertible series. Lubin conjectures that for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background. Lubin's Main Theorem in [4] supports this conjecture, in that it says that the only possible finite Weierstrass degree for such a noninvertible series is a power of p . In this paper we shall give another proof of Lubin's Theorem and extend the idea to prove our main theorem which says that if $u(x)$ commutes with some noninvertible power series, then there exists m such that for all $n > m$,

$$i_n(u) = a + bp^\lambda + bp^{2\lambda} + \dots + bp^{(n-m)\lambda}$$

for some a, b and λ , a phenomenon same as automorphisms of a formal group. Our main theorem gives us an effective method to compute the number of periodic points of these invertible series. It turns out that this computation lends support to the conjecture of Lubin.

The work presented here is part of the author's 1994 Brown Ph.D. thesis. Without Professor Rosen's continued help and encouragement, none of this work would have been possible. Professor Lubin was the one who introduced the author to the field of p -adic Dynamical Systems. His guidance in this research was indispensable.

2. Automorphisms of formal groups

At all times, formal groups come into our study as a guide. To my knowledge, the only examples we have for an invertible series $u(x)$ to commute with a noninvertible series, are when $u(x)$ is an automorphism of a formal group or a *condensation*. Let $F(x, y)$ be a one-dimensional formal group over \mathcal{O} . Recall that if $f(x) \in \text{End}_{\mathcal{O}}(F)$ (i.e. $f(x) \in \mathcal{O}[[x]]$ and satisfies $F(f(x), f(y)) = f(F(x, y))$), then $\text{widedeg}(f) = p^r$ for some natural number r . We also know that if $f, g \in \text{End}_{\mathcal{O}}(F)$

and $f'(0) = g'(0)$, then $f = g$. Therefore if $f'(0) = a$, then we denote $f(x)$ by $[a](x)$. We have the following properties:

- (1) If $[a](x) \in \text{End}_{\mathcal{O}}(F)$, then $[-a](x) \in \text{End}_{\mathcal{O}}(F)$.
- (2) If $[a](x), [b](x) \in \text{End}_{\mathcal{O}}(F)$, then $[ab](x) = [a] \circ [b](x) = [b] \circ [a](x) \in \text{End}_{\mathcal{O}}(F)$.
- (3) If $[a](x), [b](x) \in \text{End}_{\mathcal{O}}(F)$, then $[a+b](x) = F([a](x), [b](x)) \in \text{End}_{\mathcal{O}}(F)$.

Let $u(x) = [1 + b](x) \in \text{End}_{\mathcal{O}}(F)$ with $b \in \mathcal{M}$. Then $[b](x) \in \text{End}_{\mathcal{O}}(F)$ and we have that $\alpha \in \overline{\mathcal{M}}$ is a fixed point of $u(x)$ if and only if α is a root of $[b](x)$. Since every root (resp. fixed point) of a noninvertible (resp. invertible) endomorphism of a formal group is simple, we have $\text{wided}([b](x)) = \text{wided}(u(x) - x)$.

If $u(x)$ is an automorphism of a formal group, then we can easily find $i_n(u)$. Recall that K is a field which is complete with respect to a valuation, v . We normalize the valuation v such that $v(\pi) = 1$, where π is a generator of \mathcal{M} .

LEMMA 2.1. *If $f \circ g = g \circ f$, then*

$$\text{wided}(g)^{v(f'(0))} = \text{wided}(f)^{v(g'(0))}.$$

Proof. See Li [3] Corollary 3.2.1. □

PROPOSITION 2.2. *Let $u(x)$ be an automorphism of a formal group with $u'(0) = 1 + b$ where $b \in \mathcal{M}$ and suppose that $\text{wided}([p]) = p^s$.*

- (1) *If $v(p) < (p - 1)v(b)$, then*

$$i_n(u) = p^{s(\frac{v(b)}{v(p)} + n)}.$$

- (2) *If $p^m(p - 1)v(b) > v(p) > p^{m-1}(p - 1)v(b)$, then*

$$i_n(u) = \begin{cases} p^{sp^n \frac{v(b)}{v(p)}}, & \text{if } m \geq n \geq 0 \\ p^{s(n-m+p^m \frac{v(b)}{v(p)})}, & \text{if } n > m. \end{cases}$$

- (3) *If $p^m(p - 1)v(b) = v(p)$ and $(1 + b)^{p^{m+1}} = 1 + b'$ with $b' \neq 0$, then*

$$i_n(u) = \begin{cases} p^{sp^n \frac{v(b)}{v(p)}}, & \text{if } m \geq n \geq 0 \\ p^{s(n-m-1 + \frac{v(b')}{v(p)})}, & \text{if } n > m. \end{cases}$$

Proof. We have $\text{wided}([b]) = p^{sv(b)/v(p)}$, by Lemma 2.1. For every n , denote $(1 + b)^{p^n} - 1 = b_n$. Hence $u^{\circ p^n}(x) = [1 + b_n](x)$.

If $v(p) < (p - 1)v(b)$, then $(1 + b)^{p^n} = 1 + b_n$ with $v(b_n) = nv(p) + v(b)$. Suppose that $\text{wided}([b_n]) = p^l$. Since $i_n(u) = \text{wided}([b_n])$ and $lv(p) = sv(b_n)$, we find that $i_n(u) = p^{sv(b_n)/v(p)}$. Our claim follows.

Suppose $p^m(p - 1)v(b) \geq v(p) > p^{m-1}(p - 1)v(b)$. If $m \geq n \geq 0$, then we have $v(b_n) = v(b^{p^n})$. Hence $i_n(u) = \text{wided}([b_n]) = \text{wided}([b]^{\circ p^n}) = (p^{sv(b)/v(p)})^{p^n}$.

If $n > m$, then $v(b_n) = (n - m - 1)v(p) + v(b_{m+1})$. Since $v(b_{m+1}) = v(p) + v(b_m) = v(p) + p^m v(b)$ if $p^m(p - 1)v(b) > v(p)$, our proof is complete. \square

Let r be a positive integer which is not divisible by p and let ρ be a primitive r th root of unity. Suppose that $w(x) \in \mathcal{O}[[x]]$ with $w'(0) = \rho$ and $w^{\circ r}(x) = x$. Then there exists an invertible series $\mu(x) \in \mathcal{O}[[x]]$ such that $w^\mu(x) = \mu \circ w \circ \mu^{\circ -1}(x) = \rho x$. (See Lubin [5, Lemma 4.1.1].) Suppose that $f \in \mathcal{O}[[x]]$ with $f \circ w = w \circ f$. Then we also have that f^μ commutes with w^μ . Let $f^\mu(x) = \sum_i a_{n_i} x^{n_i}$ where $a_{n_i} \neq 0$. Since $\rho(\sum_i a_{n_i} x^{n_i}) = \sum_i a_{n_i} (\rho x)^{n_i}$, $\rho = \rho^{n_i}$ for all n_i . Thus $n_i - 1 \equiv 0 \pmod{r}$. Hence we can write f^μ as $x f_1(x^r)$, for some $f_1(x) \in \mathcal{O}[[x]]$. Let $\hat{f}(x) = x f_1(x)^r$. We call \hat{f} a condensation of f . It is easy to check that if $f \circ g = g \circ f$, then $\hat{f} \circ \hat{g} = \hat{g} \circ \hat{f}$.

If $F(x, y)$ is any formal group over \mathcal{O} , then by the existence of the primitive $p - 1$ -th roots of unity in \mathbf{Z}_p , we can always find a condensation. Suppose $[\rho](x) \in \text{End}_{\mathcal{O}}(F)$ where ρ is a primitive r -th roots of unity with $(r, p) = 1$. We have that $[\rho]^{\circ r}(x) = x$. If $u(x)$ is an invertible series in $\text{End}_{\mathcal{O}}(F)$, then it is an easy exercise to get

$$i_n(\hat{u}) = \frac{i_n(u) - 1}{r} + 1.$$

3. Main theorem

We denote by $\mathcal{S}_0(\mathcal{O})$ the set of power series $f \in \mathcal{O}[[x]]$ such that $f(0) = 0$ and $f'(0)$ is neither 0 nor any root of 1. Let $u, f \in \mathcal{S}_0(\mathcal{O})$ be an invertible and a noninvertible series, respectively, which commute with each other. Then the set of roots of iterates of $f(x)$ is equal to the set of periodic points of $u(x)$ (Lubin [4]). We have the following result.

PROPOSITION 3.1. *Let $u, f \in \mathcal{S}_0(\mathcal{O})$ be an invertible and a noninvertible series, respectively, which commute with each other. Suppose that $\alpha \in \overline{\mathcal{M}}$ is a fixed point of u . Then $u'(\alpha)^r = u'(0)$ if and only if α is a root of multiplicity r of some iterate of f .*

Proof. First we make the elementary observation that if there exists r such that $u'(\alpha)^r = u'(0)$, then it is unique. Suppose that $u'(\alpha)^{r'}$ is also equal to $u'(0)$. Then $u'(\alpha)^r = u'(\alpha)^{r'}$. Since $u(x) \in \mathcal{S}_0(\mathcal{O})$, $u'(0)$ is neither 0 nor a root of 1. Hence $u'(\alpha)$ can not be either 0 or root of 1. Therefore $r = r'$.

It is easy to check that if $\alpha \in \overline{\mathcal{M}}$ is a root of $f(x)$ of multiplicity r , then α is also a root of $f^{\circ n}(x)$ of multiplicity r for every $n > 0$. Without loss of generality, we suppose that $f(\alpha) = 0$. Consider

$$\frac{f \circ u(x) - f \circ u(\alpha)}{(u(x) - u(\alpha))^i} = \frac{u \circ f(x) - u \circ f(\alpha)}{f(x) - f(\alpha)} \frac{f(x) - f(\alpha)}{(x - \alpha)^i} \frac{(x - \alpha)^i}{(u(x) - u(\alpha))^i}.$$

Since $u(x)$ (resp. $f(x)$) tends to $u(\alpha) = \alpha$ (resp. $f(\alpha) = 0$) as x tends to α , we find that

$$\lim_{x \rightarrow \alpha} \frac{f \circ u(x) - f \circ u(\alpha)}{(u(x) - u(\alpha))^i} = \lim_{x \rightarrow \alpha} \frac{f(x) - f(\alpha)}{(x - \alpha)^i} \text{ and}$$

$$\lim_{x \rightarrow \alpha} \frac{u \circ f(x) - u \circ f(\alpha)}{f(x) - f(\alpha)} = u'(0).$$

Thus

$$\lim_{x \rightarrow \alpha} \frac{f(x)}{(x - \alpha)^i} = u'(0) \lim_{x \rightarrow \alpha} \frac{f(x)}{(x - \alpha)^i} u'(\alpha)^{-i}.$$

Hence if α is a root of $f(x)$ of multiplicity r , then $u'(\alpha)^r = u'(0)$. Conversely, suppose that $u'(\alpha)^r = u'(0)$. Since for $i < r$, $u'(\alpha)^i \neq u'(0)$, we have $\lim_{x \rightarrow \alpha} f(x)/(x - \alpha)^i = 0$. Thus α is a root of multiplicity greater than $r - 1$. If $\lim_{x \rightarrow \alpha} f(x)/(x - \alpha)^r = 0$, then $\lim_{x \rightarrow \alpha} f(x)/(x - \alpha)^{r+1}$ exists. Since $u'(\alpha)^{r+1} \neq u'(0)$, $\lim_{x \rightarrow \alpha} f(x)/(x - \alpha)^{r+1} = 0$. By induction, $\lim_{x \rightarrow \alpha} f(x)/(x - \alpha)^n = 0$ for all n . This is impossible, unless $f(x) = 0$. Therefore α is a root of multiplicity r . □

REMARK 1. Let α be a simple root of $u(x) - x$. Then we call α a simple fixed point of $u(x)$. We know that a fixed point α is a simple fixed point of all iterates of $u(x)$ if and only if $u'(\alpha)$ is not a root of 1. Proposition 3.1 tells us that if u commutes with some noninvertible series, then $u'(\alpha)^n = u'(0)$ for some n . Since $u'(0)$ is not a root of 1, hence $u'(\alpha)$ is not a root of 1, either. Therefore every periodic point of u is simple.

EXAMPLE 1. We know that in \mathbf{Q}_3 , $u(x) = 3x + x^3$ is a Lubin-Tate formal power series. Therefore there is an invertible series $w(x) \in \mathbf{Z}_3[[x]]$ with $w'(0) = 2$ which commutes with $u(x)$. Consider over \mathbf{Z}_2 . There is no power series $f(x) \in \mathbf{Z}_2[[x]]$ with $f'(0) = 2$ such that $f \circ u = u \circ f$. Indeed, now $u(x)$ is an invertible series with fixed points $0, \sqrt{2}i$ and $-\sqrt{2}i$. Since $u'(0) = 3$ and $u'(\pm\sqrt{2}i) = -3$, there is no $n \in \mathbf{N}$ such that $u'(\pm\sqrt{2}i)^n = u'(0)$. Therefore there is no noninvertible series over the integer ring of any algebraic extension of \mathbf{Q}_2 which can commute with $u(x)$.

The example above tells us that not every invertible series can commute with a noninvertible series. Conversely, not every noninvertible series can commute with an invertible series. In [4], Lubin’s Main Theorem says that the only possible finite Weierstrass degree for such a noninvertible series is a power of p . Here, we shall give another proof of Lubin’s Theorem and extend this idea to prove our main theorem.

First we make following simple observation. Let $s = tp^{o(s)}$ where $p^{o(s)}$ is the highest power of p dividing s and t is prime to p . Then in k (a field of characteristic p), we have

$$\begin{aligned} (x + ax^r)^{tp^{o(s)}} &\equiv (x^t + tax^{r+t-1})^{p^{o(s)}} \\ &\equiv x^{tp^{o(s)}} + (ta)^{p^{o(s)}} x^{p^{o(s)}(r+t-1)} \pmod{\text{higher degree}}. \end{aligned}$$

Thus

$$(x + ax^r)^s \equiv x^s + (ta)^{p^{o(s)}} x^{s+p^{o(s)}(r-1)} \pmod{\text{higher degree}}. \tag{*}$$

THEOREM 3.2. (Lubin) *Let u, f be invertible and noninvertible, respectively, in $S_0(\mathcal{O})$. Suppose further that $u \circ f = f \circ u$ and that f has finite Weierstrass degree d . Then $d = p^l$ for some $l > 0$.*

Moreover, let \bar{f} be the corresponding series of f over the residue field k . Then \bar{f} has the form $\bar{f}(x) = g(x^{p^l})$ for some $g \in k[[x]]$.

Proof. By replacing u by u^{o^n} for suitable n , we may assume that $u'(0) \equiv 1 \pmod{\mathcal{M}}$. Let \bar{u} and \bar{f} be the corresponding series over the residue field k . Let $i_n = \text{wdeg}(u^{o^{p^n}}(x) - x)$. According to Lubin [4] Corollary 4.3.1, we have that if $i_n = \infty$ for some n , then u has only finitely many periodic points in $\overline{\mathcal{M}}$. If u commutes with some noninvertible series, then $u(x)$ has infinitely many periodic points (Lubin [4] Proposition 3.2). Hence $i_n \neq \infty$ for all n and $i_n \rightarrow \infty$ as $n \rightarrow \infty$. According to (*) above, every non-zero term $a_s x^s$ of \bar{f} contributes a power series of lowest degree $s + (i_n - 1)p^{o(s)}$ in $\bar{f} \circ \bar{u}^{o^{p^n}}(x) - \bar{f}(x)$. Let S_0 be the set of degrees of non-zero terms of \bar{f} and let s_0 be the smallest number in S_0 with $o(s_0) = \inf \{o(s) \mid s \in S_0\}$. If $s \in S_0$ and $s > s_0$, then we have $s + (i_n - 1)p^{o(s)} > s_0 + (i_n - 1)p^{o(s_0)}$. If $s \in S_0$ and $s < s_0$, then when i_n is big enough we have that $s + (i_n - 1)p^{o(s)} > s_0 + (i_n - 1)p^{o(s_0)}$ because $o(s) > o(s_0)$. These tell us that when n is big enough the lowest degree of $\bar{f} \circ \bar{u}^{o^{p^n}}(x) - \bar{f}(x)$ is equal to $s_0 + (i_n - 1)p^{o(s_0)}$. On the other side, the first non-zero degree of $\bar{u}^{o^{p^n}}(\bar{f}(x)) - \bar{f}(x)$ is equal to di_n . Since $\bar{u}^{o^{p^n}}(\bar{f}) - \bar{f} = \bar{f}(\bar{u}^{o^{p^n}}) - \bar{f}$, we have $di_n = s_0 + (i_n - 1)p^{o(s_0)}$ for n large enough. Therefore after dividing both side of the equality by di_n and taking n to infinity, we have

$$\lim_{n \rightarrow \infty} \frac{s_0 + (i_n - 1)p^{o(s_0)}}{di_n} = \frac{p^{o(s_0)}}{d} = 1.$$

This means $d = p^{o(s_0)}$. Because $d \in S_0$, by the definition of s_0 , we have $d = p^{o(s_0)} = s_0$ and $p^{o(s_0)} \mid s$ for all $s \in S_0$. Therefore $\bar{f}(x) = g(x^{p^{o(s_0)}})$ for some $g(x) \in k[[x]]$. □

REMARK 2. In the proof of this Theorem, we only need the hypothesis that $\bar{f} \circ \bar{u} = \bar{u} \circ \bar{f}$.

Now let us consider the case that K is an unramified extension of \mathbf{Q}_p and let A be the residue ring $\mathcal{O}/\mathcal{M}^2$. Let \tilde{u} and \tilde{f} be the corresponding series over the residue ring A . Since $u'(0) \in 1 + \mathcal{M}$, by replacing u by u^{op} , we may assume that $u'(0) \equiv 1 \pmod{\mathcal{M}^2}$. Let $\tilde{u}(x) = x + \tilde{a}x^m + \dots + \tilde{b}x^n + \dots$ where m, n is the lowest degree of the monomial of $u(x) - x$ with coefficient in $\mathcal{M} \setminus \mathcal{M}^2$ and in \mathcal{O}^* , respectively. We have $\tilde{u}^{op}(x) \equiv x + p\tilde{b}x^n \pmod{x^{n+1}}$. Hence if we let j_n, i_n be the lowest degree of the monomial of $u^{op^n}(x) - x$ with coefficient in $\mathcal{M} \setminus \mathcal{M}^2$ and in \mathcal{O}^* , respectively, then we have $j_n = i_{n-1}$ and $j_n < i_n$ for all $n > 0$. Let S_1 be the set of degrees of terms of f whose coefficients are in $\mathcal{M} \setminus \mathcal{M}^2$, i.e. if $f(x) = \sum_{i=1}^{\infty} a_i x^i$, then $\forall i \in S_1, v(a_i) = 1$. We also let s_1 be the smallest number in S_1 with $o(s_1) = \inf \{o(s) \mid s \in S_1\}$. Consider $(x + pg(x) + bx^n)^{tp^r}$ where $g(x) \in \mathcal{O}[[x]]$, $b \in \mathcal{O}^*$ and $p \nmid t$. We have

$$(x + pg(x) + bx^n)^{tp^r} \equiv x^{tp^r} + tb^{p^r} x^{p^r(t-1)+np^r} \pmod{\mathcal{M}, \text{ higher degree}}.$$

Therefore if $s \in S_1$, $a_s x^s$ contributes a power series of lowest degree $s + (i_n - 1)p^{o(s)}$ in $\tilde{f} \circ \tilde{u}^{op^n}(x) - \tilde{f}(x)$. For the lowest degree contributed by $a_s x^s$ where $s \in S_0$, because $s_0 = p^{o(s_0)}$ and $o(s_0) > 0$, we only have to consider for $r > 0$,

$$(x + pg(x) + bx^n)^{p^r} \equiv x^{p^r} + pb^{p^{r-1}} x^{p^{r-1}(p-1)+np^{r-1}} \pmod{\mathcal{M}^2, \text{ higher degree}}.$$

Therefore by the definitions of s_0 and s_1 , we have that the lowest degree of $\tilde{f} \circ \tilde{u}^{op^n}(x) - \tilde{f}(x)$ is $\min \{s_1 + (i_n - 1)p^{o(s_1)}, s_0 + (i_n - 1)p^{o(s_0)-1}\}$. Notice that because $s_0 \neq s_1$, when i_n is large enough $s_1 + (i_n - 1)p^{o(s_1)} > s_0 + (i_n - 1)p^{o(s_0)-1}$, if $o(s_1) > o(s_0) - 1$ or if $o(s_1) = o(s_0) - 1$ and $s_1 > s_0$; otherwise $s_1 + (i_n - 1)p^{o(s_1)} < s_0 + (i_n - 1)p^{o(s_0)-1}$. For the lowest degree of $\tilde{u}^{op^n} \circ \tilde{f} - \tilde{f}$, we consider $(pg(x) + bx^t)^r$ where $g(x) \in \mathcal{O}[[x]]$, $g(0) = 0$ and $b \in \mathcal{O}^*$. The lowest degree of $(pg(x) + bx^t)^r \pmod{\mathcal{M}}$ is tr and the lowest degree of $(pg(x) + bx^t)^r \pmod{\mathcal{M}^2}$ is greater than $t(r - 1)$. Therefore the monomial $b_j x^j$ of $u^{op^n}(x) - x$ with $v(b_j) = 1$ contributes a power series of lowest degree $p^{o(s_0)}j$ in $\tilde{u}^{op^n} \circ \tilde{f} - \tilde{f}$ and the monomial $b_i x^i$ of $u^{op^n}(x) - x$ with $v(b_i) = 0$ contributes a power series of lowest degree greater than $p^{o(s_0)}(i - 1)$ in $\tilde{u}^{op^n} \circ \tilde{f} - \tilde{f}$. By the definitions of j_n and i_n , we have that the lowest degree of $\tilde{u}^{op^n} \circ \tilde{f} - \tilde{f}$ is $p^{o(s_0)}j_n$, because $j_n < i_n$. Suppose that $\tilde{u}^{op^n} \circ \tilde{f} - \tilde{f} = \tilde{f} \circ \tilde{u}^{op^n} - \tilde{f}$ for all n . We have that when n is large enough

$$p^{o(s_0)}j_n = \begin{cases} s_0 + (i_n - 1)p^{o(s_0)-1}, & \text{if } o(s_1) > o(s_0) - 1 \text{ or} \\ & \text{if } o(s_1) = o(s_0) - 1 \text{ and } s_1 > s_0. \\ s_1 + (i_n - 1)p^{o(s_1)}, & \text{otherwise} \end{cases}$$

Take $n = m$ and $n = m + 1$ in this equality and subtract them. We have

$$p^{o(s_0)}(j_{m+1} - j_m) = \begin{cases} (i_{m+1} - i_m)p^{o(s_0)-1}, & \text{if } o(s_1) > o(s_0) - 1 \text{ or} \\ & \text{if } o(s_1) = o(s_0) - 1 \text{ and } s_1 > s_0 \\ (i_{m+1} - i_m)p^{o(s_1)}, & \text{otherwise.} \end{cases}$$

for m large enough. Because $j_{m+1} - j_m = i_m - i_{m-1}$, we have $i_{m+1} - i_m = p^s(i_m - i_{m-1})$ where $0 < s \leq o(s_0)$. Therefore we have the following:

THEOREM 3.3 (Unramified Case). *Let \mathcal{O} be the ring of integers in a finite unramified extension field K of \mathbf{Q}_p , and let $u(x), f(x)$ be invertible and noninvertible, respectively, in $S_0(\mathcal{O})$. Suppose that $u \circ f = f \circ u$ and $\text{wideg}(f) = p^l$. If we denote $i_n(u) = \text{wideg}(u^{o p^n}(x) - x)$, then there exists M such that $\forall n > M, i_{n+1}(u) - i_n(u) = p^s(i_n(u) - i_{n-1}(u))$ for some fixed positive $s \leq l$.*

Proposition 2.2, gives us that when u is an automorphism of a formal group or a condensation, the $i_n(u)$'s satisfy the equality $i_{n+1} - i_n = p^s(i_n - i_{n-1})$ when n is large enough. Theorem 3.3 again supports Lubin's conjecture which says that for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background. This leads us to explore the general case (Theorem 3.9 below) for Theorem 3.3. Theorem 3.3 is a technically easier special case of Theorem 3.9, and the proof of Theorem 3.3 contains many of the ideas needed to prove Theorem 3.9. To prove the general case we need some notations.

NOTATION:

K is an algebraic extension of \mathbf{Q}_p with ramification index equal to e .

\mathcal{O} is the integer ring of K with maximal ideal \mathcal{M} .

$u(x) \in \mathcal{O}[[x]]$ is an invertible series with $u'(0) \equiv 1 \pmod{\mathcal{M}}$ which commutes with a noninvertible series $f(x) \in \mathcal{O}[[x]]$ with $\text{wideg}(f) = p^l$. Since we only discuss the case modulo \mathcal{M}^t for a finite number t , after taking some iterates of $u(x)$, we can always suppose that $u'(0) \equiv 1 \pmod{\mathcal{M}^t}$.

Set $m_n(0) = i_n(u) = \text{wideg}(u^{o p^n}(x) - x)$ and $m_n(r)$ equal to the lowest degrees of terms of $u^{o p^n}$ whose coefficients are in $\mathcal{M}^r \setminus \mathcal{M}^{r+1}$. Thus if $u^{o p^n}(x) - x = \sum_{i=1}^{\infty} b_i x^i$, then $m_n(r) = \inf \{i \mid v(b_i) = r\}$.

We also set $S_n(r)$ equal to the set of degrees of terms of $f^{o n}(x)$ whose coefficients are in $\mathcal{M}^r \setminus \mathcal{M}^{r+1}$. Thus if $f^{o n}(x) = \sum_{i=1}^{\infty} a_i x^i$, then $S_n(r) = \{i \mid v(a_i) = r\}$. Suppose that $m = \inf \{o(t) \mid t \in S_n(r)\}$. Let $s_n(r)$ be the smallest number in $S_n(r)$ with $o(s_n(r)) = m$, i.e. $s_n(r) = \inf \{i \mid v(a_i) = r, o(i) = m\}$.

Let $\{a_n\}_n, \{b_n\}_n$ be two sequences. Denote $\{a_n\}_n \gg \{b_n\}_n$, if $\liminf_{n \rightarrow \infty} a_n/b_n > 1$. Denote $\{a_n\}_n \sim \{b_n\}_n$, if $\liminf_{n \rightarrow \infty} a_n/b_n = 1$.

First we check some properties of the $s_n(r)$'s by taking iterates of $f(x)$.

PROPOSITION 3.4. *For every M and r there exists M' such that for every $j \leq r, o(s_n(j)) > M$ when $n \geq M'$.*

Proof. Given M , we can find n_0 such that $\text{wideg}(f^{o n_0}) = p^{n_0 l} > p^M$. By Theorem 3.2, we have that $o(s_n(0)) > M$ for all $n \geq n_0$. By induction, we suppose that for every $j < r$ there exists n_1 such that $o(s_n(j)) > M, \forall n \geq n_1$. Let

$f(x) = \sum_{i=1}^{\infty} a_i x^i$ and $f^{\circ n_1}(x) = \sum_{i=1}^{\infty} b_i x^i$. Consider $f \circ f^{\circ n_1}$. If $0 < v(a_i) \leq r$, then every non-zero term of $a_i (\sum_{i'} b_{i'} x^{i'})^i \pmod{\mathcal{M}^{r+1}}$ is contributed by some $b_{j'} x^{j'}$'s with $v(b_{j'}) < r$. Since $o(j') > M$, we have that every non-zero term of $a_i (\sum_{i'} b_{i'} x^{i'})^i \pmod{\mathcal{M}^{r+1}}$ has degree m which satisfies $o(m) > M$. If $v(a_i) = 0$, then every non-zero term of $a_i (\sum_{i'} b_{i'} x^{i'})^i \pmod{\mathcal{M}^{r+1}}$ is also contributed by some $b_{j'} x^{j'}$'s with $v(b_{j'}) < r$. The monomial $b_{j'} x^{j'}$ with $v(b_{j'}) = r$ can not happen, because $o(i) \geq o(s_1(0)) > 0$. Therefore $o(s_{n_1+1}(r)) > M$. For the same reason, we have $o(s_n(r)) > M$ for all $n \geq n_1 + 1$. □

Next we check some properties about $m_n(r)$'s by taking iterates of $u(x)$.

LEMMA 3.5. *Let π be a prime element in \mathcal{M} and let $w(x) \in \mathcal{O}[[x]]$, with $w(x) = x + \pi^r g(x)$ where $g(x) \in \mathcal{O}[[x]]$. Then $w^{\circ p}(x) \equiv x + p\pi^r g(x) \pmod{\mathcal{M}^{2r}}$.*

Proof. Consider $w^{\circ 2}(x) = w(x) + \pi^r g(w(x)) = x + \pi^r g(x) + \pi^r g(x + \pi^r g(x))$. Since $g(x + \pi^r g(x)) \equiv g(x) \pmod{\mathcal{M}^r}$, we have that $w^{\circ 2}(x) \equiv x + 2\pi^r g(x) \pmod{\mathcal{M}^{2r}}$. By induction, our claim follows. □

PROPOSITION 3.6. *If $r \geq e + 1$ and $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for all $j < r$, then $m_{n+1}(r + e) = m_n(r)$ and $\{m_n(r + e)\}_n \ll \{m_n(j)\}_n$ for all $j < r + e$.*

Proof. By the hypothesis, when n is big enough we can write $u^{\circ p^n}(x) \equiv x + \pi^r g(x) \pmod{x^{m_n(r)+1}}$, where $g(x) \in \mathcal{O}[x]$. Let $g(x) = \sum_{i=1}^{m_n(r)} a_i x^i$. Then by the definition of $m_n(r)$, we have that $v(a_i) \geq 1$ for $i < m_n(r)$ and $v(a_{m_n(r)}) = 0$. By Lemma 3.5, $u^{\circ p^{n+1}}(x) \equiv x + p\pi^r g(x) \pmod{\mathcal{M}^{2r}, x^{m_n(r)+1}} \equiv x + p\pi^r g(x) \pmod{\mathcal{M}^{r+e+1}, x^{m_n(r)+1}}$. Since $v(p) = e$, we have that $m_{n+1}(r + e) = m_n(r)$.

For every n big enough, let t_n be the number among $\{j \mid 0 \leq j < r\}$ such that $m_n(t_n) = \min\{m_n(j) \mid 0 \leq j < r\}$. We can write $u^{\circ p^n}(x) \equiv x + \pi^r h(x) \pmod{x^{m_n(t_n)}}$ where $h(x) \in \mathcal{O}[x]$. By Lemma 3.5, $u^{\circ p^{n+1}}(x) \equiv x + p\pi^r h(x) \pmod{\mathcal{M}^{2r}, x^{m_n(t_n)}} \equiv x + p\pi^r h(x) \pmod{\mathcal{M}^{r+e+1}, x^{m_n(t_n)}}$. All coefficients of $u^{\circ p^{n+1}}(x) - x \pmod{x^{m_n(t_n)}}$ are in \mathcal{M}^{r+e} . Thus $m_{n+1}(j) \geq m_n(t_n) \gg m_n(r) = m_{n+1}(r + e)$ for all $j < r + e$. □

Now we check the lowest degrees of $f \circ u^{\circ p^n}(x) - f(x)$ and $u^{\circ p^n} \circ f(x) - f(x)$ modulo \mathcal{M}^r for $r \leq 3e + 1$. Wherever convenient we write $\mathcal{L}_n(x)$ for $f \circ u^{\circ p^n}(x) - f(x)$ and $\mathcal{R}_n(x)$ for $u^{\circ p^n} \circ f(x) - f(x)$. By Proposition 3.4, there exists n such that $o(s_n(j)) > 3e$ for all $j \leq 3e$. By replacing f by $f^{\circ n}$, we may assume that $o(s_1(j)) > 3e$ for all $j \leq 3e$. For convenience, we replace $s_1(j)$ by $s(j)$.

When $r < e$, because for $v(a) = 0, p \nmid t$ and $s > 3e$,

$$(x + \pi g(x) + ax^m)^{tp^s} \equiv x^{tp^s} + ta^{p^s} x^{p^s(t-1)+mp^s} \pmod{\mathcal{M}^{r+1}, \text{ higher degree}},$$

we have that in $\mathcal{L}_n(x) \pmod{\mathcal{M}^{r+1}}$ the lowest degree contributed by the monomial $a_i x^i$ of $f(x)$ with $v(a_i) \leq r$ is $p^{o(i)}(m_n(0) - 1) + i$. By the definition of $s(j)$, the

lowest degree of $\mathcal{L}_n(x) \bmod \mathcal{M}^{r+1}$ is $\min \{ p^{o(s(j))}(m_n(0) - 1) + s(j); j \leq r \}$ when n is large enough. Therefore if we set

$$d_r = \min \{ o(s(j)) \mid j \leq r \} \text{ and}$$

$$c_r = \min \{ s(j) \mid o(s(j)) = d_r, j \leq r \},$$

then the lowest degree of $\mathcal{L}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$, for sufficiently large n .

When $e \leq r < 2e$, write $r = e + r'$ where $0 \leq r' < e$. Because for $v(a) = 0$, $p \nmid t$ and $s > 3e$,

$$(x + \pi g(x) + ax^m)^{tp^s} \equiv x^{tp^s} + tpa^{p^{s-1}}x^{p^s(t-1)+p^{s-1}(p-1)+mp^{s-1}}$$

(mod \mathcal{M}^{r+1} , higher degree),

we have that in $\mathcal{L}_n(x) \bmod \mathcal{M}^{r+1}$ the lowest degree contributed by the monomial $a_i x^i$ of $f(x)$ with $v(a_i) \leq r'$ is $p^{o(i)-1}(m_n(0) - 1) + i$ and the lowest degree contributed by the monomial $a_j x^j$ of $f(x)$ with $r' < v(a_j) \leq r$ is $p^{o(j)}(m_n(0) - 1) + j$. Therefore if we set

$$d_r = \min \{ o(s(i)) - 1, o(s(j)) \mid i \leq r', r' < j \leq r \} \text{ and}$$

$$c_r = \min \{ s(i), s(j) \mid o(s(i)) - 1 = d_r, o(s(j)) = d_r$$

for $i \leq r', r' < j \leq r \},$

then the lowest degree of $\mathcal{L}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$, for sufficiently large n .

Using a similar argument, when $r = 2e + r'$ where $0 \leq r' < e$, if we set

$$d_r = \min \{ o(s(i)) - 2, o(s(i')) - 1, o(s(j)) \mid i \leq r', r' < i' \leq e + r',$$

$e + r' < j \leq r \}$

$$c_r = \min \{ s(i), s(i'), s(j) \mid o(s(i)) - 2 = o(s(i')) - 1 = o(s(j)) = d_r,$$

for $i \leq r', r' < i' \leq e + r', e + r' < j \leq r \},$

then the lowest degree of $\mathcal{L}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$, for sufficiently large n .

For the lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$, we have the following.

LEMMA 3.7. *If for every $j < r$ we have $m_n(r) < m_n(j) - r$, then the lowest degree of $u^{op^n} \circ f(x) - f(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_0}m_n(r)$.*

Proof. We consider modulo \mathcal{M}^{r+1} . The lowest degree of $\mathcal{R}_n(x)$ contributed by the monomial $b_i x^i$ of $u^{op^n}(x)$ with $v(b_i) < r$ is greater than $p^{d_0}(i - r)$. The lowest degree contributed by the monomial $b_i x^i$ of $u^{op^n}(x)$ with $v(b_i) = r$ is $p^{d_0}i$. Therefore by the definition of $m_n(j)$ and by $m_n(j) - r > m_n(r)$ for all $j < r$, we

have that the lowest degree equals to $p^{d_0}m_n(r)$. □

Now we use the equality $f \circ u^{op^n} - f = u^{op^n} \circ f - f$ to find the relationship between $s(j)$'s and $m_n(i)$'s. Keep the notations about d_r and c_r as above. Notice that these d_r 's have the properties that $d_r \leq d_{r-1}$ and $d_{r+\epsilon} \leq d_r - 1$.

LEMMA 3.8. *If $d_r = d_{r-1}$, then when n is large enough the lowest degree of $u^{op^n} \circ f - f \pmod{\mathcal{M}^{r+1}}$ is $p^{d_0}m_n(t) - (c_t - c_r)$, for some $t < r$ which is independent of n . In fact, t is the number such that $d_r = d_{r-1} = \dots = d_t < d_{t-1}$ and $m_n(t)$ has the property that when n is big enough $m_n(j) \geq m_n(t) - B_r$ for all $j \leq r$, where B_r is independent of n .*

If $d_r < d_{r-1}$ then the lowest degree of $u^{op^n} \circ f - f \pmod{\mathcal{M}^{r+1}}$ is $p^{d_0}m_n(r)$ and we have $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for every $j < r$.

Proof. Suppose that n is large enough such that the lowest degree of $\mathcal{L}_n(x) \pmod{\mathcal{M}^{r+1}}$ is $p^{d_r}(m_n(0) - 1) + c_r$. We use induction on r . First we consider $\mathcal{L}_n(x) \equiv \mathcal{R}_n(x) \pmod{\mathcal{M}^2}$. The lowest degree of $\mathcal{L}_n(x) \pmod{\mathcal{M}^2}$ is $p^{d_1}(m_n(0) - 1) + c_1$. If $d_1 = d_0$, this means $d_0 \leq o(s(1))$. Since $s(0) = p^{d_0}$ (Theorem 3.2), we have $c_1 = c_0 = s(0) = p^{d_0}$. Hence the lowest degree of $\mathcal{R}_n(x) \pmod{\mathcal{M}^2}$ is $p^{d_1}(m_n(0) - 1) + c_1 = p^{d_0}m_n(0) - (c_0 - c_1)$. If $m_n(1) < m_n(0) - 1$, then by Lemma 3.7, the lowest degree of $\mathcal{R}_n(x)$ is $p^{d_0}m_n(1)$, which is not equal to $p^{d_0}m_n(0)$. It is a contradiction. Thus $m_n(1) \geq m_n(0) - 1$.

If $d_1 < d_0$, then since $\{p^{d_1}(m_n(0) - 1) + c_1\}_n \ll \{p^{d_0}m_n(0)\}_n$, we have that the lowest degree of $\mathcal{R}_n(x) \pmod{\mathcal{M}^2}$ is $\ll \{p^{d_0}m_n(0)\}_n$. Notice that the lowest degree of $\mathcal{R}_n(x) \pmod{\mathcal{M}^2}$ is either greater than $p^{d_0}(m_n(0) - 1)$ or equal to $p^{d_0}m_n(1)$. Suppose that the lowest degree is greater than $p^{d_0}(m_n(0) - 1)$. This contradicts that the lowest degree is $\ll \{p^{d_0}m_n(0)\}_n$. Therefore the lowest degree is $p^{d_0}m_n(1)$ and so $\{m_n(1)\}_n \ll \{m_n(0)\}_n$. This proves our assertion for the case $r = 1$.

Suppose our assertion is true for $j < r$. We consider $\mathcal{L}_n(x) \equiv \mathcal{R}_n(x) \pmod{\mathcal{M}^r}$. The lowest degree of $\mathcal{L}_n(x) \pmod{\mathcal{M}^r}$ is $p^{d_{r-1}}(m_n(0) - 1) + c_{r-1}$ and equals to the lowest degree of $\mathcal{R}_n(x) \pmod{\mathcal{M}^r}$, which is $p^{d_0}m_n(t) - (c_t - c_{r-1})$ for some $t \leq r - 1$ such that $d_{r-1} = \dots = d_t < d_{t-1}$. Now consider $\mathcal{L}_n(x) \equiv \mathcal{R}_n(x) \pmod{\mathcal{M}^{r+1}}$. The lowest degree of $\mathcal{L}_n(x) \pmod{\mathcal{M}^{r+1}}$ is $p^{d_r}(m_n(0) - 1) + c_r$. Suppose that $d_r = d_{r-1}$. Since $p^{d_{r-1}}(m_n(0) - 1) + c_{r-1} - p^{d_r}(m_n(0) - 1) - c_r = c_{r-1} - c_r$, we have that the lowest degree of $\mathcal{R}_n(x) \pmod{\mathcal{M}^{r+1}}$ is equal to $p^{d_0}m_n(t) - (c_t - c_r)$. Our assumption also tells us that $\forall j \leq r - 1, m_n(j) \geq m_n(t) - B_{r-1}$ for n big enough. Choose B_r such that $B_r > B_{r-1} + r$ and $p^{d_0}B_r > c_t - c_r$. If there exists n' such that $m_{n'}(r) < m_{n'}(t) - B_r$, then $m_{n'}(r) < m_{n'}(j) - r$. Hence by Lemma 3.7, the lowest degree of $\mathcal{R}_{n'}(x) \pmod{\mathcal{M}^{r+1}}$ is $p^{d_0}m_{n'}(r) < p^{d_0}m_{n'}(t) - (c_t - c_r)$. This contradicts the result that the lowest degree of $\mathcal{R}_n(x) \pmod{\mathcal{M}^{r+1}}$ is $p^{d_0}m_n(t) - (c_t - c_r)$ for n big enough. Therefore we have $m_n(r) \geq m_n(t) - B_r$ when n is large enough.

If $d_r < d_{r-1}$, then $\{p^{d_r}(m_n(0) - 1) + c_r\}_n \ll \{p^{d_{r-1}}(m_n(0) - 1) + c_{r-1}\}_n$. We have that the lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$ is $\ll \{p^{d_0}m_n(t)\}_n$. The lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$ is either greater than $p^{d_0}(m_n(t_n) - r)$ for some $t_n < r$ or equal to $p^{d_0}m_n(r)$. If this degree is greater than $p^{d_0}(m_n(t_n) - r)$, then we have $\{p^{d_0}m_n(t_n)\}_n \ll \{p^{d_0}m_n(t)\}_n$. This contradicts our assumption that $m_n(t_n) \geq m_n(t) - B_{r-1}$. Thus the lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_0}m_n(r)$ and we have that $\{m_n(r)\}_n \ll \{m_n(j)\}_n, \forall j < r$. \square

REMARK 3. If $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for every $j < r$, then by Lemma 3.7, when n is large enough the lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_0}m_n(r)$. Lemma 3.8 tells us that if $d_r = d_{r-1}$, then the lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_0}m_n(t) - (c_t - c_r)$ for some $t < r$. Therefore we have $p^{d_0}m_n(r) = p^{d_0}m_n(t) - (c_t - c_r)$, which contradicts the assumption that $\{m_n(r)\}_n \ll \{m_n(t)\}_n$. Hence $d_r < d_{r-1}$. This implies that $d_r < d_{r-1}$ if and only if $\{m_n(r)\}_n \ll \{m_n(j)\}_n$ for every $j < r$.

Suppose that there exists r such that $e + 1 \leq r \leq 2e$ and $d_r < d_{r-1}$. Then when n is large enough the lowest degree of $\mathcal{L}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_r}(m_n(0) - 1) + c_r$ and the lowest degree of $\mathcal{R}_n(x) \bmod \mathcal{M}^{r+1}$ is $p^{d_0}m_n(r)$. Hence for n big enough we have that

$$\begin{aligned} (1) \quad & p^{d_r}(m_n(0) - 1) + c_r = p^{d_0}m_n(r) \\ (2) \quad & p^{d_r}(m_{n-1}(0) - 1) + c_r = p^{d_0}m_{n-1}(r) \\ (1) - (2) \quad & p^{d_r}(m_n(0) - m_{n-1}(0)) = p^{d_0}(m_n(r) - m_{n-1}(r)). \end{aligned}$$

By Proposition 3.6, we have that $\{m_n(r + e)\}_n \ll \{m_n(j)\}_n$ for all $j < r + e$. Since $d_{r+e} < d_{r+e-1}$, by the same argument as above, we have that

$$\begin{aligned} (3) \quad & p^{d_{r+e}}(m_{n+1}(0) - 1) + c_{r+e} = p^{d_0}m_{n+1}(r + e) \\ (4) \quad & p^{d_{r+e}}(m_n(0) - 1) + c_{r+e} = p^{d_0}m_n(r + e) \\ (3) - (4) \quad & p^{d_{r+e}}(m_{n+1}(0) - m_n(0)) = p^{d_0}(m_{n+1}(r + e) - m_n(r + e)). \end{aligned}$$

Because $m_{n+1}(r + e) - m_n(r + e) = m_n(r) - m_{n-1}(r)$, it follows that

$$\frac{(1) - (2)}{(3) - (4)} \quad m_{n+1}(0) - m_n(0) = p^{d_r - d_{r+e}}(m_n(0) - m_{n-1}(0)).$$

Notice that $d_r > d_{r+e}$.

THEOREM 3.9 (General Case). *Let $u(x), f(x)$ be invertible and noninvertible, respectively, in $\mathcal{S}_0(\mathcal{O})$. Suppose further that $u'(0) \equiv 1 \pmod{\mathcal{M}}$ and $f \circ u = u \circ f$. If we denote $\text{wideg}(u^{op^n}(x) - x)$ by i_n , then there exist M and $\lambda > 0$ such that when $n > M$,*

$$\frac{i_{n+1} - i_n}{i_n - i_{n-1}} = p^\lambda.$$

Proof. We only have to show that there exists r such that $e + 1 \leq r \leq 2e$ and $d_r < d_{r-1}$. This follows immediately from the fact that $d_t \leq d_{t-1}$ and $d_e > d_e - 1 \geq d_{2e}$. \square

REMARK 4. In our proof we only need the assumption that $f \circ u \equiv u \circ f \pmod{\mathcal{M}^{3e+1}}$.

I have used *Mathematica* to run the following examples. All power series are considered over \mathbf{Z}_2 .

EXAMPLE 2. $u_1(x) = 3x + 3x^2 + x^3$

n	$m_n(0)$	$m_n(1)$	$m_n(2)$	$m_n(3)$	$m_n(4)$	$m_n(5)$
0	2	1				
1	8	4	2	1		
2	16	8	4	2	1	
3	32	16	8	4	2	1
4	64	32	16	8	4	2
5	128	64	32	16	8	4

This is an automorphism of the formal group $\mathcal{F}(x, y) = x + y + xy$. As what we calculated before (Proposition 2.2), $m_{n+1}(0) = pm_n(0)$ when $n \geq 1$.

EXAMPLE 3. $u_2(x) = 9x + 6x^2 + x^3$

n	$m_n(0)$	$m_n(1)$	$m_n(2)$	$m_n(3)$	$m_n(4)$	$m_n(5)$
0	3	2		1		
1	5	3	2		1	
2	9	5	3	2	19	1
3	17	9	5	3	2	19
4	33	17	9	5	3	2
5	65	33	17	9	5	3

This is a kind of ‘condensation’ case. $u_2(x)$ commutes with $4x + x^2$ and $m_{n+1}(0) = pm_n(0) - 1$.

EXAMPLE 4. $u_3(x) = 3x + x^3$

n	$m_n(0)$	$m_n(1)$	$m_n(2)$	$m_n(3)$	$m_n(4)$	$m_n(5)$
0	3	1				
1	5	3		1		
2	9	5	3	21	1	51
3	17	9	5	3	37	1
4	33	17	9	5	3	69
5	65	33	17	9	5	3

This is an interesting example. Although $u_3(x)$ can not commute with any non-invertible series (Example 1), we still have $m_{n+1}(0) - m_n(0) = p(m_n(0) - m_{n-1}(0))$. Indeed, since $u_3(x) \equiv u_2(x) \pmod{2\mathbf{Z}}$, we have that $i_n(u_2) = i_n(u_3)$.

References

1. K. Keating: Automorphisms and Extensions of $k((t))$, *J. Number Theory* 41 (1992) no. 3, 314–321.
2. H-C. Li: p -adic Periodic Points and Sen's Theorem, *J. Number Theory*, to appear.
3. H-C. Li: p -adic Power Series which Commute under Composition, *Tran. of A.M.S.*, to appear.
4. J. Lubin: Nonarchimedean Dynamical Systems, *Comp. Math.* 94 (1994) 321–346.
5. J. Lubin: One-Parameter Formal Lie Groups over p -adic Integer Rings, *Ann. of Math.* 80 (1964) 464–484.
6. S. Sen: On Automorphisms of Local Fields, *Ann. of Math.* (2) (1969) 33–46.