p-ADIC FOURIER THEORY FOR $\mathbf{Q}_{p^2}$ AND THE MONNA MAP

KONSTANTIN ARDAKOV AND LAURENT BERGER

ABSTRACT. We show that the coefficients of a power series occurring in p-adic Fourier theory for $\mathbf{Q}_{p^2}$ have valuations that are given by an intriguing formula.

INTRODUCTION

Let L be a finite extension of $\mathbf{Q}_p$, let π be a uniformizer of o_L and let LT be the Lubin-Tate formal o_L-module attached to π. The formal group maps over $o_{\mathbf{C}_p}$ from LT to $\mathbf{G}_{\mathrm{m}}$ play an important role in p-adic Fourier theory (see [ST01]). Choose a coordinate Z on LT, and let $G(Z) \in o_{\mathbf{C}_p}[\![Z]\!]$ be a generator of $\mathrm{Hom}_{o_{\mathbf{C}_p}}(\mathrm{LT}, \mathbf{G}_{\mathrm{m}})$, so that

$$G(Z) = \sum_{k \geq 1} P_k(\Omega) \cdot Z^k = \exp(\Omega \cdot \log_{\mathrm{LT}}(Z)) - 1$$

for a certain element $\Omega \in o_{\mathbf{C}_p}$ and polynomials $P_k(Y) \in L[Y]$. We have (§3 of [ST01]) $\mathrm{val}_p(\Omega) = 1/(p-1) - 1/e(q-1)$ where e is the ramification index of L and $q = |o_L/\pi o_L|$. The power series $G(Z)$ gives rise to a function on $\mathfrak{m}_{\mathbf{C}_p}$ and the theory of Newton polygons then allows us to compute the valuation of $P_k(\Omega)$ for $k = q^j/p^{\lfloor (j-1)/e \rfloor + 1}$ with $j \geq 0$ (Theorem 1.5.2 of [AB24]). However, the valuation of $P_k(\Omega)$ for most $k \geq 2$ has no geometric significance and depends on the choice of the coordinate Z.

During our work on the character variety, we computed the valuation of $P_k(\Omega)$ for many small values of k in a special case: we took $L = \mathbf{Q}_{p^2}$ and $\pi = p$ and chose a coordinate Z on LT for which $\log_{\mathrm{LT}}(Z) = \sum_{m \geq 0} Z^{q^m}/p^m$ (this is possible by §8.3 of [Haz12]). Note that in this setting, the theory of Newton polygons gives $\mathrm{val}_p(P_k(\Omega))$ precisely when k is a power of p. Let $w : \mathbf{Z}_{\geq 0} \to \mathbf{Q}$ be the map defined by

$$w(k) = \frac{p}{q-1} \cdot (k_0 + p^{-1} k_1 + \cdots + p^{-h} \cdot k_h) \text{ if } k = (k_h \cdots k_0)_p \text{ in base } p.$$

For all k for which we were able to compute $\mathrm{val}_p(P_k(\Omega))$, we found that $\mathrm{val}_p(P_k(\Omega)) = w(k)$. The main result of this note is that this formula holds for all k.

Theorem A. *For all $k \geq 1$, we have* $\mathrm{val}_p(P_k(\Omega)) = w(k)$.

The proof involves a careful study of the functional equation that $G(Z)$ satisfies, and a direct computation of $\mathrm{val}_p(P_k(\Omega))$ for small values of k. The function w is related to the Monna map, defined in [Mon52].

Date: May 9, 2024.

1. The polynomials $P_m(Y)$

Let $L = \mathbf{Q}_{p^2}$ and $\pi = p$, so that $q = p^2$, and choose a coordinate Z on LT for which $\log_{\mathrm{LT}}(Z) = \sum_{k \geq 0} Z^{q^k}/p^k$. The polynomials $P_m(Y) \in L[Y]$ are given by

$$\exp(Y \cdot \log_{\mathrm{LT}}(Z)) = \sum_{m=0}^{+\infty} P_m(Y) \cdot Z^m.$$

Proposition 1.1. *We have*

$$P_m(Y) = \sum_{m_0 + q m_1 + \cdots + q^d m_d = m} \frac{Y^{m_0 + \cdots + m_d}}{m_0! \cdots m_d! \cdot p^{1 \cdot m_1 + 2 \cdot m_2 + \cdots + d \cdot m_d}}$$

Proof. Since $\log_{\mathrm{LT}}(Z) = \sum_{k \geq 0} Z^{q^k}/p^k$ and exp is the usual exponential,

$$\sum_{m=0}^{+\infty} P_m(Y) Z^m = \exp(Y \cdot \log_{\mathrm{LT}}(Z)) = \prod_{k \geq 0} \exp(Y \cdot Z^{q^k}/p^k) = \prod_{k \geq 0} \sum_{j \geq 0} (Y \cdot Z^{q^k}/p^k)^j / j!$$

The coefficient of Z^m is the sum of $Y^{m_0 + \cdots + m_d}/m_0! \cdots m_d! \cdot p^{1 \cdot m_1 + 2 \cdot m_2 + \cdots + d \cdot m_d}$ over all $d \geq 0$ and $(m_0, \cdots, m_d) \in \mathbf{Z}_{\geq 0}^{d+1}$ such that $m_0 + q m_1 + \cdots + q^d m_d = m$. □

For example, if $i \leq q - 1$, then

$$P_i(Y) = Y^i / i!$$
$$P_{q+i}(Y) = \frac{Y^{q+i}}{(q+i)!} + \frac{Y^{i+1}}{p \cdot i!}$$
$$P_{2q+i}(Y) = \frac{Y^{2q+i}}{(2q+i)!} + \frac{Y^{q+i+1}}{p \cdot (q+i)!} + \frac{Y^{i+2}}{2p^2 \cdot i!}.$$

Because $L = \mathbf{Q}_{p^2}$, it follows from Lemma 3.4.b of [ST01] that

$$\mathrm{val}_p(\Omega) = \frac{1}{p-1} - \frac{1}{e(q-1)} = \frac{p}{q-1}.$$

Lemma 1.2. *If $i \leq q - 1$ and $i = (ab)_p$ in base p, then* $\mathrm{val}_p(P_i(\Omega)) = \frac{a+bp}{q-1} = w(i)$.

Proof. If $i \leq q - 1$, then $P_i(\Omega) = \Omega^i / i!$ by Proposition 1.1, so that

$$\mathrm{val}_p(P_i(\Omega)) = i \cdot \left(\frac{1}{p-1} - \frac{1}{q-1} \right) - \frac{i - s_p(i)}{p-1} = \frac{s_p(i)}{p-1} - \frac{i}{q-1} = \frac{a+bp}{q-1}.$$ □

2. The map w

Recall that $w : \mathbf{Z}_{\geq 0} \to \mathbf{Q}$ is the map defined by

$$w(k) = \frac{p}{q-1} \cdot (k_0 + p^{-1} k_1 + \cdots + p^{-h} \cdot k_h) \text{ if } k = (k_h \cdots k_0)_p \text{ in base } p.$$

Proposition 2.1. *The function $w : \mathbf{Z}_{\geq 0} \to \mathbf{Q}_{\geq 0}$ has the following properties:*

1. $w(k) < 1 + 1/(q-1)$;
2. $w(k) \geq 1$ *if and only if* $k \equiv -1 \bmod q$, *and then* $w(k) > 1$ *unless* $k = q - 1$;

(3) *if* $\ell > k$, *then* $w(\ell) - w(k) \in \mathbf{Z}$ *if and only if* $k = qj$ *and* $\ell = qj + (q-1)$;
(4) $w(pk) = 1/p \cdot w(k)$;
(5) $w(p^n k + i) = w(p^n k) + w(i)$ *if* $0 \le i \le p^n - 1$;
(6) *For all* $a, b \ge 0$ *we have* $w(a+b) \le w(a) + w(b)$.

Proof. Item (1) results from the fact that

$$w(k) = (k_0 + p^{-1}k_1 + \cdots + p^{-h} \cdot k_h) \cdot \frac{p}{q-1} < \frac{p^2}{q-1} = 1 + \frac{1}{q-1}.$$

If $k_0 \le p-2$, or if $k_0 = p-1$ and $k_1 \le p-2$, then $w(k) \le (p^{h+1}-1-p^{h-1})/p^{h-1}(q-1) < 1$, so if $w(k) \ge 1$, then $k_0 = p-1$ and $k_1 = p-1$, and $k \equiv -1 \bmod q$. Conversely, if $k \equiv -1 \bmod q$, then $k_0 = p-1$ and $k_1 = p-1$, and $w(k) \ge 1$. Finally, if we have equality, then $k_i = 0$ for all $i \ge 2$. This proves (2).

Write $k = (k_h \cdots k_0)_p$ and $\ell = (\ell_i \cdots \ell_0)_p$. Since $w(k) < 1 + 1/(q-1)$, if $w(\ell) - w(k) \in \mathbf{Z}_{\ge 0}$, then $w(\ell) = w(k)$ or $w(\ell) = w(k)+1$. If $w(\ell) = w(k)$, then $k_0 + p^{-1}k_1 + \cdots + p^{-h} \cdot k_h = \ell_0 + p^{-1}\ell_1 + \cdots + p^{-i} \cdot \ell_i$. By comparing p-adic valuations, we get $h = i$, and then $k_h \equiv \ell_i \bmod p$ so that $k_h = \ell_i$. By descending induction, $k_j = \ell_j$ for all j, and $k = \ell$. If $w(\ell) = w(k) + 1$, then $w(\ell) \ge 1$, and hence $\ell = (\ell_i \cdots \ell_2 (p-1)_1 (p-1)_0)_p$ by item (2). We then have $w((\ell_i \cdots \ell_2 0_1 0_0)_p) = w(k)$ and hence $k = (\ell_i \cdots \ell_2 0_1 0_0)_p$. This implies (3).

Items (4) and (5) are straightforward. For item (6), let $\{a_i\}$, $\{b_i\}$ and $\{c_i\}$ be the digits of a, b and c in base p. Let $r_0 = 0$ and let $r_i \in \{0, 1\}$ be the ith carry when adding a and b, so that $c_i = a_i + b_i + r_i - p r_{i+1}$. The result follows from the following computation.

$$\sum_{i \ge 0} \frac{c_i}{p^i} = \sum_{i \ge 0} \frac{a_i + b_i}{p^i} + \frac{r_i}{p^i} - \frac{p r_{i+1}}{p^i} = \sum_{i \ge 0} \frac{a_i + b_i}{p^i} - (p^2 - 1) \sum_{i \ge 1} \frac{r_i}{p^i} \le \sum_{i \ge 0} \frac{a_i + b_i}{p^i}. \qquad \square$$

3. Congruences for the $P_k(\Omega)$

From now on, we write u_k for $P_k(\Omega)$ to lighten the notation. Recall that $q = p^2$. The power series $G(Z)$ is a map between LT and $\mathbf{G}_{\mathrm{m}}$, so that $G([p]_{\mathrm{LT}}(Z)) = [p]_{\mathbf{G}_{\mathrm{m}}}(G(Z))$.

Proposition 3.1. *We have* $\sum_{m=1}^{+\infty} u_m Z^{qm} \equiv \sum_{k=1}^{+\infty} u_k^p Z^{kp} \bmod p \cdot \mathfrak{m}_{\mathbf{C}_p}$.

Proof. We have $G(Z) \in \mathfrak{m}_{\mathbf{C}_p}[\![Z]\!]$ and $[p]_{\mathrm{LT}}(Z) \equiv Z^q \bmod p$ and $[p]_{\mathbf{G}_{\mathrm{m}}}(Z) = Z^p \bmod p$.

Since $G([p]_{\mathrm{LT}}(Z)) = [p]_{\mathbf{G}_{\mathrm{m}}}(G(Z))$, we get $G(Z^q) \equiv G(Z)^p \bmod p \cdot \mathfrak{m}_{\mathbf{C}_p}$. $\square$

Corollary 3.2. *If k is not divisible by p, then* $\mathrm{val}_p(u_k) > 1/p$.

Corollary 3.3. *We have* $u_{pm}^p \equiv u_m \bmod p \cdot \mathfrak{m}_{\mathbf{C}_p}$.

Proof. Take $k = pm$ in Proposition 3.1. $\square$

Corollary 3.4. *Take* $m \ge 0$.

(1) *Suppose that* $\mathrm{val}_p(u_m) \le 1$. *Then* $\mathrm{val}_p(u_{pm}) = 1/p \cdot \mathrm{val}_p(u_m)$.

(2) *Suppose that* $\mathrm{val}_p(u_m) > 1$. *Then* $\mathrm{val}_p(u_{pm}) > 1/p$.

Proof. Both cases follow easily from Corollary 3.3. □

We now compare $[p]_{\mathrm{LT}}(Z)$ and $Z^q + pZ$ (compare with (iv) of §2.2 of [Haz12]).

Lemma 3.5. *We have* $[p]_{\mathrm{LT}}(Z) = Z^q + pZ + p^2 \cdot s(Z)$ *for some* $s(Z) \in Z^2 \cdot \mathbf{Z}_p[\![Z]\!]$.

Proof. There exists $r(Z) \in Z^2 \cdot \mathbf{Z}_p[\![Z]\!]$ such that $[p]_{\mathrm{LT}}(Z) = Z^q + pZ + pr(Z)$. By the properties of $\log_{\mathrm{LT}}$, we have $\log_{\mathrm{LT}}([p]_{\mathrm{LT}}(Z)) = p\log_{\mathrm{LT}}(Z)$. Expanding around Z^q, we get

$$\log_{\mathrm{LT}}(Z^q+pZ+pr(Z)) = \log_{\mathrm{LT}}(Z^q)+(pZ+pr(Z))\log'_{\mathrm{LT}}(Z^q)+\sum_{i\geq 2}\frac{(pZ+pr(Z))^i}{i!}\log^{(i)}_{\mathrm{LT}}(Z^q)$$

Our choice of $\log_{\mathrm{LT}}$ is such that $\log_{\mathrm{LT}}(Z^q) = p\log_{\mathrm{LT}}(Z) - pZ$ and $\log'_{\mathrm{LT}}(Z) \in 1+pZ\cdot\mathbf{Z}_p[\![Z]\!]$ and $\log^{(i)}_{\mathrm{LT}}(Z) \in p\mathbf{Z}_p[\![Z]\!]$ for all $i \geq 2$. Note also that $p^{i+1}/i! \in p^2\mathbf{Z}_p$ for all $i \geq 2$.

The above equation now implies that $pr(Z) \equiv 0 \bmod p^2$ so that $r(Z) = ps(Z)$. □

Corollary 3.6. *The coefficient of* Z^{qn} *in* $G([p]_{LT}(Z))$ *is congruent to* $u_n \bmod p^2$.

Proof. Since $[p]_{\mathrm{LT}}(Z) \equiv Z^q + pZ \bmod p^2$, Lemma 3.5 tells us that

$$\begin{aligned} G([p]_{\mathrm{LT}}(Z)) &\equiv G(Z^q) + pZ\cdot G'(Z^q) \bmod p^2 \\ &\equiv \sum_{k\geq 1} u_k Z^{qk} + \sum_{m\geq 1} pm\cdot u_m Z^{q(m-1)+1} \bmod p^2. \end{aligned}$$

Hence $pZ\cdot G'(Z^q)$ doesn't contribute to the coeffiicent of Z^{qn} modulo p^2. □

Proposition 3.7. *For all* $k \geq 1$, *we have* $k\cdot u_k = u_1 \cdot \sum_{r=0}^{\lfloor \log_q(k)\rfloor} p^r u_{k-q^r}$.

Proof. We have $\sum_{k\geq 0} u_k Z^k = \exp(u_1\cdot\log_{\mathrm{LT}}(Z))$. Applying d/dZ, we get

$$\begin{aligned} \sum_{k\geq 1} ku_k Z^{k-1} &= \exp(u_1\cdot\log_{\mathrm{LT}}(Z))\cdot u_1\cdot\log'_{\mathrm{LT}}(Z) \\ &= u_1\cdot(\sum_{i\geq 0} u_i Z^i)\cdot(\sum_{r\geq 0}(q/p)^r Z^{q^r-1}). \end{aligned}$$

The result follows from looking at the coefficient of Z^{k-1} on both sides. □

Corollary 3.8. *We have* $u_1\cdot u_{k-1} \equiv ku_k \bmod p$ *for all* $k \geq 1$.

Proposition 3.9. *If* $0 \leq i \leq p-1$ *and* $m \geq p$, *then there exists* $\zeta_{i,m} \in o_L$ *such that*

$$u_{mp+i} \equiv \binom{mp+i}{i}^{-1}\cdot u_{mp}\cdot u_i + p\cdot\zeta_{i,m}\cdot u_{p(m-p)+i+1} \bmod p^2.$$

Proof. We proceed by induction on i. When $i = 0$, we can even achieve equality by setting $\zeta_{0,m} := 0$, because $u_0 = 1$. Write $k := mp+i$ for brevity. For $i \geq 1$ we have

$$u_k \equiv \frac{1}{k}u_1\cdot u_{k-1} + \frac{p}{k}u_1\cdot u_{k-q} \bmod p^2$$

by Proposition 3.7, because here $k \in o_L^\times$. By the inductive hypothesis, we have

$$u_{k-1} \equiv \binom{k-1}{i-1}^{-1} u_{mp} \cdot u_{i-1} + p\zeta_{i-1,m} \cdot u_{k-q} \bmod p^2.$$

Note that since $i \leq p-1$, we have $u_i = u_1^i/i!$ by Proposition 1.1, so $u_1 u_{i-1} = \frac{u_1^i}{(i-1)!} = iu_i$. Substituting this information, we obtain

$$\begin{aligned} u_k &\equiv \frac{u_1}{k} \cdot \left(\binom{k-1}{i-1}^{-1} u_{mp} \cdot u_{i-1} + p\zeta_{i-1,m} u_{k-q} \right) + \frac{p}{k} u_1 \cdot u_{k-q} \\ &\equiv \frac{i}{k} \binom{k-1}{i-1}^{-1} u_{mp} \cdot u_i + \frac{p}{k}(\zeta_{i-1,m} + 1) u_1 \cdot u_{k-q} \bmod p^2. \end{aligned}$$

On the other hand, by Corollary 3.8, we have

$$pu_1 \cdot u_{k-q} \equiv p(k-q+1) u_{k-q+1} \bmod p^2.$$

Hence we can rewrite the congruence as follows:

$$u_k \equiv \binom{k}{i}^{-1} u_{mp} \cdot u_i + p\frac{k-q+1}{k}(\zeta_{i-1,m} + 1) u_{k-q+1} \bmod p^2.$$

Define $\zeta_{i,m} := \frac{k-q+1}{k}(\zeta_{i-1,m} + 1)$ and observe that this lies in o_L because $p \nmid k$. □

We need to know what $\zeta_{p-1,m}$ is modulo p.

Lemma 3.10. *Take $1 \leq i \leq p-1$ and $m \geq 0$ and let $k = mp + i$.*
If $\zeta_{0,m} = 0$ and $\zeta_{i,m} = \frac{k-q+1}{k}(\zeta_{i-1,m}+1)$ whenever $1 \leq i \leq p-1$, then $\zeta_{p-1,m} \equiv 0 \bmod p$.

Proof. Note that modulo p, the recurrence relation satisfied by $\zeta_{i,m}$ is simply

$$\zeta_{i,m} \equiv \frac{i+1}{i}(\zeta_{i-1,m} + 1) \bmod p.$$

Now set $i = p-1$ to see that $\zeta_{p-1,m} \equiv 0 \bmod p$. □

4. Proof of Theorem A

We now use the functional equation of $G(Z)$ modulo p^2 in order to prove Theorem A.

Definition 4.1. *For each $n \geq 0$, let C_n be the coefficient of Z^{qn} in*

$$(1 + G(Z))^p = \left(\sum_{k=0}^{\infty} u_k Z^k \right)^p.$$

We develop some notation to compute C_n.

Definition 4.2.

(1) *Let $|\mathbf{k}| := k_1 + \cdots + k_p$ for all $\mathbf{k} \in \mathbf{N}^p$.*
(2) *For each $\mathbf{k} \in \mathbf{N}^p$, define $u_{\mathbf{k}} := u_{k_1} \cdot u_{k_2} \cdot \cdots \cdot u_{k_p}$.*
(3) *For each $n \geq 0$, let $X_n \subset \mathbf{N}^p$ be a complete set of representatives for the orbits of the natural action of S_p on $\{\mathbf{k} \in \mathbf{N}^p : |\mathbf{k}| = n\}$.*

In this language, expanding $\left(\sum_{k=0}^{\infty} u_k Z^k\right)^p$ gives the following

Lemma 4.3. *We have* $C_n = \sum_{\mathbf{k}\in X_{qn}} |S_p \cdot \mathbf{k}|\, u_{\mathbf{k}}$.

Lemma 4.4. *We have* $\mathrm{val}_p(|S_p \cdot \mathbf{k}|) = 1$ *whenever* $k_i \neq k_j$ *for some* $i \neq j$.

Proof. Let H be the stabiliser of $\mathbf{k}$ in S_p, so that $|S_p \cdot \mathbf{k}| = |S_p|/|H|$. If $k_i \neq k_j$ for some $i \neq j$, then H cannot contain any p-cycle. The only elements of S_p of order p are p-cycles, so by Cauchy's Theorem, $\mathrm{val}_p(|H|) = 0$. Hence $\mathrm{val}_p(|S_p|/|H|) = \mathrm{val}_p(|S_p|) = 1$. □

Lemma 4.5. *If* $\mathbf{k} \in X_{qn} \setminus q\mathbf{N}^p$, *then* $\mathrm{val}_p(u_{\mathbf{k}}) > w(n) - 1$.

Proof. Since $\frac{1}{q-1} > w(n) - 1$ by Proposition 2.1(1), it is enough to show that

$$\mathrm{val}_p(u_{\mathbf{k}}) > \frac{1}{q-1}.$$

If some k_i is not divisible by p, then by Corollary 3.2,

$$\mathrm{val}_p(u_{\mathbf{k}}) \geq \mathrm{val}_p(u_{k_i}) > \frac{1}{p} > \frac{1}{q-1}.$$

Assume now that for each $i = 1, \ldots, p$, we can write $k_i = pm_i$ for some $m_i \geq 0$ so that $|\mathbf{m}| = \frac{1}{p}|\mathbf{k}| = pn$. Since $\mathbf{k} \notin q\mathbf{N}^p$ by assumption, we must have $m_i \not\equiv 0 \bmod p$ for some i. Because $|\mathbf{m}| = np \equiv 0 \bmod p$, in this case there must be at least two distinct indices i, j such that $m_i \neq 0 \bmod p$ and $m_j \neq 0 \bmod p$. Using Corollary 3.2 again, we obtain

$$\mathrm{val}_p(u_{\mathbf{m}}) \geq \mathrm{val}_p(u_{m_i}) + \mathrm{val}_p(u_{m_j}) \geq \frac{2}{p} > \frac{p}{q-1}.$$

Suppose now that $\mathrm{val}_p(u_{m_i}) \leq 1$ for all i. Then Corollary 3.4(1) implies that

$$\mathrm{val}_p(u_{\mathbf{k}}) = \frac{1}{p}\,\mathrm{val}_p(u_{\mathbf{m}}) > \frac{1}{p} \cdot \frac{p}{q-1} = \frac{1}{q-1}.$$

Otherwise, for at least one index i we have $\mathrm{val}_p(u_{m_i}) > 1$, and then Corollary 3.4(2) gives

$$\mathrm{val}_p(u_{\mathbf{k}}) \geq \mathrm{val}_p(u_{k_i}) > \frac{1}{p} > \frac{1}{q-1}.$$ □

We can now prove Theorem A.

Theorem 4.6. *We have* $\mathrm{val}_p(u_n) = w(n)$ *for all* $n \geq 0$.

Proof. We prove the stronger statement $\mathrm{val}_p(u_n) = w(n) = p \cdot \mathrm{val}_p(u_{pn})$ by induction on n. The base case $n = 0$ is clear, so assume $n \geq 1$. We first show that $\mathrm{val}_p(u_n) = w(n)$.

Write $n = mp + i$ with $0 \leq i \leq p-1$. Then $\mathrm{val}_p(u_i) = w(i)$ holds by Lemma 1.2. Since $n \neq 0$, we must have $m < n$ so $\mathrm{val}_p(u_{mp}) = \frac{1}{p}w(m)$ by the inductive hypothesis. Using (4) and (5) of Proposition 2.1, we see that

$$\mathrm{val}_p(u_i u_{mp}) = \mathrm{val}_p(u_i) + \mathrm{val}_p(u_{mp}) = w(i) + \frac{1}{p}w(m) = w(pm + i) = w(n).$$

Suppose first that $n \not\equiv -1 \bmod q$. Then $w(n) < 1$ by Proposition 2.1(2), which means that $\operatorname{val}_p(u_i u_{mp}) = w(n) < 1$. By Proposition 3.9, we have

$$u_n \equiv \binom{mp+i}{i}^{-1} u_i u_{mp} \bmod p.$$

We have $\binom{mp+i}{i} \equiv 1 \bmod p$ by Lucas' theorem, and therefore $\operatorname{val}_p(u_n) = w(n)$.

Suppose now that $n \equiv -1 \bmod q$. Then $i = p-1$, and Proposition 3.9 tells us that

$$u_n \equiv \binom{n}{p-1}^{-1} u_{mp} \cdot u_{p-1} + p\zeta_{p-1,m} \cdot u_{n-q+1} \bmod p^2.$$

We have $\zeta_{p-1,m} \equiv 0 \bmod p$ by Lemma 3.10. Hence in fact $u_n \equiv \binom{n}{p-1}^{-1} u_{mp} u_{p-1} \bmod p^2$. Since $\operatorname{val}_p(u_{mp}u_{p-1}) = w(n) < 2$ by Proposition 2.1(1), we again conclude that

$$\operatorname{val}_p(u_n) = \operatorname{val}_p(u_{mp}) + \operatorname{val}_p(u_{p-1}) = w(n).$$

To complete the induction step, we must show that $w(n) = p \operatorname{val}_p(u_{pn}) = \operatorname{val}_p(u_{pn}^p)$. In order to do this, we compare the coefficients of Z^{qn} in the functional equation for $G(Z)$

$$G([p]_{\mathrm{LT}}(Z)) = [p]_{\mathbf{G}_m}(G(Z)) = (1 + G(Z))^p - 1$$

modulo p^2. Using Corollary 3.6 and Lemma 4.3, we see that

$$(\diamond) \qquad u_n \equiv C_n = \sum_{\mathbf{k} \in X_{qn}} |S_p \cdot \mathbf{k}|\, u_{\mathbf{k}} \bmod p^2.$$

Define $\mathbf{k}_0 := (pn, pn, \cdots, pn)$. We will now proceed to show that in fact

$$(\star) \qquad \operatorname{val}_p(|S_p \cdot \mathbf{k}| u_{\mathbf{k}}) > w(n) \quad \text{for all} \quad \mathbf{k} \in X_{qn} \setminus \{\mathbf{k}_0\}.$$

Note that $w(n) < 2$ by Proposition 2.1(1) and that $u_{\mathbf{k}_0} = u_{pn}^p$. Hence congruence $(\diamond)$ together with $(\star)$ imply that $\operatorname{val}_p(u_n - u_{np}^p) > w(n)$. Since we already know that $\operatorname{val}_p(u_n) = w(n)$ this shows that $\operatorname{val}_p(u_{np}^p) = \operatorname{val}_p(u_n) = w(n)$ and completes the proof.

Since at least two entries of $\mathbf{k}$ must be distinct when $\mathbf{k} \neq \mathbf{k}_0$, we have $\operatorname{val}_p(|S_p \cdot \mathbf{k}|) = 1$ by Lemma 4.4, so we're reduced to showing that

$$(\star\star) \qquad \operatorname{val}_p(u_{\mathbf{k}}) > w(n) - 1 \quad \text{for all} \quad \mathbf{k} \in X_{qn} \setminus \{\mathbf{k}_0\}.$$

Fix $\mathbf{k} \in X_{qn} \setminus \{\mathbf{k}_0\}$. When $\mathbf{k} \notin q\mathbf{N}^p$, $(\star\star)$ is precisely the conclusion of Lemma 4.5, so we may assume that $\mathbf{k} \in q\mathbf{N}^p$. Write $\mathbf{k} = q\mathbf{m}$ for some $\mathbf{m} \in \mathbf{N}^p$, so that $|\mathbf{m}| = \frac{1}{q}|\mathbf{k}| = \frac{qn}{q} = n$. We first consider the case where $m_i < n$ for all i, so that by the inductive hypothesis we have $\operatorname{val}_p(u_{pm_i}) = w(m_i)/p$. Suppose that $\operatorname{val}_p(u_{pm_i}) > 1$ for some i. Then by Corollary 3.4(2) and Proposition 2.1(1),

$$\operatorname{val}_p(u_{\mathbf{k}}) \geq \operatorname{val}_p(u_{k_i}) = \operatorname{val}_p(u_{qm_i}) > \frac{1}{p} > \frac{1}{q-1} > w(n) - 1$$

and $(\star\star)$ holds. Otherwise, $\operatorname{val}_p(u_{pm_i}) \leq 1$ for all i and then by Corollary 3.4(1) we have

$$\operatorname{val}_p(u_{k_i}) = \operatorname{val}_p(u_{qm_i}) = \frac{1}{p} \operatorname{val}_p(u_{pm_i}) = \frac{1}{q} w(m_i).$$

Since $|\mathbf{m}| = n$, Proposition 2.1(6) gives

$$\mathrm{val}_p(u_{\mathbf{k}}) \geq \frac{1}{q} \sum w(m_i) \geq \frac{1}{q} \cdot w(n) > w(n) - 1$$

because $w(n) < 1 + 1/(q-1)$ by Proposition 2.1(1). Hence $(\star\star)$ follows.

We're left with the case where at least one m_i is equal to n. But then since $|\mathbf{m}| = n$, all other m_j's are zero and such $\mathbf{m}$'s form a single S_p-orbit of size p. Hence we have to show $(\star\star)$ holds when $\mathbf{k} = (0, 0, \cdots, qn)$.

The congruence $(\diamond)$ together with our estimates above implies

$$\mathrm{val}_p(u_n - (u_{np}^p + pu_{nq})) > w(n).$$

Now, $u_{np} \equiv u_{nq}^p \bmod p$ by Corollary 3.3 so that $u_{np}^p \equiv u_{nq}^q \bmod p^2$. Therefore

$$\mathrm{val}_p(u_n - (u_{nq}^q + pu_{nq})) > w(n).$$

Since we already know that $\mathrm{val}_p(u_n) = w(n)$, we get that

$$\mathrm{val}_p(u_{nq}^q + pu_{nq}) = w(n).$$

We will now see that $\mathrm{val}_p(pu_{nq}) \leq w(n)$ is not possible. Indeed, if $\mathrm{val}_p(pu_{nq}) = w(n)$, then $\mathrm{val}_p(u_{nq}^q) \geq w(n)$ so that $\mathrm{val}_p(u_{nq}) \geq w(n)/q$ and $\mathrm{val}_p(pu_{nq}) \geq 1 + w(n)/q > w(n)$. And if $\mathrm{val}_p(pu_{nq}) < w(n)$ then $\mathrm{val}_p(pu_{nq}) = \mathrm{val}_p(u_{nq}^q)$, so $\mathrm{val}_p(u_{nq}) = 1/(q-1)$. But then $\mathrm{val}_p(pu_{nq}) > 1 + 1/(q-1) > w(n)$ by Proposition 2.1(1).

Hence $\mathrm{val}_p(pu_{nq}) > w(n)$ after all, which is $(\star\star)$ for $\mathbf{k} = (0, 0, \cdots, 0, qn)$. □

References

[AB24] K. Ardakov and L. Berger, *Bounded functions on the character variety*, Münster J. Math. (2024), to appear.

[Haz12] M. Hazewinkel, *Formal groups and applications*, AMS Chelsea Publishing, Providence, RI, 2012, Corrected reprint of the 1978 original.

[Mon52] A. F. Monna, *Sur une transformation simple des nombres p-adiques en nombres réels*, Indag. Math. **14** (1952), 1–9, Nederl. Akad. Wetensch. Proc. Ser. A **55**.

[ST01] P. Schneider and J. Teitelbaum, *p-adic Fourier theory*, Doc. Math. **6** (2001), 447–481.

Konstantin Ardakov, Mathematical Institute, University of Oxford
Email address: ardakov@maths.ox.ac.uk
URL: http://people.maths.ox.ac.uk/ardakov/

Laurent Berger, UMPA, ENS de Lyon, UMR 5669 du CNRS
Email address: laurent.berger@ens-lyon.fr
URL: https://perso.ens-lyon.fr/laurent.berger/