PERIODICITY IN THE p-ADIC VALUATION OF A POLYNOMIAL

LUIS A. MEDINA, VICTOR H. MOLL, AND ERIC ROWLAND

Abstract. For a prime p and an integer x, the p-adic valuation of x is denoted by $\nu_p(x)$. For a polynomial Q with integer coefficients, the sequence of valuations $\nu_p(Q(n))$ is shown to be either periodic or unbounded. The first case corresponds to the situation where Q has no roots in the ring of p-adic integers. In the periodic situation, the period length is determined.

1. Introduction

For p prime and $n \in \mathbb{N}$, the exponent of the highest power of p that divides n is called the *p-adic valuation of n*. This is denoted by $\nu_p(n)$. Given a function $f : \mathbb{N} \to \mathbb{N}$, the study of sequences $\nu_p(f(n))$ goes back to at least Legendre [16], who established the classical formula

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1}, \tag{1.1}$$

where $s_p(n)$ is the sum of the digits of n in base p.

The work presented here forms part of a general project to analyze the sequence

$$V_x = \{\nu_p(x_n) : n \in \mathbb{N}\}$$

for given sequence $x = \{x_n\}$. Valuations have been studied for the Stirling numbers $S(n,k)$ [3, 6], sequences satisfying first-order recurrences [4], the Fibonacci numbers [17], the ASM (alternating sign matrices) numbers [7, 20], and coefficients of a polynomial connected to a quartic integral [2, 8, 21]. Other results of this type appear in [1, 11, 12, 13, 19].

Consider the sequence of valuations

$$V_p(Q) = \{\nu_p(Q(n)) : n \in \mathbb{N}\}, \tag{1.2}$$

for a prime p and a polynomial $Q \in \mathbb{Z}[x]$. The polynomial Q is assumed to be irreducible over $\mathbb{Z}$; otherwise the identity

$$V_p(Q_1 Q_2) = V_p(Q_1) + V_p(Q_2) \tag{1.3}$$

Date: March 28, 2017.

2010 *Mathematics Subject Classification.* Primary 11B83, Secondary 11Y55, 11S05.

Key words and phrases. valuations, polynomial sequences, Hensel's lemma, p-adic integers.

can be used to express $V_p(Q)$ in terms of its irreducible factors. The first result established in this paper is that $V_p(Q)$ is either periodic or unbounded (Theorem 2.1). In the case of a periodic sequence, the period length is explicitly determined (Theorem 5.1). The special case of quadratic polynomials is discussed in detail in Sections 3 and 4.

The analysis includes the p-adic numbers $\mathbb{Q}_p$ and the ring of integers $\mathbb{Z}_p$. Recall that each $x \in \mathbb{Q}_p$ can be expressed in the form

$$x = \sum_{k=k_0}^{\infty} c_k p^k \tag{1.4}$$

with $0 \leq c_k \leq p-1$ and $c_{k_0} \neq 0$.

The p-adic integers $\mathbb{Z}_p$ correspond to the case $k_0 \geq 0$, and invertible elements in this ring have $k_0 = 0$. The set of invertible elements is denoted by $\mathbb{Z}_p^{\times}$. The p-adic absolute value of $x \in \mathbb{Q}_p$ is defined by $|x|_p = p^{-k_0}$. In particular, $x \in \mathbb{Z}_p^{\times}$ if and only if $x \in \mathbb{Z}_p$ and $|x|_p = 1$.

The determination of the sequence $V_p(Q)$ will require examining the irreducibility of Q in $\mathbb{Z}_p[x]$. Some classical criteria are stated below.

Theorem 1.1 (Eisenstein criterion [15, Proposition 5.3.11])**.** *Let* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$*. Assume*

1. $\nu_p(a_n) = 0$,
2. $\nu_p(a_j) > 0$ *for* $0 \leq j < n$, *and*
3. $\nu_p(a_0) = 1$.

Then f *is irreducible in* $\mathbb{Z}_p[x]$*.*

Theorem 1.2 (Hensel's lemma, polynomial version [15, Theorem 3.4.6])**.** *Let* $f \in \mathbb{Z}_p[x]$ *and assume there are non-constant polynomials* g, $h \in \mathbb{Z}_p[x]$, *such that*

1. g *is monic,*
2. g *and* h *are coprime modulo* p, *and*
3. $f(x) \equiv g(x)h(x) \mod p$.

Then f *is reducible in* $\mathbb{Z}_p[x]$*.*

Theorem 1.3 (Dumas Irreducibility Criterion [14])**.** *Let* $f \in \mathbb{Z}_p[x]$ *be given by*

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n. \tag{1.5}$$

Suppose that

1. $\nu_p(a_0) = 0$,
2. $\nu_p(a_i)/i > \nu_p(a_n)/n$ *for* $1 \leq i \leq n-1$, *and*
3. $\gcd(\nu_p(a_n), n) = 1$.

Then f *is irreducible in* $\mathbb{Z}_p[x]$*.*

2. Boundedness of the sequence $V_p(Q)$.

This section characterizes the boundedness of the sequence $V_p(Q)$ in terms of the existence of zeros of the polynomial Q in $\mathbb{Z}_p$. Bell [5] showed that $V_p(Q)$ is periodic in the case that Q has no zeros in $\mathbb{Z}_p$ and gave a bound for the minimal period length.

Theorem 2.1. *Let p be a prime and $Q \in \mathbb{Z}[x]$. Then $V_p(Q)$ is either periodic or unbounded. Moreover, $V_p(Q)$ is periodic if and only if Q has no zeros in $\mathbb{Z}_p$. In the periodic case, the minimal period length is a power of p.*

Proof. Assume that Q has no zeros in $\mathbb{Z}_p$. If $V_p(Q)$ is not bounded there exists a sequence $n_j \to \infty$ such that $\nu_p(Q(n_j)) \to \infty$. The compactness of $\mathbb{Z}_p$ (see [18]) gives a subsequence converging to $n_\infty \in \mathbb{Z}_p$. Then $Q(n_\infty)$ is divisible by arbitrary large powers of p, thus $Q(n_\infty) = 0$. This contradiction shows $V_p(Q)$ is bounded. In order to show $V_p(Q)$ is periodic, define

$$d = \sup \left\{ k \,:\, p^k \text{ divides } Q(n) \text{ for some } n \in \mathbb{Z} \right\}. \tag{2.1}$$

Then $d \geq 0$ and

$$Q(n + p^{d+1}) = Q(n) + Q'(n)p^{d+1} + O(p^{d+2}). \tag{2.2}$$

Since $\nu_p(Q(n)) \leq d$, it follows that

$$\nu_p\left(Q(n + p^{d+1})\right) = \nu_p(Q(n)), \tag{2.3}$$

proving that $\nu_p(Q(n))$ is periodic. The minimal period length is a divisor of p^{d+1}, thus a power of the prime p.

On the other hand, if Q has a zero $x = \alpha$ in $\mathbb{Z}_p$,

$$Q(x) = (x - \alpha)Q_1(x), \text{ with } Q_1 \in \mathbb{Z}_p[x]. \tag{2.4}$$

Then $\nu_p(Q(n)) \geq \nu_p(n - \alpha)$, and $V_p(Q)$ is unbounded. $\square$

The most basic result for establishing the existence of a zero of a polynomial in $\mathbb{Z}_p$ is Hensel's lemma [15, Theorem 3.4.1]. In the following form, it states that a simple root of a polynomial modulo p has a unique lifting to a root in $\mathbb{Z}_p$.

Theorem 2.2 (Hensel's lemma)**.** *If $f \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}_p$ satisfies*

$$f(a) \equiv 0 \mod p \text{ and } f'(a) \not\equiv 0 \mod p \tag{2.5}$$

then there is a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \mod p$.

The following extension appears in [10, Lemma 3.1].

Proposition 2.3. *Assume $f \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}_p$ satisfies*

$$\nu_p(f(a)) > 2\nu_p(f'(a)). \tag{2.6}$$

Then there is $\alpha \in \mathbb{Z}_p$ with $f(\alpha) = 0$ and $\alpha \equiv a \mod p$.

3. Quadratic polynomials and the prime $p = 2$

Let $a \in \mathbb{Z}$ and $Q_a(x) = x^2 - a$. This section considers the periodicity of the sequence $\{\nu_2(n^2 - a)\}$. In view of Theorem 2.1, this is equivalent to the existence of a zero of Q_a in $\mathbb{Z}_2$. An elementary proof of Proposition 3.1 appears in [9]. Define c and $\mu(a)$ by

$$a = 4^{\mu(a)} c \tag{3.1}$$

with $c \not\equiv 0 \mod 4$.

Proposition 3.1. *The polynomial Q_a has no zeros in $\mathbb{Z}_2$ if and only if $c \not\equiv 1 \mod 8$.*

Proof. Assume first that Q_a has no zeros in $\mathbb{Z}_2$ and $c \equiv 1 \mod 8$. If a is odd, then $a = c = 1 + 8j$ with $j \in \mathbb{Z}$. Then $Q_a(1) = 1 - a = -8j$ and

$$|Q_a(1)|_2 \leq \tfrac{1}{8} \text{ and } |Q_a'(1)|_2 = \tfrac{1}{2}. \tag{3.2}$$

Therefore $|Q_a(1)|_2 < (|Q_a'(1)|_2)^2$ and Proposition 2.3 produces $\alpha \in \mathbb{Z}_2$ with $Q_a(\alpha) = 0$. This is a contradiction.

In the case a even, write $a = 4^i(1 + 8j)$ with $i > 0$ and $i \in \mathbb{Z}$. The previous case shows the existence of $\alpha \in \mathbb{Z}_2$ with $\alpha^2 = (1 + 8j)$. Then $\beta = 2^i\alpha$ satisfies $Q_2(\beta) = 0$, yielding a contradiction.

Assume now that $c \not\equiv 1 \mod 8$. If a is odd, then $a = c$ and $a \equiv 3, 5, 7 \mod 8$. A simple calculation shows that

$$\nu_2(n^2 - 8i - 3) = \nu_2(n^2 - 8i - 7) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even,} \end{cases} \tag{3.3}$$

and

$$\nu_2(n^2 - 8i - 5) = \begin{cases} 2 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even.} \end{cases} \tag{3.4}$$

For these values of a, the sequence $V_2(Q)$ is bounded. Theorem 2.1 now shows that Q_a has no zeros in $\mathbb{Z}_2$.

If a is even, then it can be written as $a = 4^j(8i + r)$ with $j \geq 0$ and $r = 2, 3, 5, 6, 7$. The excluded case $r = 4$ can be reduced to one of the residues listed above by consideration of the parity of the index i. Now suppose $Q_a(x)$ has a zero $\beta \in \mathbb{Z}_2$; that is, $\beta^2 = a = 4^j(8i + r)$. Then $\alpha = \beta/2^j \in \mathbb{Z}_2$ satisfies $\alpha^2 = 8i + r$. Each of these cases lead to a contradiction. Indeed, if $r = 3, 5, 7$ the valuations $\nu_2(n^2 - 8i - r)$ are bounded contradicting Theorem 2.1. In the remaining two cases, the polynomial $x^2 - 8i - r$ is irreducible over $\mathbb{Z}_2$ by a direct application of the Eisenstein criterion. Therefore $Q_a(x)$ has no zeros. This concludes the proof. $\square$

The previous result is now restated in terms of periodicity. The explicit period length is given in Section 5.

Theorem 3.2. *Let $Q(x) = x^2 - a$. Define c by the relation $a = 4^{\mu(a)}c$, with $c \not\equiv 0 \mod 4$. Then the sequence $V_2(Q)$ is periodic if and only if $c \not\equiv 1 \mod 8$.*

Combining Theorem 2.1, Proposition 3.1, and the classical result of Lagrange on representations of integers as sums of squares shows that the sequence of valuations $\{\nu_2(n^2 + b) : n \in \mathbb{N}\}$ is bounded if and only if b cannot be written as a sum of three squares.

4. Quadratic polynomials and an odd prime

This section extends the results of Section 3 to the case of odd primes.

Theorem 4.1. *Let $p \neq 2$ be a prime, and let $a \in \mathbb{Z}$ with $k = \nu_p(a)$. The sequence $\nu_p(n^2 - a)$ is periodic if and only if k is odd or a/p^k is a quadratic non-residue modulo p. If it is periodic, its period length is $p^{\lceil k/2 \rceil}$.*

Proof. Let $p \neq 2$. Hensel's lemma shows that an integer a not divisible by p has a square root in $\mathbb{Z}_p$ if and only if a is a quadratic residue modulo p. This implies that $a \in \mathbb{Q}_p$ is a square if and only if it can be written as $a = p^{2m}u^2$ with $m \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$ a p-adic unit. Then $x^2 - a$ has a zero in $\mathbb{Z}_p$ is equivalent to k being even and a/p^k being a quadratic residue modulo p. This proves the first part of the theorem.

Now assume that $\nu_p(n^2 - a)$ is periodic. It is shown that its period length is given by $p^{\lceil k/2 \rceil}$. Suppose first that k is odd. Let $k_* = (k+1)/2$ so that $\lceil k/2 \rceil = k_*$ and

$$\nu_p((n + p^{k_*})^2 - a) = \nu_p(n^2 - a + 2p^{k_*}n + p^{2k_*}). \tag{4.1}$$

It is shown that

$$\nu_p(2p^{k_*}n + p^{2k_*}) > \nu_p(n^2 - a), \tag{4.2}$$

which implies $\nu_p((n + p^{k_*})^2 - a) = \nu_p(n^2 - a)$. Write $n = p^{\nu_p(n)}n_0$ and $a = p^{2k_*+1}a_0$. Finally, let $\gamma = \min(\nu_p(n), k_*)$. Then

$$\begin{aligned}
\nu_p\left(p^{k_*}(2n + p^{k_*})\right) &\geq k_* + \min(\nu_p(2n), k_*) \\
&= k_* + \gamma \\
&> k_* + \gamma + \nu_p(p^{2\nu_p(n) - k_* - \gamma}n_0^2 - p^{k_* - 1 - \gamma}a_0) \\
&= \nu_p(p^{2\nu_p(n)}n_0^2 - p^{2k_* - 1}a_0) \\
&= \nu_p(n^2 - a)
\end{aligned} \tag{4.3}$$

since $0 > \nu_p(p^{2\nu_p(n) - k_* - \gamma}n_0^2 - p^{k_* - 1 - \gamma}a_0)$. To justify this last inequality, observe that if $\nu_p(n) \geq k_*$ then $2\nu_p(n) - k_* - \gamma = 2(\nu_p(n) - k_*) \geq 0$ and $k_* - 1 - \gamma = -1 < 0$, and if $\nu < k_*$ then $2\nu - k_* - \gamma = \nu - k_* < 0$ and $k_* - 1 - \gamma \geq 0$.

Suppose now that k is even and a/p^k a quadratic non-residue. Then, there is $m \in \mathbb{N}_0$ and $a_0 \in \mathbb{Z}$ such that $a = p^{2m}a_0$ with a_0 a quadratic non-residue modulo p. It is now shown that

$$\nu_p((n+p^m)^2 - a) = \nu_p(n^2 - a) \tag{4.4}$$

and that p^m is minimal with this property. If $m = 0$, then (4.4) becomes $\nu_p((n+1)^2) = \nu_p(n^2 - a)$. Both sides vanish since a is a quadratic non-residue modulo p. Now, for $m > 0$, the statement (4.4) becomes

$$(n+p^m)^2 - a \quad = \quad n^2 + 2np^m + p^{2m} - p^{2m}a_0.$$

The proof of (4.4) is divided into cases. In the argument given below, it is assumed that $\gcd(n, n_0) = 1$.

Case 1: Suppose that $n = p^\beta n_0$ with $\beta, n_0 \in \mathbb{Z}$ and $\beta < m$. Observe that

$$\nu_p(n^2 - a) = \nu_p(p^{2\beta} - p^{2m}a_0) = 2\beta$$

and

$$\nu_p(2p^m n + p^{2m}) = \beta + m > 2\beta.$$

Then $\nu_p((n+p^m)^2 - a) = \nu_p(n^2 - a)$ as claimed.

Case 2: Suppose that $n = p^m n_0$ with $n_0 \in \mathbb{Z}$. Note that

$$\nu_p(n^2 - a) = \nu_p(p^{2m}(n_0^2 - a_0)) = 2m,$$

where the last equality follows from the fact that p does not divide $n_0^2 - a_0$, since a_0 is a quadratic non-residue modulo p. On the other hand,

$$\begin{aligned} \nu_p((n+p^m)^2 - a) &= \nu_p(p^{2m}n_0^2 + 2p^{2m}n_0 + p^{2m} - p^{2m}a_0) \\ &= \nu_p(p^{2m}[n_0^2 + 2n_0 + 1 - a_0]) \\ &= \nu_p(p^{2m}[(n_0+1)^2 - a_0]) \\ &= 2m. \end{aligned}$$

This gives (4.4).

Case 3: Finally, suppose that $n = p^\beta n_0$ with $\beta, n_0 \in \mathbb{Z}$ and $\beta > m$. It is easy to see that $\nu_p(n^2 - a) = 2m$. Then

$$\begin{aligned} (n+p^m) - a &= n^2 + 2p^m n + p^{2m} - p^{2m}a_0 \\ &= p^{2\beta}n_0^2 + 2p^{m+\beta}n_0 + p^{2m} - p^{2m}a_0 \\ &= p^{2m}(p^{2\beta-2m}n_0^2 + 2p^{\beta-m} + (1 - a_0)). \end{aligned}$$

Now $1 - a_0 \not\equiv 0 \mod p$ since a_0 is a quadratic non-residue. Therefore p does not divide $1 - a_0$ and (4.4) follows.

The conclusion is that $\nu_p((n + p^{\lceil k/2 \rceil})^2 - a) = \nu_p(n^2 - a)$ for every $n \in \mathbb{N}$. Therefore, the period length is a divisor of $p^{\lceil k/2 \rceil}$. The period length cannot be smaller, since for $n = 0$

$$\nu_p((n+p^i)^2 - a) = \nu_p(p^{2i} - a) = 2i \neq k = \nu_p(-a) = \nu_p(n^2 - a).$$

This completes the proof. $\square$

5. The sequence $V_p(Q)$ for a general polynomial

This section extends the results described in the previous two sections to the more general case of an arbitrary prime p and an arbitrary polynomial in $\mathbb{Z}_p[x]$.

Let $Q \in \mathbb{Z}_p[x]$. The p-adic Weierstrass preparation theorem [15, Theorem 6.2.6] implies the existence of a factorization $Q(x) = p^m u Q_1(x) H(x)$ where $Q_1(x)$ is a monic polynomial with coefficients in $\mathbb{Z}_p$, $u \in \mathbb{Z}_p^{\times}$, m is an integer, and $H(x)$ is a series that converges in $\mathbb{Z}_p$ with the property that $\nu_p(H(x)) = 0$ for every $x \in \mathbb{Z}_p$. Therefore,

$$V_p(Q) = \{\nu_p(Q(n)) : n \in \mathbb{N}\} \tag{5.1}$$

is a shift of $V_p(Q_1)$, showing that the general case can be reduced to the case when $Q(x)$ is a monic polynomial.

Theorem 5.1. *Let $Q \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geq 2$, irreducible over $\mathbb{Z}_p$. Let $\alpha \geq 0$ be the largest non-negative integer such that $Q(x) \equiv 0 \mod p^{\alpha}$ for some $x \in \mathbb{Z}$. Then $V_p(Q)$ is periodic with period length $p^{\lceil \alpha/d \rceil}$.*

In fact a more general result, where $\mathbb{Q}$ is replaced with an arbitrary number field, can be proved in a similar way. Let K be a number field with corresponding number ring R. Choose a prime ideal $\mathfrak{p}$ of R and let $\nu : K^{\times} \to \mathbb{Z}$ be the corresponding valuation. Let $K_{\mathfrak{p}}$ be the completion of K with respect to ν and let $\mathcal{O} = \{a \in K_{\mathfrak{p}} : \nu(a) \geq 0\}$ be the closed unit ball. Let $\pi \in \mathcal{O}$ be a uniformizer, that is, $\nu(\pi) = 1$, and relabel the valuation as ν_{π}.

Theorem 5.2. *Let $Q \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geq 2$, irreducible over $\mathcal{O}$. Let $\alpha \geq 0$ be the largest non-negative integer such that $Q(x) \equiv 0 \mod \pi^{\alpha}$ for some $x \in \mathbb{Z}$. Suppose the residue field $\mathcal{O}/\pi\mathcal{O}$ has characteristic p, and let $e = \nu_{\pi}(p)$ be the ramification index. Then $\{\nu_{\pi}(Q(n)) : n \in \mathbb{N}\}$ is periodic with period length $p^{\lceil \alpha/(ed) \rceil}$.*

The proofs of Theorems 5.1 and 5.2 are based on an expression for the valuation $\nu_{\pi}(Q(n))$.

Theorem 5.3. *Let $A \subseteq \mathcal{O}$ be a subring and let $Q(x) \in A[x]$ be monic polynomial of degree $d \geq 2$, irreducible over $\mathcal{O}$. Let $\alpha \geq 0$ be the largest non-negative integer such that $Q(x) \equiv 0 \mod \pi^{\alpha}$ for some $x \in A$. Choose $n_0 \in A$ such that $Q(n_0) \equiv 0 \mod \pi^{\alpha}$. Then, for $n \in A$,*

$$\nu_{\pi}(Q(n)) = \begin{cases} d\,\nu_{\pi}(n - n_0) & \text{if } n \not\equiv n_0 \mod \pi^{\lfloor \alpha/d \rfloor + 1} \\ \alpha & \text{if } n \equiv n_0 \mod \pi^{\lfloor \alpha/d \rfloor + 1}. \end{cases}$$

Proof. Define the absolute value $|\cdot|_{\pi}$ on K as $|a|_{\pi} = q^{-\nu_{\pi}(a)}$, where $|\mathcal{O}/\pi\mathcal{O}| = q$. Write

$$Q(x) = (x - r_1)(x - r_2) \cdots (x - r_d) \tag{5.2}$$

over a splitting field for Q. Let $r = r_1$ and define $E = K_{\mathfrak{p}}(r)$. Then $E/K_{\mathfrak{p}}$ is a field extension of degree d and the π-adic absolute value extends to E by

$$|s|_\pi = |\operatorname{norm}_{E/K_{\mathfrak{p}}}(s)|_\pi^{1/d}. \tag{5.3}$$

The norm of an element $s \in E$ is

$$\operatorname{norm}_{E/K_{\mathfrak{p}}}(s) = (-1)^{ml} a_0^l, \tag{5.4}$$

where $x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ is the minimal polynomial of s over $K_{\mathfrak{p}}$ and l is the degree of the extension of $E/K_{\mathfrak{p}}(s)$.

For every element $n \in A$, the minimal polynomial of $n - r$ is

$$(x - (n - r_1))(x - (n - r_2)) \cdots (x - (n - r_d)). \tag{5.5}$$

Therefore

$$\begin{aligned} |n - r|_\pi &= |(n - r_1) \cdots (n - r_d)|_\pi^{1/d} \\ &= |Q(n)|_\pi^{1/d} \\ &= \left(q^{-\nu_\pi(Q(n))} \right)^{1/d}. \end{aligned}$$

This gives

$$\nu_\pi(Q(n)) = -d \log_q |n - r|_\pi \tag{5.6}$$

(where $\log_q$ is the real logarithm to base q). Now take any $n_0 \in A$ such that $Q(n_0) \equiv 0 \mod q^\alpha$. Then

$$\begin{aligned} |n - r|_\pi &\leq \max\left(|n - n_0|_\pi, |n_0 - r|_\pi\right) \\ &= \max\left(|n - n_0|_\pi, q^{-\nu_\pi(Q(n_0))/d}\right) \\ &= \max\left(|n - n_0|_\pi, q^{-\alpha/d}\right) \end{aligned}$$

with equality if $|n - n_0|_\pi \neq q^{-\alpha/d}$. The computation of $\nu_\pi(Q(n))$ from this equation is divided into three cases. Define $\beta = \lfloor \alpha/d \rfloor$.

Case 1: If $n \equiv n_0 \mod \pi^{\beta+1}$, then $\nu_\pi(n - n_0) \geq \beta + 1 > \alpha/d$, and it follows that

$$|n - n_0|_\pi = q^{-\nu_\pi(n - n_0)} < q^{-\alpha/d}. \tag{5.7}$$

Then $|n - r|_\pi = q^{-\alpha/d}$ and

$$\nu_\pi(Q(n)) = -d \log_q |n - r|_\pi = \alpha. \tag{5.8}$$

Case 2: If $n \not\equiv n_0 \mod \pi^\beta$, then $\nu_\pi(n - n_0) < \beta \leq \alpha/d$, and

$$|n - n_0|_\pi = q^{-\nu_\pi(n - n_0)} > q^{-\alpha/d}. \tag{5.9}$$

In this case, $|n - r|_\pi = |n - n_0|_\pi$ and

$$\nu_\pi(Q(n)) = -d \log_q |n - r|_\pi = d\, \nu_\pi(n - n_0), \tag{5.10}$$

as claimed.

Case 3: The final case is $n \equiv n_0 \mod \pi^\beta$ and $n \not\equiv n_0 \mod \pi^{\beta+1}$. Then $\nu_\pi(n-n_0) = \beta$ and

$$|n-n_0|_\pi = q^{-\nu_\pi(n-n_0)} = q^{-\beta}. \tag{5.11}$$

If α/d is not an integer, this implies that $|n-n_0|_\pi > q^{-\alpha/d}$, so that $|n-r|_\pi = |n-n_0|_\pi$ as in Case 2, and

$$\nu_\pi(Q(n)) = -d\log_q |n-r|_\pi = d\,\nu_\pi(n-n_0). \tag{5.12}$$

On the other hand, if α/d is an integer then $|n-n_0|_\pi = q^{-\alpha/d}$. In this case, $|n-r|_\pi \le q^{-\alpha/d}$ and

$$\nu_\pi(Q(n)) = -d\log_q |n-r|_\pi \ge \alpha. \tag{5.13}$$

Since $\nu_\pi(Q(n)) \le \alpha$ for all $n \in A$, it follows that $\nu_\pi(Q(n)) = \alpha = d\,\nu_\pi(n-n_0)$, as claimed. □

The proof of Theorem 5.1 is presented next, followed by the proof of Theorem 5.2.

Proof of Theorem 5.1. Let $n_0 \in \mathbb{Z}$ with $Q(n_0) \equiv 0 \mod p^\alpha$ and define $\beta = \lfloor \alpha/d \rfloor$. Assume first that $\alpha/d \notin \mathbb{Z}$. In the rational case, i.e. $\pi = p$, Theorem 5.3 shows that $\nu_p(Q(n))$ depends only on the residue of n modulo $p^{\beta+1}$. Therefore the period length of $V_p(Q)$ is at most $p^{\beta+1}$. Since α/d is not an integer and

$$\nu_p(Q(n_0+p^\beta)) = d\,\nu_p(p^\beta) = d\,\beta \ne \alpha = \nu_p(Q(n_0)), \tag{5.14}$$

the period length is not p^β; therefore the period length is $p^{\beta+1} = p^{\lceil \alpha/d \rceil}$ as claimed.

In the case $\alpha/d \in \mathbb{Z}$ (equal to β), Theorem 5.3 gives

$$\nu_p(Q(n)) = \begin{cases} d\,\nu_p(n-n_0) & \text{if } n \not\equiv n_0 \mod p^{\beta+1} \\ \alpha & \text{if } n \equiv n_0 \mod p^{\beta+1}. \end{cases}$$

If $n \equiv n_0 \mod p^\beta$ and $n \not\equiv n_0 \mod p^{\beta+1}$, then $d\,\nu_p(n-n_0) = \alpha$ and one can move this case to obtain

$$\nu_p(Q(n)) = \begin{cases} d\,\nu_p(n-n_0) & \text{if } n \not\equiv n_0 \mod p^{\beta} \\ \alpha & \text{if } n \equiv n_0 \mod p^{\beta}. \end{cases}$$

It follows that the period length of $V_p(Q)$ is at most p^β. Since

$$\nu_p(Q(n_0+p^{\beta-1})) = d\,\nu_p(p^{\beta-1}) = d\,(\beta-1) \ne \alpha = \nu_p(Q(n_0)),$$

the period length is not $p^{\beta-1}$; therefore the period length is $p^\beta = p^{\lceil \alpha/d \rceil}$. □

The general case follows from the proof of Theorem 5.1.

Proof of Theorem 5.2. Let m be an integer. Since $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then π divides $Q(m)$ if and only if p divides $Q(m)$ (since the coefficients of $Q(x)$ are rational integers). Therefore the sequences $\{\nu_\pi(Q(n)) : n \in \mathbb{N}\}$ and

$\{\nu_p(Q(n)) : n \in \mathbb{N}\}$ have the same period length. Let α_1 be the largest non-negative integer such that $Q(x) \equiv 0 \mod p^{\alpha_1}$ has a solution in $\mathbb{Z}$. Similarly, let α be the largest non-negative integer such that $Q(x) \equiv 0 \mod \pi^{\alpha}$ has a solution in $\mathbb{Z}$. From the proof of Theorem 5.1 one knows that the period length of these sequences is $p^{\lceil \alpha_1/d \rceil}$. However, it follows from $e = \nu_\pi(p)$ that $\alpha = e\alpha_1$. Thus, the period length is given by

$$p^{\lceil \alpha_1/d \rceil} = p^{\lceil \alpha/(ed) \rceil}. \tag{5.15}$$

This concludes the proof. $\square$

6. A collection of examples

This final section presents some examples that illustrate the preceding theorems.

Example 6.1. Let $Q(x) = x^3 + 9x^2 + 81x + 243$ and $p = 3$. Dumas' criterion shows that $Q(x)$ is irreducible over $\mathbb{Z}_3$. A direct calculation yields $\alpha = 5$, i.e. $Q(x) \equiv 0 \mod 3^5$ has solutions, but $Q(x) \equiv 0 \mod 3^6$ does not. Theorem 5.1 implies that $V_3(Q)$ is periodic with period length 9. The explicit 3-adic valuation of $Q(n)$ for $n \in \mathbb{Z}$ is provided by Theorem 5.3. In this case, $\beta = 1$ and choosing $n_0 = 0$ gives

$$\nu_3(Q(n)) = \begin{cases} 0 & \text{if } n \not\equiv 0 \mod 3 \\ 3 & \text{if } n \equiv 3, 6 \mod 9 \\ 5 & \text{if } n \equiv 0 \mod 9. \end{cases}$$

Therefore the fundamental period of $V_3(Q)$ is given by $5, 0, 0, 3, 0, 0, 3, 0, 0$.

The next example offers an interesting twist, using the periodicity of $V_p(Q)$ to determine the reducibility of a polynomial Q.

Example 6.2. Take $Q(x) = x^4 + x^3 + x^2 + 3x + 3 \in \mathbb{Z}_3[x]$ and check $\alpha = 3$. Suppose Q is irreducible in $\mathbb{Z}_3[x]$. Theorem 5.1 then implies that $V_3(Q)$ is periodic with period length 3. But $V_3(Q) = \{1, 2, 0, 1, 3, 0, \dots\}$ does not have period length 3; this contradicts the assumption, and therefore Q is reducible. Now $Q(x) \equiv x^2(x+2)^2 \mod 3$ and Hensel's lemma implies that Q factors in the form

$$Q(x) = (x^2 + \gamma_1 x + \gamma_0)(x^2 + \beta_1 x + \beta_0) \tag{6.1}$$

with γ_j, $\beta_j \in \mathbb{Z}_3$. The polynomials are chosen so that

$$x^2 + \gamma_1 x + \gamma_2 \equiv x^2 \mod 3 \text{ and } x^2 + \beta_1 x + \beta_2 \equiv x^2 + x + 1 \mod 3. \tag{6.2}$$

A direct application of Hensel's lemma gives the expansions

$$\begin{aligned} \gamma_0 &= p + p^2 + p^3 + 2p^4 + 2p^7 + 2p^9 + \cdots \\ \gamma_1 &= 2p^2 + 2p^3 + p^4 + p^7 + 2p^8 + \cdots \\ \beta_0 &= 1 + 2p + 2p^2 + p^3 + 2p^4 + p^5 + p^6 + p^7 + \cdots \\ \beta_1 &= 1 + p^2 + p^4 + 2p^5 + 2p^6 + p^7 + 2p^9 + \cdots , \end{aligned}$$

with $p = 3$. The reader can now check that $V_3(Q_1)$ has period length 3 and $V_3(Q_2)$ has period length 9. It follows that $V_3(Q)$ is periodic with period length 9, and the fundamental period is $1, 2, 0, 1, 3, 0, 1, 2, 0$.

The final examples show how Theorem 5.2 and Theorem 5.3 work in the more general setting of a number field.

Example 6.3. Consider the number field $K = \mathbb{Q}(\sqrt[3]{2})$ and its ring of integers $\mathbb{Z}[\sqrt[3]{2}]$. Choose the prime ideal $\mathfrak{p} = (\sqrt[3]{2})$ and $\pi = \sqrt[3]{2}$. Observe that π lies above the rational prime 2. Let $Q(x) = x^2 - 384 = x^2 - 2^7 \cdot 3$. In this case, $\alpha = 21$, $\beta = 10$, and $n_0 = 0$. Theorem 5.3 implies that

$$\nu_\pi(Q(n)) = \begin{cases} 2\,\nu_\pi(n) & \text{if } n \not\equiv 0 \mod \pi^{11} \\ 21 & \text{if } n \equiv 0 \mod \pi^{11}. \end{cases} \tag{6.3}$$

Using the fact that $e = \nu_\pi(2) = 3$, then equation (6.3) can be written as

$$\nu_\pi(Q(n)) = \begin{cases} 0 & \text{if } n \equiv 1 \mod 2 \\ 6 & \text{if } n \equiv 2 \mod 4 \\ 12 & \text{if } n \equiv 4 \mod 8 \\ 18 & \text{if } n \equiv 8 \mod 16 \\ 21 & \text{if } n \equiv 0 \mod 16. \end{cases} \tag{6.4}$$

Finally, Theorem 5.2 implies that the period length is given by $2^{\lceil \alpha/(ed) \rceil} = 2^{\lceil 21/6 \rceil} = 16$. Indeed, the fundamental period of this sequence is

$$21, 0, 6, 0, 12, 0, 6, 0, 18, 0, 6, 0, 12, 0, 6, 0.$$

The fundamental period of $V_2(Q)$ is

$$7, 0, 2, 0, 4, 0, 2, 0, 6, 0, 2, 0, 4, 0, 2, 0.$$

The next example deals with the case when the values of n are chosen from a subring A different from $\mathbb{Z}$.

Example 6.4. Consider the same number field $K = \mathbb{Q}(\sqrt[3]{2})$, but now choose the prime ideal $\mathfrak{p} = (1 + \sqrt[3]{2})$ with uniformizer $\pi = 1 + \sqrt[3]{2}$. Note that

$$\pi^3 = 3 + 3\sqrt[3]{2} + 3(\sqrt[3]{2})^2 = 3(1 + \sqrt[3]{2} + \sqrt[3]{4}).$$

Let $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ and $v = \sqrt[3]{2} - 1$ and observe that

$$uv = (1 + \sqrt[3]{2} + \sqrt[3]{4})(\sqrt[3]{2} - 1) = 1,$$

thus u and v are units. This implies that $3 = v\pi^3$ and therefore $\mathcal{O}/\pi\mathcal{O} = \mathbb{F}_3$.

Consider the polynomial $Q(x) = x^2 - \pi^5 \in (\mathbb{Z}[\sqrt[3]{2}])[x]$. Observe that in this case, the subring $A \subseteq \mathcal{O}$ from Theorem 5.3 is $A = \mathbb{Z}[\sqrt[3]{2}]$. For this polynomial, $\alpha = 5, \beta = 2$, and $n_0 = 0$. Theorem 5.3 implies

$$\nu_\pi(Q(n)) = \begin{cases} 2\,\nu_\pi(n) & \text{if } n \not\equiv 0 \mod \pi^3 \\ 5 & \text{if } n \equiv 0 \mod \pi^3. \end{cases} \tag{6.5}$$

This equation can be simplified to

$$\nu_\pi(Q(n)) = \begin{cases} 0 & \text{if } n \equiv 1, 2 \mod \pi \\ 2 & \text{if } n \equiv \pi, 2\pi \mod \pi^2 \\ 4 & \text{if } n \equiv \pi^2, 2\pi^2 \mod \pi^3 \\ 5 & \text{if } n \equiv 0 \mod \pi^3. \end{cases} \tag{6.6}$$

If n is restricted to the subring $\mathbb{Z} \subseteq A$, then

$$\nu_\pi(Q(n)) = \begin{cases} 0 & \text{if } n \equiv 1, 2 \mod 3 \\ 5 & \text{if } n \equiv 0 \mod 3. \end{cases} \tag{6.7}$$

In this case, the period length is clearly 3.

Acknowledgments

The authors thank the referee for helpful suggestions. The first author acknowledges the partial support of UPR-FIPI 1890015.00. The second author acknowledges the partial support of NSF-DMS 1112656. The last author was partially supported by a Marie Curie Actions COFUND Fellowship.

References

[1] T. Amdeberhan, D. Callan, and V. Moll. Valuations and combinatorics of truncated exponential sums. *INTEGERS: The Electronic Journal of Combinatorial Number Theory*, 13:#A21, 2013.

[2] T. Amdeberhan, D. Manna, and V. Moll. The 2-adic valuation of a sequence arising from a rational integral. *Jour. Comb. A*, 115:1474–1486, 2008.

[3] T. Amdeberhan, D. Manna, and V. Moll. The 2-adic valuation of Stirling numbers. *Experimental Mathematics*, 17:69–82, 2008.

[4] T. Amdeberhan, L. Medina, and V. Moll. Asymptotic valuations of sequences satisfying first order recurrences. *Proc. Amer. Math. Soc.*, 137:885–890, 2009.

[5] J. Bell. p-adic valuations and k-regular sequences. *Disc. Math.*, 307:3070–3075, 2007.

[6] A. Berribeztia, L. Medina, A. Moll, V. Moll, and L. Noble. The p-adic valuation of Stirling numbers. *Journal for Algebra and Number Theory Academia*, 1:1–30, 2010.

[7] E. Beyerstedt, V. Moll, and X. Sun. The p-adic valuation of ASM numbers. *Journal of Integer Sequences*, 14:art. 11.8.7, 2011.

[8] G. Boros, V. Moll, and J. Shallit. The 2-adic valuation of the coefficients of a polynomial. *Scientia, Series A*, 7:37–50, 2001.

[9] A. Byrnes, J. Fink, G. Lavigne, I. Nogues, S. Rajasekaran, A. Yuan, L. Almodovar, X. Guan, A. Kesarwani, L. Medina, E. Rowland, and V. Moll. A closed-form solution might be given by a tree: the valuation of quadratic polynomials. *Submitted for publication*, 2015.

[10] J. W. S. Cassels. *Local Fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, 1986.

[11] F. Castro, O. Gonzalez, and L. Medina. The p-adic valuation of Eulerian numbers: trees and Bernoulli numbers. *Experimental Mathematics*, 24 (2), 183–195, 2015.

[12] H. Cohen. On the 2-adic valuation of the truncated polylogarithmic series. *The Fibonacci Quarterly*, 37:117–121, 1999.

[13] H. Cohn. 2-adic behavior of numbers of domino tilings. *Elec. Jour. Comb.*, 6:1–14, 1999.

[14] G. Dumas. Sur quelques cas d'irréductibilité des polynômes à coefficientes rationnels. *Journal de Math. Pures et Appl.*, 12:191–258, 1906.

[15] F. Gouvêa. *p-adic Numbers: An Introduction* second edition. Springer–Verlag, 1997.

[16] A. M. Legendre. *Théorie des Nombres.* Firmin Didot Frères, Paris, 1830.

[17] L. Medina and E. Rowland. p-regularity of the p-adic valuation of the Fibonacci sequence. *The Fibonacci Quarterly*, 53(3), 265–271, 2015.

[18] M. R. Murty. *Introduction to p-adic Analytic Number Theory*, volume 27 of *Studies in Advanced Mathematics.* American Mathematical Society, 1st edition, 2002.

[19] A. Straub, V. Moll, and T. Amdeberhan. The p-adic valuation of k-central binomial coefficients. *Acta Arith.*, 149:31–42, 2009.

[20] X. Sun and V. Moll. The p-adic valuation of sequences counting alternating sign matrices. *Journal of Integer Sequences*, 12:09.3.8, 2009.

[21] X. Sun and V. Moll. A binary tree representation for the 2-adic valuation of a sequence arising from a rational integral. *INTEGERS: The Electronic Journal of Combinatorial Number Theory*, 10:211–222, 2010.

Departament of Mathematics, University of Puerto Rico, Rio Piedras, San Juan, PR 00936-8377

E-mail address: `luis.medina17@upr.edu`

Department of Mathematics, Tulane University, New Orleans, LA 70118

E-mail address: `vhm@tulane.edu`

University of Liege, Département de Mathématiques, 4000 Liège, Belgium

Current address: Department of Mathematics, Hofstra University, Hempstead, NY

E-mail address: `eric.rowland@hofstra.edu`