THE VALUATION OF POLYNOMIAL SEQUENCES

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 exact period is determined.

1. INTRODUCTION

For p prime and $n \in \mathbb{N}$, 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 set

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

for given sequence $x = \{x_n\}$. Examples of such sequences include 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, 21], coefficients of a polynomial connected to a quartic integral [2, 8, 18, 22]. Other results of this type appear in [1, 11, 12, 13, 20].

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

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

can be used to express $V_p(Q)$ in terms of its irreducible factors. The main result established here is that $V_p(Q)$ is either periodic or unbounded. In the

Date: May 8, 2015.

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

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

case of a periodic sequence, the period is explicitly determined. The special case of quadratic polynomials is discussed in detail.

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 $0 \leq c_k < p$ 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 $k_0 = 0$. This set is denoted by $\mathbb{Z}_p^{\times}$. The p-adic valuation of $x \in \mathbb{Q}_p$ is defined by $|x|_p = p^{-k_0}$. In particular, $x \in \mathbb{Z}_p^{\times}$ is equivalent to $x \in \mathbb{Z}_p$ and $|x|_p = 1$.

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

Theorem 1.1 (Eisenstein criteria)**.** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$. Assume
a) $\nu_p(a_n) = 0$,
b) $\nu_p(a_j) > 0$ for $0 \leq j < n$,
c) $\nu_p(a_0) = 1$.
Then f is irreducible over $\mathbb{Z}_p[x]$.

Theorem 1.2 (Hensel lemma, polynomial version)**.** Let $f \in \mathbb{Z}_p[x]$ and assume there are non-constant polynomials g_1, $h_1 \in \mathbb{Z}_p[x]$, such that
a) g_1 is monic,
b) g_1 and h_1 are coprime modulo p and
c) $f_1(x) \equiv g_1(x)h_1(x) \bmod p$.
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 over $\mathbb{Z}_p[x]$.

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

This section characterizes the boundedness of the set $V_p(Q)$, in terms of the existence of zeros of the polynomial Q in the ring of p-adic integers $\mathbb{Z}_p$. Bell [5] showed that $V_p(Q)$ is periodic and gave a bound for the minimal period.

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 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 [19]) 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 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. □

3. Hensel's lemma

The criteria developed in Section 2 converts the boundedness of V_Q to the existence of zeros of Q in the ring of p-adic integers $\mathbb{Z}_p$. The most basic analysis of this question involves Hensel's lemma. In the form used here, it states that a simple root of a polynomial modulo p, has a unique lifting to a root in $\mathbb{Z}_p$.

Theorem 3.1. *If $f \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}_p$ satisfies*

$$f(a) \equiv 0 \bmod p \text{ and } f'(a) \not\equiv 0 \bmod p \tag{3.1}$$

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

The idea of the proof is simple: if $\alpha = c_0 + c_1 p + c_2 p^2 + \cdots$ is a root of $f(x) = 0$ in $\mathbb{Z}_p$, it follows that $f(\alpha) \equiv 0 \bmod p$. Write $\alpha = c_0 + tp$ and observe that

$$f(\alpha) = f(c_0 + pt) = f(c_0) + f'(c_0)pt + O(p^2). \tag{3.2}$$

Therefore $f(c_0) \equiv 0 \bmod p$ is a necessary condition for $\alpha \in \mathbb{Z}_p$ to be a root of f. Now (3.2) yields

$$f'(c_0)t \equiv -\frac{f(c_0)}{p} \bmod p. \tag{3.3}$$

The assumption $f'(c_0) \not\equiv 0 \bmod p$ guarantees the existence of a unique solution $t = c_1$ with $0 \le c_1 < p$. The construction of the coefficients c_i in the expansion of the root α proceeds inductively, as explained next. Write $\alpha = c_0 + c_1 p + tp^2$ and expand

$$f(\alpha) = f(c_0 + c_1 p + tp^2) = f(c_0 + c_1 p) + f'(c_0 + c_1 p)tp^2 + O(p^3) \tag{3.4}$$

and check that $f(\alpha) \equiv 0 \bmod p^2$ requires

$$f(c_0 + c_1 p) + f'(c_0 + c_1 p)tp^2 \equiv 0 \bmod p^3. \tag{3.5}$$

The choice of c_1 guarantees $f(c_0 + c_1 p) \equiv 0 \bmod p^2$ and then $f'(c_0 + c_1 p) \equiv f'(c_0) \bmod p$, it follows that (3.5) is equivalent to

$$f'(c_0)t \equiv -\frac{f(c_0 + c_1 p)}{p^2} \bmod p. \tag{3.6}$$

This equation has a unique solution $t = c_2$ with $0 \le c_2 < p$ and the process can be continued indefinitely. This construction produces a sequence $\alpha_k = c_0 + c_1 p + \cdots + c_k p^k$ that converges to $\alpha \in \mathbb{Z}_p$ that solves $f(\alpha) = 0$.

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

Proposition 3.2. *Assume $f \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}_p$ satisfies*

$$\nu_p(f(a)) > 2\nu_p(f'(a)). \tag{3.7}$$

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

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

Let $a \in \mathbb{Z}$ and $Q_a(x) = x^2 - a$. This section considers the existence of a zero of Q_a in $\mathbb{Z}_2$. In view of Theorem 2.1, this is equivalent to the periodicity of the sequence $\{\nu_2(n^2 - a)\}$. An elementary proof of Proposition 4.1 appears in [9]. Define c and $\mu(a)$ by

$$a = 4^{\mu(a)}c \tag{4.1}$$

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

Proposition 4.1. *The polynomial Q_a has no zeros in $\mathbb{Z}_2$ if and only if $c \not\equiv 1 \bmod 8$.*

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

$$|Q_a(1)|_2 \le \tfrac{1}{8} \text{ and } |Q_a'(1)|_2 = \tfrac{1}{2}. \tag{4.2}$$

Therefore $|Q_a(1)|_2 < (|Q_a'(1)|_2)^2$ and Proposition 3.2 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 $c \not\equiv 1 \bmod 8$. If a is odd, then $a = c$ and $a \equiv 3, 5, 7 \bmod 8$. A simple calculation shows that

$$\nu_2(n^2 - 8i - 3) = \nu_2(n^2 - 8i - 7) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} , \end{cases} \tag{4.3}$$

and

$$\nu_2(n^2 - 8i - 5) = \begin{cases} 2 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} . \end{cases} \tag{4.4}$$

For these values of a, the set $V_2(Q)$ 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 Einsenstein criterion [15, Proposition 5.3.11, p. 156]. Therefore $Q_a(x)$ has no zeros. This concludes the proof. □

The previous result is now restated in terms of periodicity. The explicit form of the period is given in Section 6.

Theorem 4.2. *Let $Q(x) = x^2 - a$. Define c by the relation $a = 4^{\mu(a)}c$, with $c \not\equiv 0 \bmod 4$. Then the set $V_2(Q)$ is periodic if and only if $c \not\equiv 1 \bmod 8$.*

Combining Theorem 2.1, Proposition 4.1 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.

5. Quadratic polynomials and an odd prime

This section extends the results of Section 4 to the case of odd primes.

Theorem 5.1. *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 nonresidue 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 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

$$\nu_p((n+p^{k_*})^2-a)=\nu_p(n^2-a+2p^{k_*}n+p^{2k_*}). \tag{5.1}$$

It is shown that

$$\nu_p(2p^{k_*}n+p^{2k_*})>\nu_p(n^2-a), \tag{5.2}$$

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

$$\begin{aligned}\nu_p\left(p^{k_*}(2n+p^{k_*})\right) &\geq k_*+\min(\nu_p(2n),k_*)\\ &= k_*+\gamma\\ &> k_*+\gamma+\nu_p(p^{2\nu_p(n)-k_*-\gamma}n_0^2-p^{k_*-1-\gamma}a_0)\\ &= \nu_p(p^{2\nu_p(n)}n_0^2-p^{2k_*-1}a_0)\\ &= \nu_p(n^2-a)\end{aligned} \tag{5.3}$$

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 nonresidue. 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

$$\nu_p((n+p^m)^2-a)=\nu_p(n^2-a) \tag{5.4}$$

and that p^m is minimal with this property. If $m=0$, then (5.4) 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 (5.4) becomes

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

The proof of (5.4) 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 (5.4).

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 $1 - a_0 \not\equiv 0 \bmod p$ since a_0 is a quadratic non-residue. Therefore p does not divide $1 - a_0$ and (5.4) 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 is a divisor of $p^{\lceil k/2 \rceil}$. The period 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. □

6. The set $V_p(Q)$ for a general irreducible monic polynomial

This section extends the results described in the last two sections to the set

$$V_p(Q) = \{\nu_p(Q(n)) : n \in \mathbb{N}\} \tag{6.1}$$

where p is a prime and Q is a monic polynomial, irreducible over the ring of p-adic integers $\mathbb{Z}_p$.

The main result is described next. Bell [5] showed that $V_p(Q)$ is periodic, the next theorem provides the exact period.

Theorem 6.1. *Let $Q \in \mathbb{Z}[x]$ be a monic polynomial of degree $d \geq 2$, irreducible over $\mathbb{Z}_p$. Let $\alpha \geq 1$ be the smallest non-negative integer such that $Q(x) \equiv 0 \bmod p^\alpha$ has no solutions. Then $V_p(Q)$ is periodic of period length $p^{\lceil \frac{\alpha-1}{d} \rceil}$.*

The proof of Theorem 6.1 is based on an expression for the valuation $\nu_p(Q(n))$.

Theorem 6.2. *Let Q, p and α as in Theorem 6.1. Let $n_0 \in \mathbb{Z}$ such that $Q(n_0) \equiv 0 \bmod p^{\alpha-1}$. Define $\beta = \left\lfloor \dfrac{\alpha-1}{d} \right\rfloor$. Then*

(6.2)
$$\nu_p(Q(n)) = \begin{cases} d\,\nu_p(n-n_0) & \text{if} \quad n \not\equiv n_0 \bmod p^{\beta}, \\ d\beta & \text{if} \quad n \equiv n_0 \bmod p^{\beta} \text{ and } n \not\equiv n_0 \bmod p^{\beta+1}, \\ \alpha - 1 & \text{if} \quad n \equiv n_0 \bmod p^{\beta+1}. \end{cases}$$

Proof. Write

$$Q(x) = (x-r_1)(x-r_2)\cdots(x-r_d) \tag{6.3}$$

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

$$|s|_p = |\mathrm{norm}_{K/\mathbb{Q}_p}(s)|_p^{1/d}. \tag{6.4}$$

(See [15, Theorem 5.3.5]). The norm of an element $s \in K$ is given by

$$\mathrm{norm}_{K/\mathbb{Q}_p} = (-1)^{me} a_0^e, \tag{6.5}$$

where $x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ is the minimal polynomial of s over $\mathbb{Q}_p$ and e is the degree of the extension $K/\mathbb{Q}_p(s)$.

For every integer n, the minimal polynomial of $n - r$ is

$$(x-(n-r_1))(x-(n-r_2))\cdots(x-(n-r_d)) \tag{6.6}$$

therefore

$$\begin{aligned} |n-r|_p &= |(n-r_1)\cdots(n-r_d)|_p^{1/d} \\ &= |Q(n)|_p^{1/d} \\ &= \left(p^{-\nu_p(Q(n))}\right)^{1/d}. \end{aligned}$$

This gives

$$\nu_p(Q(n)) = -d \log_p |n-r|_p \tag{6.7}$$

(where $\log_p$ is the real logarithm to base p). Now take any $n_0 \in \mathbb{Z}$ such that $Q(n_0) \equiv 0 \bmod p^{\alpha-1}$. Then

$$\begin{aligned} |n-r|_p &\le \max\{|n-n_0|_p, |n_0-r|_p\} \\ &= \max\left(|n-n_0|_p, p^{-\nu_p(Q(n_0))/d}\right) \\ &= \max\left(|n-n_0|_p, p^{-(\alpha-1)/d}\right) \end{aligned}$$

with equality if $|n-n_0|_p \neq p^{-(\alpha-1)/d}$. The computation of $\nu_p(Q(n))$ from (6.7) is divided into three cases (recall $\beta = \left\lfloor \frac{\alpha-1}{d} \right\rfloor$):

Case 1. If $n \not\equiv n_0 \bmod p^{\beta}$, then $\nu_p(n-n_0) < \left\lfloor \frac{\alpha-1}{d} \right\rfloor \le \frac{\alpha-1}{d}$, and it follows that

$$|n-n_0|_p = p^{-\nu_p(n-n_0)} > p^{-\frac{\alpha-1}{d}}. \tag{6.8}$$

Then $|n-r|_p = |n-n_0|_p$ and

$$\nu_p(Q(n)) = -d\log|n-r|_p = d\nu_p(n-n_0), \tag{6.9}$$

as claimed.

Case 2. On the other hand, if $n \equiv n_0 \bmod p^{\beta+1}$, then

$$\nu_p(n-n_0) \geq \left\lfloor \frac{\alpha-1}{d} \right\rfloor + 1 > \frac{\alpha-1}{d}, \tag{6.10}$$

and

$$|n-n_0|_p = p^{-\nu_p(n-n_0)} < p^{-\frac{\alpha-1}{d}}. \tag{6.11}$$

In this case, $|n-n_0| = p^{-(\alpha-1)/d}$ and

$$\nu_p(Q(n)) = -d\log|n-r|_p = \alpha - 1. \tag{6.12}$$

Case 3. The final case is $n \equiv n_0 \bmod p^\beta$ and $n \not\equiv n_0 \bmod p^{\beta+1}$. Then $\nu_p(n-n_0) = \beta$ and therefore

$$|n-n_0|_p = p^{-\nu_p(n-n_0} < p^{-\frac{\alpha-1}{d}}. \tag{6.13}$$

If $(\alpha-1)/d$ is not an integer, this implies $|n-n_0|_p > p^{-(\alpha-1)/d}$, so that $|n-r|_p = |n-n_0|_p$ and

$$\nu_p(Q(n)) = -d\log_p|n-r|_p = d\nu_p(n-n_0) = d\beta. \tag{6.14}$$

On the other hand, if $(\alpha-1)/d$ is an integer, $|n-n_0|_p = p^{-(\alpha-1)/d}$. Then $|n-r|_p \leq p^{-(\alpha-1)/d}$ and

$$\nu_p(Q(n)) = -d\log_p|n-r|_p \geq \alpha - 1. \tag{6.15}$$

Since $\nu_p(Q(n)) \leq \alpha - 1$ holds for all $n \in \mathbb{Z}$, it follows that $\nu_p(Q(n)) = \alpha - 1$, as claimed. □

The proof of Theorem 6.1 is presented next.

Take $n_0 \in \mathbb{Z}$ with $Q(n_0) \equiv 0 \bmod p^{\alpha-1}$ and recall $\beta = \left\lfloor \frac{\alpha-1}{d} \right\rfloor$. Assume first that $\frac{\alpha-1}{d} \notin \mathbb{Z}$. Theorem 6.2 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 $(\alpha-1)/d$ is not an integer and

$$\nu_p\left(Q\left(n_0+p^\beta\right)\right) = d\beta \neq \alpha - 1 = \nu_p(Q)(n_0), \tag{6.16}$$

the period length is not p^β. In the case $\frac{\alpha-1}{d} \in \mathbb{Z}$ (equal to β), Theorem 6.2 gives

$$\nu_p(Q(n)) = \begin{cases} d\nu_p(n-n_0) & \text{if } n \not\equiv n_0 \bmod p^\beta \\ \alpha - 1 & \text{if } n \equiv n_0 \bmod p^\beta. \end{cases} \tag{6.17}$$

It follows that the period length of $V_p(Q)$ is at most p^β. This is exactly the period length, since

$$\nu_p\left(Q\left(n_0+p^{\beta-1}\right)\right) = d\nu_p\left(p^{\beta-1}\right) = d(\beta-1) \neq \alpha - 1 = \nu_p(Q(n_0)).$$

The expression for the period is easily seen to agree with the statement of Theorem 6.1. The proof is complete.

7. Extension to the non-monic situation

This section discusses the set $V_p(Q)$ for a general polynomial

$$Q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{7.1}$$

with coefficients in $\mathbb{Z}_p$.

Example 7.1. Let $Q(x) = a_1 x + a_0$ with $a_k \in \mathbb{Z}_p$. If $a_1 \in \mathbb{Z}_p^\times$, write $Q(x) = a_1 Q_1(x)$ with $Q_1(x) = x + b_0$ and $b_0 = a_1^{-1} a_0 \in \mathbb{Z}_p$. Then

$$\nu_p(Q(n)) = \nu_p(a_1) + \nu_p(Q_1(n)) = \nu_p(Q_1(n)). \tag{7.2}$$

The situation has been reduced to the monic case.

The previous example extends to polynomials of higher degree in a natural way.

Proposition 7.1. Let $Q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}_p[x]$. Assume $a_n \in \mathbb{Z}_p^\times$. Then $Q(x) = a_n Q_1(x)$ with $Q_1 \in \mathbb{Z}_p[x]$ monic and $V_p(Q) = V_p(Q_1)$.

Example 7.2. Let $Q(x) = a_2 x^2 + a_1 x + a_0$ with $a_k \in \mathbb{Z}_p$. If p does not divide a_2, then a_2 is invertible and $V_p(Q)$ can be reduced to the monic case as explained above. Assume now that p divides a_2. The discussion is divided into three cases. It may be assumed that one of the coefficients a_k is not divisible by p. Otherwise, factoring the highest power of p appearing among the coefficients, produces a shift in the set $V_p(Q)$.

Case 1. Suppose p divides a_1 but not a_0. Then p does not divide $Q(n)$ and $V_p(Q) = \{0\}$.

Case 2. Assume p divides a_0 but not a_1. Then

$$Q(0) \equiv 0 \bmod p \text{ and } Q'(0) \equiv a_1 \not\equiv 0 \bmod p. \tag{7.3}$$

Hensel's lemma implies the existence of $\alpha \in \mathbb{Z}_p$ such that $Q(\alpha) = 0$. Thus Q is reducible. Since $\deg(Q) = 2$, this implies $V_p(Q)$ is unbounded.

Case 3. Assume p does not divide either a_1 nor a_0. Define

$$g(x) = x^2 Q(1/x) = a_0 x^2 + a_1 x + a_2 \tag{7.4}$$

and observe that $g(x) \equiv x(a_0 x + a_1) \bmod p$. Hensel's lemma implies the existence of polynomials g_1, $g_2 \in \mathbb{Z}_p[x]$ with $\deg(g_1) = \deg(g_2) = 1$ and $g(x) = g_1(x) g_2(x)$. Then $Q(x) = \hat{g_1}(x)\hat{g_2}(x)$, with $\hat{g_k}(x) = x g_k(1/x)$. This implies that Q is reducible and, as in Case 2, $V_p(Q)$ is unbounded.

Theorem 7.2. Let $Q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}_p[x]$ with $a_n \equiv 0 \bmod p$. Then the analysis of $V_p(Q)$ can be reduced to the monic case.

Proof. Assume first that there is an index k such that p does not divide a_k. Otherwise factoring the maximal power of p produces a shift in $V_p(Q)$. The discussion is divided into two cases.

Case 1. Suppose $p|a_k$ for $k = 1, 2, \cdots, n$, but p does not divide a_0. Then $\nu_p(Q(n)) = 0$ and $V_p(Q) = \{0\}$.

Case 2. Let $0 < k < n$ be the largest index such that p does not divide a_k. Define

$$g(x) = x^n Q(1/x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \tag{7.5}$$

then

$$g(x) \equiv x^{n-k}\left(a_0 x^k + a_1 x^{k-1} + \cdots + a_k\right) \bmod p. \tag{7.6}$$

Hensel's lemma implies the existence of q_1, $q_2 \in \mathbb{Z}_p[x]$ with $\deg(q_1) = k$ and $\deg(q_2) = n - k$ and $g(x) = g_1(x)g_2(x)$. This shows that $Q(x)$ is reducible. The result now follows by induction on the degree of Q. The initial cases $\deg(Q) = 1$, 2 have been discussed above. □

Example 7.3. Consider $Q(x) = 6x^5 + x^4 + 3x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$. Let $g(x) = x^5Q(1/x) = x^5+x^3+3x^2+x+6$. Then $g(x) \equiv x(x+1)^2(x+2)^2 \bmod 3$. Hensel Lemma produces polynomials

$$\begin{aligned} q_1(x) &= x + \gamma_0 \\ q_2(x) &= x^2 + \beta_1 x + \beta_0 \\ q_3(x) &= x^2 + \lambda_1 x + \lambda_0 \end{aligned}$$

with $\gamma_0, \beta_0, \beta_1, \lambda_0, \lambda_1 \in \mathbb{Z}_p$ such that $g(x) = q_1(x)q_2(x)q_3(x)$. In fact, the first few iterations of Hensel Lemma yields (with $p = 3$):

$$\begin{aligned} \gamma_0 &= 2p + 2p^3 + p^4 + 2p^5 + 2p^6 + 2p^7 + p^8 + p^9 + p^{10} + \cdots \\ \beta_0 &= 1 + 2p + p^2 + p^6 + 2p^7 + 2p^8 + p^{10} + \cdots \\ \beta_1 &= 2 + p + 2p^2 + p^5 + 2p^6 + p^7 + p^8 + 2p^9 + \cdots \\ \lambda_0 &= 1 + p + p^2 + 2p^3 + p^7 + p^{10} + \cdots \\ \lambda_1 &= 1 + 2p + 2p^2 + 2p^3 + 2p^5 + p^7 + 2p^8 + p^9 + \cdots . \end{aligned}$$

Therefore,

$$Q(x) = (\gamma_0 x + 1)(\beta_0 x^2 + \beta_1 x + 1)(\lambda_0 x^2 + \lambda_1 x + 1) = \hat{q}_1(x)\hat{q}_2(x)\hat{q}_3(x).$$

Since $p|\gamma_0$, it follows that $\nu_3(\hat{q}_1(n)) = 0$ for all $n \in \mathbb{Z}$. After multiplication by β_0^{-1}, Theorem 6.1 implies that $V_3(\hat{q}_2)$ is periodic with fundamental period $\{0, 0, 1\}$. Similarly, $V_3(\hat{q}_3)$ is periodic with fundamental period is $\{0, 1, 0\}$. The conclusion is that $V_3(Q)$ is periodic with period length 3 and fundamental period $\{0, 1, 1\}$.

8. A collection of examples

This final section presents some examples that illustrate the results given here. The analysis of the examples often requires to check the irreducibility of the underlying polynomial.

The first collection of examples deals with quadratic polynomials. Theorem 2.1 states that $V_p(Q)$ is periodic if and only if Q has no zeros in $\mathbb{Z}_p$. For polynomials of degree 2 or 3 the non-existence of zeros is equivalent to the irreducibility of Q. In particular, if $Q(x) = x^2 - a$, then writing $a = 4^{\mu(a)}c$, with $c \not\equiv 0 \bmod 4$, it was shown that Q is irreducible (equivalently $V_2(Q)$ is periodic) if and only if $c \not\equiv 1 \bmod 8$.

Example 8.1. Let $Q(x) = x^2 - 1$. Then $Q(1) = 0$ and $1 \in \mathbb{Z}_2$, so $V_2(Q)$ is unbounded. The complete set $V_2(Q)$ is easy to determine. For $n \in \mathbb{Z}$ even, $\nu_2(n^2 - 1) = 0$. Therefore $0 \in V_2(Q)$. For n odd, written as $n = 2^\alpha t + 1$ with $\alpha \geq 1$ and t odd, the identity

$$(2^\alpha t + 1)^2 - 1 = 2^{\alpha+1} t \left(2^{\alpha-1} t + 1\right) \tag{8.1}$$

shows that $\nu_2(n^2 - 1) = \alpha + 1$ for $\alpha > 1$. Therefore $\{3, 4, 5, \cdots\} \subset V_2(Q)$. In the case $\alpha = 1$, the identity $n^2 - 1 = 2^2 t(t + 1)$, implies $\nu_2(n^2 - 1) \geq 3$. Therefore

$$V_2(Q) = \{0, 3, 4, 5, \cdots\}. \tag{8.2}$$

Example 8.2. Let $Q(x) = x^2 - 2$. Eisenstein's criteria shows that Q is irreducible over $\mathbb{Z}_2$ and Theorem 4.2 shows that $V_2(Q)$ is periodic. The congruence $Q(x) \equiv 0 \bmod 2$ has solutions but $Q(x) \equiv 0 \bmod 2^2$ does not. Therefore $\alpha = 2$ and Theorem 6.1 shows that $V_2(Q)$ has period 2. Indeed, the fundamental period for $V_2(Q)$ is $\{0, 1\}$.

Example 8.3. The polynomial $Q(x) = x^2 - 32$ has $V_2(Q)$ periodic of period 8. The basic period is $\{0, 2, 0, 4, 0, 2, 0, 5, 0, 2\}$ and

$$\nu_2(n^2 - 32) = \begin{cases} 0 & \text{if } n \equiv 1 \bmod 2 \\ 2 & \text{if } n \equiv 2 \bmod 4 \\ 4 & \text{if } n \equiv 4 \bmod 8 \\ 5 & \text{if } n \equiv 5 \bmod 8. \end{cases} \tag{8.3}$$

Example 8.4. Using the notation in (4.1) observe that $68 = 4 \cdot 17$ and $17 \equiv 1 \bmod 8$. Then $Q(x) = x^2 - 68$ is reducible over $\mathbb{Z}_2$ and $V_2(Q)$ is unbounded. The first few values of this sequence are given by

$$\{2, 0, 6, 0, 2, 0, 5, 0, 2, 0, 5, 0, 2, 0, 7\}. \tag{8.4}$$

The reader might check that $V_2(Q)$ includes 0, 2 and every integer above 5.

The next example consider a quadratic polynomial and the prime $p = 3$.

Example 8.5. Let $Q(x) = x^2 - 405$. From $405 = 3^4 \cdot 5$ it follows that $k = \nu_3(405) = 4$ is even. Moreover $405/3^4 = 5$ and 5 is a quadratic non-residue modulo 3. Theorem 5.1 shows that $V_3(Q)$ is periodic with period 9. The fundamental period of this sequence is $\{4, 0, 0, 2, 0, 0, 2, 0, 0\}$.

The next series of examples involve polynomials of degree at least 3.

Example 8.6. Take $Q(x) = x^3 + 9x^2 + 81x + 243$. Dumas's criterion shows that $Q(x)$ is irreducible over $\mathbb{Z}_3$. A direct calculation yields $\alpha = 6$, i.e. $Q(x) \equiv 0 \bmod 3^5$ has solutions, but $Q(x) \equiv 0 \bmod 3^6$ does not. Theorem 6.1 implies that $V_3(Q)$ is periodic with period length 9. The reader can verify that the fundamental period is given by $\{5, 0, 0, 3, 0, 0, 3, 0, 0\}$.

The explicit 3-adic valuation of $Q(n)$ for $n \in \mathbb{Z}$ is provided by Theorem 6.2. In this case, $\beta = 1$ and choosing $n_0 = 0$ gives

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

Example 8.7. Now take $Q(x) = x^3 + 619x^2 + 13137x + 49367$. Apply Dumas's criterion to $Q(x+2)$ to conclude that $Q(x)$ is irreducible over $\mathbb{Z}_5$. In this case $\alpha = 8$ and Theorem 6.1 shows $V_5(Q)$ is periodic with period length 125.

The explicit 5-adic valuation of $Q(n)$ for $n \in \mathbb{Z}$ is provided by Theorem 6.2. In this case $\beta = 2$ and n_0 can be chosen to be 2. Thus,

$$\nu_5(Q(n)) = \begin{cases} 3\,\nu_5(n-2) & \text{if } n \not\equiv 2 \bmod 25 \\ 6 & \text{if } n \equiv 2 \bmod 25 \text{ and } n \not\equiv 2 \bmod 125 \\ 7 & \text{if } n \equiv 2 \bmod 125. \end{cases}$$

The valuation $\nu_5(n-2)$, for $n \not\equiv 2 \bmod 25$, is now made explicit to produce

$$\nu_5(Q(n)) = \begin{cases} 0 & \text{if } n \not\equiv 2 \bmod 5 \\ 3 & \text{if } n \equiv 7, 12, 17, 22 \bmod 25 \\ 6 & \text{if } n \equiv 27, 52, 77, 102 \bmod 125 \\ 7 & \text{if } n \equiv 2 \bmod 125. \end{cases}$$

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

Example 8.8. Take $Q(x) = x^4 + x^3 + x^2 + 3x + 3 \in \mathbb{Z}_3[x]$ and check $\alpha = 4$. It is claimed that Q is reducible over $\mathbb{Z}_3[x]$. Otherwise Theorem 6.1 shows that $V_3(Q)$ is periodic of period 3. But $V_3(Q) = \{1, 2, 0, 1, 3, 0, \cdots\}$ does not have period 3 and Q is reducible. Now $Q(x) \equiv x^2(x+2)^2 \bmod 3$ and Hensel's lemma implies that Q factors in the form

$$Q(x) = (x^2 + \gamma_1 x + \gamma_0)(x^2 + \beta_1 x + \beta_0) \tag{8.5}$$

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

$$x^2+\gamma_1 x+\gamma_2 \equiv x^2 \bmod 3 \text{ and } x^2+\beta_1 x+\beta_2 \equiv x^2+x+1 \bmod 3. \tag{8.6}$$

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 3 and $V_3(Q_2)$ has period 9. It follows that $V_3(Q)$ is periodic is period 9 with fundamental period is $\{1, 2, 0, 1, 3, 0, 1, 2, 0\}$.

Example 8.9. Take $p=3$ and $Q(x)=27x^5+x^4+2x^3+x^2+3x+9 \in \mathbb{Z}_3[x]$. Then $Q(x) \equiv x^2(x^2+2x+1) \bmod 3$. Hensel Lemma implies the existence of polynomials $Q_1(x), Q_2(x) \in \mathbb{Z}_3[x]$ with $\deg(Q_1)=2$ and $\deg(Q_2)=3$ such that $Q(x)=Q_1(x)Q_2(x)$. Indeed, the first iterations of Hensel's Lemma produce $Q_1(x)=x^2+\gamma_1 x+\gamma_0$ and $Q_2(x)=27x^3+\beta_2 x^2+\beta_1 x+\beta_0$ where

$$\begin{aligned}
\gamma_0 &= p^2+2p^3+p^4+2p^5+p^7+p^9+\cdots\\
\gamma_1 &= p+p^4+2p^5+2p^6+p^7+2p^8+p^9+\cdots\\
\beta_0 &= 1+p+2p^2+2p^4+2p^6+p^7+2p^8+2p^9+\cdots\\
\beta_1 &= 2+2p+2p^2+2p^3+p^4+p^6+2p^7+2p^8+p^9+\cdots\\
\beta_2 &= 1+2p^4+2p^5+2p^6+p^7+\cdots,
\end{aligned}$$

with $p=3$.

Theorem 6.1 implies that $V_3(Q_1)$ is periodic with period length 9. Define now $\hat{Q}_2(x)=x^3Q_2(1/x)$ and observe that $\hat{Q}_2(x) \equiv x(1+x)^2 \bmod 3$. Hensel's lemma now gives polynomials $\hat{q}_1(x), \hat{q}_2(x) \in \mathbb{Z}_3[x]$ such that $\hat{Q}_2(x)=\hat{q}_1(x)\,\hat{q}_2(x)$ with $\deg(\hat{q}_1)=1$, $\deg(\hat{q}_2)=2$. An approximation of $\hat{q}_1(x)=x+\lambda_0$ and $\hat{q}_2(x)=\omega_2 x^2+\omega_1 x+\omega_0$ is

$$\begin{aligned}
\lambda_0 &= p^3+2p^6+p^9+\cdots\\
\omega_0 &= 1+p^3+2p^4+2p^5+2p^6+p^7+2p^8+p^9+\cdots\\
\omega_1 &= 2+2p+2p^2+p^3+p^5+p^6+\cdots\\
\omega_2 &= 1+p+2p^2+2p^4+2p^6+p^7+2p^8+2p^9+\cdots.
\end{aligned}$$

Then $Q_2(x)=x^3\hat{Q}_2(1/x)=(\lambda_0 x+1)(\omega_0 x^2+\omega_1 x+\omega_2)=q_1(x)q_2(x)$. Observe that $\nu_3(q_1(n))=0$ for all $n \in \mathbb{Z}$. Theorem 6.1 gives that $V_3(q_2)$ is periodic with period length 3. The conclusion is that $V_3(Q)$ is periodic with period 9 and fundamental period $\{2, 0, 1, 4, 0, 1, 2, 0, 1\}$.

Acknowledgments. 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 is partially supported by a Marie Curie Actions COFUND Fellowship.

References

[1] T. Amdeberhan, D. Callan, and V. Moll. p-adic analysis and combinatorics of truncated exponential sums. *INTEGERS, Electronic Journal of Combinatorial Number Theory*, 13, #A21:1–16, 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*, To appear, 2015.

[12] H. Cohen. On the 2-adic valuation of the truncated polylogarithmic series. *Fib. Quart.*, 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. Gouvea. *p-adic numbers*. Springer-Verlag, 2nd edition, 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*, To appear, 2015.

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

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

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

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

[22] X. Sun and V. Moll. A binary tree representation for the 2-adic valuation of a sequence arising from a rational integral. *Integers*, 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
E-mail address: rowland@lacim.ca