PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 3, March 2009, Pages 885–890
S 0002-9939(08)09580-4
Article electronically published on September 24, 2008

ASYMPTOTIC VALUATIONS OF SEQUENCES SATISFYING FIRST ORDER RECURRENCES

TEWODROS AMDEBERHAN, LUIS A. MEDINA, AND VICTOR H. MOLL

(Communicated by Martin Lorenz)

ABSTRACT. Let t_n be a sequence that satisfies a first order homogeneous recurrence $t_n = Q(n)t_{n-1}$, where Q is a polynomial with integer coefficients. We describe the asymptotic behavior of the p-adic valuation of t_n.

1. INTRODUCTION

The p-adic valuation $\nu_p(x)$, for $x \in \mathbb{Q}$, $x \neq 0$, is defined by

$$x = p^{\nu_p(x)} \frac{a}{b}, \tag{1.1}$$

where $a, b \in \mathbb{Z}$ and p divides neither a nor b. The value $\nu_p(0)$ is defined to be ∞.

In this paper we establish the asymptotic behavior of the p-adic valuation of sequences that satisfy first order recurrences,

$$t_n = Q(n)t_{n-1}, \; n \geq n_0, \tag{1.2}$$

where Q is a polynomial with integer coefficients and $n_0 \in \mathbb{N}$. Let v be the maximum modulus of all the (possibly none) zeros of Q in $\mathbb{Z}$. If $v > 0$, we choose $n_0 > v$ to guarantee $t_n \neq 0$. Without loss of generality, we always assume that $n_0 = 0$ and $t_0 = 1$. The notation $t_n(Q)$ is used while referring to (1.2).

The identity

$$\nu_p(t_n(Q)) = \sum_{i=1}^{n} \nu_p(Q(i)) \tag{1.3}$$

shows that only the zeros of Q in $\mathbb{Z}/p\mathbb{Z}$ contribute to the value of $\nu_p(t_n(Q))$. Moreover, it shows that it suffices to consider the case where $Q(x)$ is irreducible over $\mathbb{Z}$. This assumption will be enforced. The asymptotic analysis employs Hensel's lemma. The version stated here is reproduced from [3].

Lemma 1.1 (Hensel's Lemma). *Let f be a polynomial with coefficients in the p-adic integers $\mathbb{Z}_p$. Write $f'(x)$ for its formal derivative. If $f(x) \equiv 0 \bmod p$ has a solution a_1, satisfying $f'(a_1) \not\equiv 0 \bmod p$, then there is a unique p-adic integer a such that $f(a) = 0$ and $a \equiv a_1 \bmod p$.*

We now state our main result. It provides an asymptotic description of the valuation of the sequence t_n, defined by (1.2).

Received by the editors September 10, 2007, and, in revised form, March 18, 2008.
2000 *Mathematics Subject Classification.* Primary 11B37; Secondary 11B50, 11B83.
Key words and phrases. Valuations, Hensel's lemma, recurrences.

Theorem 1.2. *Let $Q(x) \in \mathbb{Z}[x]$. Assume $Q(x)$ factors over $\mathbb{Z}_p$ as*

$$Q(x) = \left(\prod_{j=1}^{m} (x - \beta_j) \right) Q_1(x), \tag{1.4}$$

where $Q_1(x) \not\equiv 0 \bmod p$ for any $x \in \mathbb{Z}_p$. Then the sequence $\{t_n\}$, defined by (1.2), satisfies

$$\nu_p(t_n(Q)) = \frac{mn}{p-1} + O(\log n). \tag{1.5}$$

Section 2 contains the proof of Theorem 1.2, and Section 3 presents examples illustrating the main result.

2. The proof

Assume Q has no roots in $\mathbb{N} \cup \{0\}$. The general case is reduced to this one by a shift of the independent variable. Using (1.4), this suffices to study the asymptotic behavior of

$$\nu_p \left(\prod_{i=1}^{n} (i - \beta_j) \right). \tag{2.1}$$

Define

$$r_{jn} = \max\{k : p^k | (i - \beta_j) \text{ for some } 1 \leq i \leq n\}. \tag{2.2}$$

The value of (2.1) is given by

$$\sum_{k=1}^{r_{jn}} \#\{1 \leq i \leq n : p^k | (i - \beta_j)\}. \tag{2.3}$$

Let $\gamma_{jk} \in \mathbb{Z}$ be such that

$$\beta_j \equiv \gamma_{jk} \bmod p^k. \tag{2.4}$$

Then $p^k | (i - \beta_j)$ if and only if $i \equiv \gamma_{jk} \bmod p^k$. Since the number of such i between 1 and n is either

$$\left\lfloor \frac{n}{p^k} \right\rfloor \text{ or } \left\lfloor \frac{n}{p^k} \right\rfloor + 1, \tag{2.5}$$

we have

$$\sum_{k=1}^{r_{jn}} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \nu_p \left(\prod_{i=1}^{n} (i - \beta_j) \right) \leq \sum_{k=1}^{r_{jn}} \left\lfloor \frac{n}{p^k} \right\rfloor + 1. \tag{2.6}$$

By definition $p^{r_{jn}}$ divides $|Q(i)|$ for some $1 \leq i \leq n$. Therefore

$$p^{r_{jn}} \leq |Q(i)| \leq \max\{|Q(1)|, |Q(2)|, \cdots, |Q(n)|\} \leq C n^{\deg(Q)}, \tag{2.7}$$

where the constant C depends only on the coefficients of Q. This implies that $r_{jn} = O(\log n)$. From (2.6) we now obtain

$$\sum_{k=1}^{r_{jn}} \left(\frac{n}{p^k} - 1 \right) \leq \nu_p \left(\prod_{i=1}^{n} (i - \beta_j) \right) \leq \sum_{k=1}^{r_{jn}} \left(\frac{n}{p^k} + 1 \right) \tag{2.8}$$

and

$$\nu_p\left(\prod_{i=1}^{n}(i-\beta_j)\right) = \frac{n}{p-1} - \frac{np^{-r_{jn}}}{p-1} + O(\log n). \tag{2.9}$$

The bound $r_{jn} \geq \lfloor \log n/\log p \rfloor$ shows that the second term in (2.9) satisfies

$$\frac{np^{-r_{jn}}}{p-1} = O(1), \tag{2.10}$$

and we conclude that

$$\nu_p\left(\prod_{i=1}^{n}(i-\beta_j)\right) = \frac{n}{p-1} + O(\log n). \tag{2.11}$$

Theorem 1.2 has been established.

We now consider the factorization (1.4). If all zeros of $Q(x)$ in $\mathbb{Z}/p\mathbb{Z}$ satisfy the hypothesis of Hensel's Lemma, then $Q(x)$ factors over the p-adic numbers as

$$Q(x) = \left(\prod_{j=1}^{z_p(Q)}(x-\beta_j)\right) Q_1(x), \tag{2.12}$$

where the β_j are p-adic integers and $Q_1(x) \equiv 0 \bmod p$ has no solutions in $\mathbb{Z}/p\mathbb{Z}$. Therefore we have

Corollary 2.1. *Let $Q(x) \in \mathbb{Z}[x]$. Assume each of the roots of Q satisfies the hypothesis of Hensel's Lemma. Let $z_p(Q)$ denote the number of roots of Q in $\mathbb{Z}/p\mathbb{Z}$, that is,*

$$z_p(Q) = \left|\{b \in \{1, 2, \cdots, p\} : Q(b) \equiv 0 \bmod p\}\right|. \tag{2.13}$$

Then the sequence $\{t_n\}$, defined by (1.2), satisfies

$$\nu_p(t_n(Q)) = \frac{z_p(Q)n}{p-1} + O(\log n). \tag{2.14}$$

3. Examples

In this section we present some examples illustrating Theorem 1.2.

Definition 3.1. Given a polynomial $Q(x) \in \mathbb{Z}[x]$ and a prime p, we say that $a \in \mathbb{Z}/p\mathbb{Z}$ is a *Hensel zero* of Q if $Q(a) \equiv 0 \bmod p$ and $Q'(a) \not\equiv 0 \bmod p$. The prime p is called a *Hensel prime* for Q if all the zeros of Q in $\mathbb{Z}/p\mathbb{Z}$ are Hensel zeros.

If $Q(x)$ is irreducible over $\mathbb{Z}$, any prime that does not divide the discriminant $D(Q)$ of Q is a Hensel prime. This follows from the fact that $D(Q)$ is the resultant of Q and Q' (see [2]), and so there exist polynomials $A(x)$ and $B(x)$ with integer coefficients such that $A(x)Q(x) + B(x)Q'(x) = D(Q)$.

Corollary 2.1 is now expressed as:

Corollary 3.1. *Let p be a Hensel prime for $Q(x) \in \mathbb{Z}[x]$. Then the sequence $\{t_n\}$ satisfies*

$$\nu_p(t_n(Q)) = \frac{z_p(Q)n}{p-1} + O(\log n). \tag{3.1}$$

This is illustrated in the next example.

Example 3.2. Let $Q(x) = x^2 - 17$. The discriminant of Q is given by $D(Q) = 68 = 2^2 \cdot 17$. Therefore the non-Hensel primes for Q are $p = 2$ and 17. For all other primes p we have

$$\nu_p(t_n(Q)) \sim \frac{z_p(Q)n}{p-1} = \frac{2n}{p-1} \tag{3.2}$$

if 17 is a square modulo p and $\nu_p(t_n) = 0$, otherwise.

The cases $p = 2$ and $p = 17$ are discussed next. For $p = 2$, note that only $1 \in \mathbb{Z}/2\mathbb{Z}$ is a zero modulo 2 with $Q(1) = -16$ and $Q'(1) = 2$. The analysis of the asymptotics of $\nu_2(t_n)$ requires a modified version of Hensel's Lemma in which the condition $f'(a_1) \not\equiv 0 \bmod p$ is replaced by $|f(a_1)|_p < (|f'(a_1)|_p)^2$. See [1] for details. The inequality $|Q(1)|_2 < (|Q'(1)|_2)^2$ shows that the root $a = 1 \in \mathbb{Z}/2\mathbb{Z}$ can be lifted to an element $\alpha \in \mathbb{Z}_2$ with $Q(\alpha) = 0$. Then $-\alpha$ is the second root of $Q(x)$ and we conclude that $\nu_2(t_n) \sim 2n$. Figure 1 shows $\nu_2(t_n)$. For the prime $p = 17$, this method does not apply because $Q(x)$ is irreducible over $\mathbb{Z}_{17}$. The result $\nu_{17}(t_n) \sim n/17$ will be established as a consequence of Theorem 3.4.

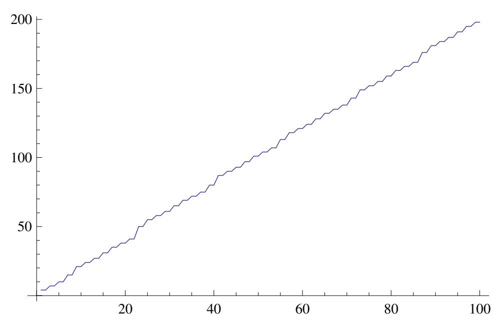

FIGURE 1. The valuation $\nu_2(t_n)$ for $Q(x) = x^2 - 17$.

Example 3.3. Let $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$ for p an odd prime. This polynomial is irreducible over $\mathbb{Z}_p$, so the general method described above does not apply. However, it is easy to establish

$$\nu_p(\Phi_p(x)) = \begin{cases} 0 & \text{if } x \not\equiv 1 \bmod p, \\ 1 & \text{if } x \equiv 1 \bmod p. \end{cases} \tag{3.3}$$

We conclude that $\nu_p(t_n(\Phi_p)) \sim n/p$. Figure 2 shows $\nu_5(t_n(\Phi_5))$.

The next theorem provides a framework for irreducible polynomials that includes the previous two examples.

Theorem 3.4. *Assume that $Q(x)$ is a monic irreducible polynomial of degree $m > 1$ over $\mathbb{Z}_p$. Define $l = \sup\{k : p^k | Q(i) \text{ for some } i \in \mathbb{Z}\}$. Then*

$$\nu_p(t_n(Q)) = \sum_{k=1}^{\lfloor l/m \rfloor} m\frac{n}{p^k} + \left(l - m\left\lfloor \frac{l}{m} \right\rfloor \right) \frac{n}{p^{\lfloor l/m \rfloor + 1}} + O(1). \tag{3.4}$$

Proof. The compactness of $\mathbb{Z}_p$ shows that $l < \infty$. If not, there is a sequence of integers $\{a_n\}$ such that $Q(a_n) \to 0$ in $\mathbb{Q}_p$. The limit of any convergent subsequence produces a zero of Q in $\mathbb{Z}_p$. This contradicts the irreducibility of $Q(x)$ over $\mathbb{Z}_p$.

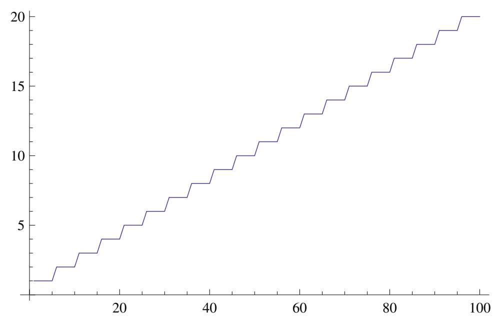

FIGURE 2. The valuation $\nu_5(t_n(\Phi_5))$.

Without loss of generality assume $l \geq 1$. Let $n_0 \in \mathbb{Z}$ be such that $p^l | Q(n_0)$. Assume that $\alpha_1, \cdots, \alpha_m$ are the roots of $Q(x)$ in the algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. The p-adic absolute value on $\mathbb{Q}_p$ can be extended to $\bar{\mathbb{Q}}_p$ and this extension is invariant under Galois transformations over $\mathbb{Q}_p$. Therefore, for $i \in \mathbb{Z}$ we have that $|i - \alpha_j|_p$ is the same for all $j = 1, \cdots, m$. Since $|Q(n_0)|_p = p^{-l}$ we conclude that $|n_0 - \alpha_j|_p = p^{-l/m}$.

Now, assume $|i - n_0|_p = p^{-k}$. If $k \leq l/m$, then it is clear that $|i - \alpha_j|_p = p^{-k}$ and $|Q(i)|_p = p^{-mk}$. This is a direct consequence of the non-Archimedean triangle inequality. On the other hand, if $k > l/m$, then $|Q(i)|_p = p^{-l}$. This is because $|Q(i)|_p \geq p^{-l}$ for any $i \in \mathbb{Z}$. Since

$$\#\{1 \leq i \leq n : |i - n_0|_p = p^{-k}\} = \frac{n}{p^k} - \frac{n}{p^{k+1}} + O(1)$$

and

$$\#\{1 \leq i \leq n : |i - n_0|_p \leq p^{-(\lfloor l/m \rfloor + 1)}\} = \frac{n}{p^{\lfloor l/m \rfloor + 1}} + O(1),$$

we conclude that

$$\begin{aligned}
(3.5) \qquad \nu_p(t_n(Q)) &= \sum_{k=1}^{\lfloor l/m \rfloor} mk \frac{n}{p^k} \left(1 - \frac{1}{p}\right) + l \frac{n}{p^{\lfloor l/m \rfloor + 1}} + O(1) \\
&= \sum_{k=1}^{\lfloor l/m \rfloor} m \frac{n}{p^k} + \left(l - m \left\lfloor \frac{l}{m} \right\rfloor\right) \frac{n}{p^{\lfloor l/m \rfloor + 1}} + O(1).
\end{aligned}$$

Theorem 3.4 has been established. □

Note 3.1. In example 3.3 we have $l = 1$. Therefore (3.4) gives $\nu_p(t_n(\Phi_p)) = n/p + O(1)$, as before. A similar argument shows that, in the case $p = 17$ in example 3.2, we obtain $\nu_{17}(t_n(Q)) = n/17 + O(1)$. This completes the analysis presented in that example.

ACKNOWLEDGMENTS

The authors wish to thank Michael Joyce and Tài Huy Hà for discussions about the problems presented here and the referee for improving the presentation of this manuscript. The work of the third author was partially funded by NSF-DMS 0409968. The second author was partially supported as a graduate student by the same grant.

References

[1] F. Gouvea. *p-adic Numbers*. Springer-Verlag, 2nd edition, 1997. MR1488696 (98h:11155)

[2] S. Lang. *Algebra*. Springer-Verlag, revised third edition, 2002. MR1878556 (2003e:00003)

[3] M. Ram Murty. *Introduction to p-adic Analytic Number Theory*, volume 27 of Studies in Advanced Mathematics. American Mathematical Society, 1st edition, 2002. MR1913413 (2003c:11151)

Department of Mathematics, Tulane University, New Orleans, Louisiana 70118
E-mail address: tamdeberhan@math.tulane.edu

Department of Mathematics, Tulane University, New Orleans, Louisiana 70118
E-mail address: lmedina@math.tulane.edu

Department of Mathematics, Tulane University, New Orleans, Louisiana 70118
E-mail address: vhm@math.tulane.edu